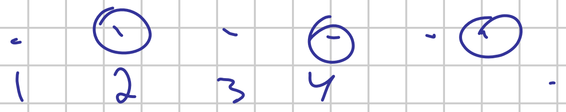
3) $|\{1,2,3,4,\dots\}| = |\{2,4,6,\dots\}|$:

betrachte $f: \{1,2,3,\dots\} \to \{2,4,6,\dots\}$
$n \mapsto 2n$



$\boxed{\text{Def. 2.10}}$ M heißt **höchstens gleichmächtig** zu N (schreibe $|M| \leq |N|$), wenn es eine inj. Abb. $f: M \to N$ gibt. Wenn $|M| \leq |N|$, aber $|M| \neq |N|$, dann heißt M **weniger mächtig** als N (und N **mächtiger** als M)

Schreibe: $|M| < |N|$.

Bsp

1) M, N endlich. Dann ist N mächtiger als M $\iff$ mehr Elemente. (warum?)

2) M endlich, N unendl. $\Rightarrow |M| < |N|$ (warum?)

Bemerkung

1) Wenn $|M| \leq |N|$, dann ist M gleichmächtig mit einer Teilmenge von N ($f(M)$, wobei $f: M \to N$ inj.)

2) Allgemein gilt:

Hörsaalübung ($|M| \leq |N| \iff \exists A \subset N$ mit $|M| = |A|$

$\iff \exists$ surj. $g: N \to M$

Auswahlaxiom (kommt fast gleich)

3) Es gilt: $|M| \le |N|$ und $|N| \le |M| \Rightarrow |N| = |M|$

– ohne Beweis (Satz von Schröder – Bernstein)

Satz 2.11 (Cantor, 1890)

Sei M eine Menge. Dann $\nexists$ surj. Abb. $f: M \to \mathcal{P}(M)$ und es gilt:

$$\boxed{|M| < |\mathcal{P}(M)|}$$

Beweis 1) $|M| \le |\mathcal{P}(M)|$: betrachte

$$f: M \to \mathcal{P}(M), \quad x \mapsto \{x\} \quad \text{– inj}$$

2) $\nexists$ surj. Abb. $f: M \to \mathcal{P}(M)$ (damit auch keine bij., d.h., $|M| \ne |\mathcal{P}(M)|$)

Ang.: $\exists$ surj. $f: M \to \mathcal{P}(M)$.

Def. $A := \{x \in M : x \notin \underbrace{f(x)}_{\text{Teilmenge von } M}\} \subset M$

Da f surj. ist, $\exists\, a \in M$ mit $f(a) = A$

<u>Fall 1:</u> $a \in A$. Dann gilt nach Def. von A:

$a \notin f(a) = A$, also $a \notin A$ $\lightning$

<u>Fall 2:</u> $a \notin A$. Nach Def. von A muss

$a \in f(a) = A$ gelten, d.h., $a \in A$ $\lightning$

$\lightning$ $\blacksquare$

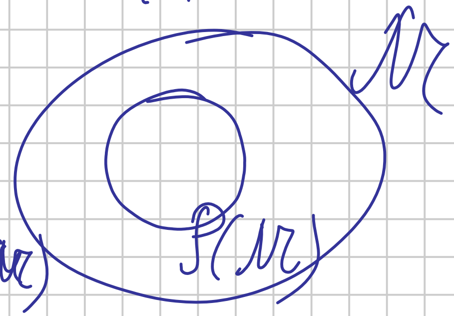
Cantorsches Paradoxon / Cantorsche Antinomie 2.12

Cantor, 1899!

Es gibt keine Allmenge (= Menge aller Mengen)

<u>Beweis</u> Ang., $\exists\, \mathcal{M} := \{ M : M \text{ Menge} \}$ - eine Menge.

Da $\mathcal{M}$ eine Menge ist, gilt $\mathcal{M} \in \mathcal{M}$ und auch $\mathcal{P}(\mathcal{M}) \subset \mathcal{M}$ (warum?)



Def. $f : \mathcal{M} \to \mathcal{P}(\mathcal{M})$ durch

$$f(x) := \begin{cases} x, & \text{wenn } x \in \mathcal{P}(\mathcal{M}) \\ \emptyset & \text{sonst.} \end{cases}$$

$\in \mathcal{P}(\mathcal{M})$

f ist surj., da $\mathcal{P}(\mathcal{M}) \subset \mathcal{M}$ $\lightning$ (Satz von Cantor 2.11) $\blacksquare$

<u>Bem.</u> Nicht alle Objekte kann man also zu einer Menge zusammenfassen. $\mathcal{M}$ aus dem Beweis

nennt man eine „Klasse" statt Menge (also: Allklasse) in der „modernen" Mengentheorie.

Das Auswahlaxiom 2.13 (Zermelo 1904)

Formulierung: Jede Familie $(M_\alpha)_{\alpha \in I}$ von Mengen (wobei I eine beliebige Indexmenge) besitzt eine Auswahlabbildung, d.h.,

$$\exists f : I \longrightarrow \bigcup_{\alpha \in I} M_\alpha \text{ mit } f(\alpha) \in M_\alpha \quad \forall \alpha \in I.$$

(d.h., man kann „gleichzeitig" aus $\forall M_\alpha$ ein Element $f(\alpha) \in M_\alpha$ auswählen.)

<u>Bem.</u> 1) Wenn $|I| < \infty$, dann klar möglich!

2) Manchmal auch für $|I| = \infty$ möglich:

Wenn z.B. $\forall M_\alpha$ aus natürlichen Zahlen besteht, wähle $f(\alpha) :=$ das kleinste Element.

3) Geschichte:

- Gödel 1938: kein Widerspruch zu Zermelo-Fraenkel Axiomen!
- Cohen 1963: Auch nicht-~~A~~ Axiom führt zu keinem Widerspruch!

D.h.: unabh. von anderen Axiomen $\Rightarrow$ ein weiteres Axiom.

Überwiegende Mehrheit von Mathematikern nehmen das A'Axiom an.

4) A'Axiom sagt nicht, wie f aussieht.

5) A'Axiom braucht man für die (schnelle) Def. des Produktes von beliebig vielen Mengen:

Erinnere: $\prod_{\alpha \in I} M_\alpha = \{ (x_\alpha)_{\alpha \in I} : x_\alpha \in M_\alpha \ \forall \alpha \}$

$= \{$ alle Auswahlabb. $\alpha \mapsto x_\alpha \in M_\alpha \}$

6) $\exists$ viele äquivalente Aussagen zum A'Axiom, z.B.:

$\forall A, B$ Mengen gilt $|A| \leq |B|$ oder $|B| \leq |A|$

Def. 2.14 Seien A, B Mengen und $R \subset A \times B$.
Dann heißt R eine <u>Relation</u> zwischen A und B.
Man sagt: „a steht in Relation zu b" (schreibe aRb), wenn $(a,b) \in R$.
Wenn $A = B$, heißt R <u>Relation auf A</u> (<u>in A</u>)

Bsp

1) $A = B = \{\text{Menschen}\}$, Def. R durch:
$(a,b) \in R \overset{\text{Def.}}{\iff} a$ und b kennen sich.

2) $A = B = \{\text{Internetseiten}\}$,
$aRb \overset{\text{Def.}}{\iff} a$ verlinkt b.

3) $A = \{1, 2, 3, \dots\} = B$, $aRb \overset{\text{Def}}{\iff} a \mid b$

4) Sei $f: A \to B$. Dann ist der Graph von f

$$\{(x, f(x)) : x \in A\} \subset A \times B$$

eine Relation. Umgekehrt: Eine Relation R ist genau dann der Graph einer Abb., wenn $\forall x_{\in A}\ \exists!\, y_{\in B}$ mit xRy.

$\boxed{\text{Def. 2.15}}$ Sei R eine Relation auf einer Menge M.

R heißt:

- reflexiv, wenn $\forall x \in M \quad xRx$,
- symmetrisch, wenn $\forall x, y \in M$
  $$xRy \Rightarrow yRx$$

- antisymmetrisch, wenn $\forall x, y \in M$:

  $$xRy \text{ und } yRx \Rightarrow x = y$$

- transitiv, wenn $\forall x, y, z \in M$

  $$xRy,\ yRz \Rightarrow xRz$$

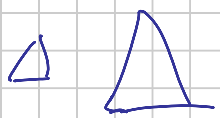
Bsp Oben: 1) refl., symm., nicht trans., nicht antisymm.
2) keine der Eigensch..
3) refl., antisymm., transitiv.

Def. 2.16 Eine Relation R auf M heißt Äquivalenzrelation, wenn R refl., symmetrisch und transitiv ist. Man schreibt $a \sim_R b$ oder $a \sim b$ für aRb.

$a \sim a$
$a \sim b \Rightarrow b \sim a$

$a \sim b,\ b \sim c \Rightarrow a \sim c$.

Bsp 1) $M = \{\text{Dreiecke}\}$, $a \sim b \overset{\text{Def}}{\Longleftrightarrow}$ a und b ähnlich



– Ä' Rel.

2) $M = \{1, 2, 3, \dots\}$, $a \sim b \overset{\text{Def}}{\Longleftrightarrow} 2 \mid a - b$

– a und b heißen **kongruent modulo 2**

3) M beliebige Menge,

$\sim$ auf $\mathcal{P}(M)$:

$$A \sim B \overset{\text{Def}}{\Longleftrightarrow} |A| = |B|$$

- $A \sim A$: nimm $f: A \to A$, $x \mapsto x$ – Identität oder identische Abb.
- $A \sim B \Rightarrow B \sim A$: nimm $f^{-1}: B \to A$

- $A \sim B,\ B \sim C \Rightarrow A \sim C$:
  $f: A \to B,\ g: B \to C$ bij $\Rightarrow g \circ f: A \to C$ bij

$\boxed{\text{Def. 2.17}}$ Sei R eine Ä'Relation auf M. Für $x \in M$ heißt

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

die Äquivalenzklasse von x. $\forall$ Element einer Ä'Klasse heißt Repräsentant oder Vertreter der Ä'Klasse.

Es gilt:

$$[a] = [b] \Leftrightarrow a \sim b \Leftrightarrow b \in [a] \Leftrightarrow a \in [b].$$

Def. von $[\cdot]$

Warum? (Trans. + Symm.)

Symm.

Ü

Man schreibt auch $a/\sim$ oder $[a]_\sim$.

Bsp $\mathbb{N} := \{1, 2, 3, \dots\}$, $a \sim b :\overset{\text{Def}}{\Longleftrightarrow}$ kongruent mod. 2 $\;(2 \mid (a-b))$

Äq'klassen sind $\{1, 3, 5, \dots\}$ und $\{2, 4, 6, \dots\}$.

Def. 2.18 Die Menge der Ä'klassen bzgl. einer Ä'Relation $\sim$ auf M bezeichnet man mit $M/\sim$ „M modulo $\sim$"

Die Abb. $f: M \to M/\sim$, $x \mapsto [x]$

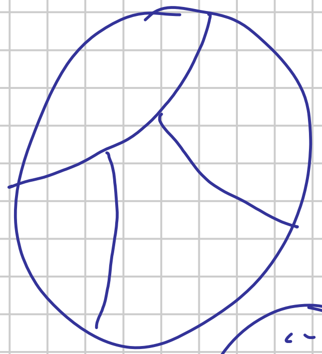
heißt Quotientenabbildung

Bsp $M := \{\text{Menschen}\}$, $a \sim b :\overset{\text{Def}}{\Longleftrightarrow}$ gleiches Geburtsjahr.

Dann ist $f(a) = [a] = \{$ Menschen mit demselben Geburtsjahr wie a $\}$

Def. 2.19 Sei M eine Menge und $\mathcal{P} \subset \mathcal{P}(M)$. Dann heißt $\mathcal{P}$ eine Partition (oder: (disjunkte) Zerlegung) von M, wenn:

- $\bigcup_{A \in \mathcal{P}} A = M$
- $\forall A, B \in \mathcal{P}$ gilt: $A = B$ oder $A \cap B = \emptyset$ (die Teilmengen sind paarweise disjunkt)



Ü 1) $\forall$ Ä'Rel. auf M bilden die Ä'Klassen eine Partition von M. Insbesondere sind sie paarweise disjunkt.

2) $\forall$ Partition $\mathcal{P}$ von M $\exists!$ „Ä" Rel. $\sim$ auf M mit $\mathcal{P} = M/\sim$.

(Def. $x \sim y \overset{\text{Def.}}{\Leftrightarrow} \exists A \in \mathcal{P}: x \in A, y \in A.$)

$\boxed{\text{Bsp}}$ $\mathbb{N}$: $1, 2, 3, 4, 5, 6, \ldots$ – Partition:

$\mathcal{P} = M/\sim = \{[1], [2]\}$

$\boxed{\text{Def. 2.20}}$ Eine Relation auf einer Menge heißt **Partielle Ordnung** (oder: **Halbordnung**, **Teilordnung**), wenn sie reflexiv, antysymmetrisch und transitiv ist.

Wir schreiben oft $\preccurlyeq$ statt R und $a \preccurlyeq b$ statt aRb.

Außerdem schreibe $a \succsim b$, wenn $b \precsim a$,

$a \prec b$, wenn $a \precsim b$ und $a \neq b$

$a \succ b$, wenn $b \prec a$.

Eine partielle Ordnung $\precsim$ heißt Ordnung (oder: totale / lineare Ordnung), wenn dazu noch gilt:

$$\forall a, b \in M \quad (a \precsim b \text{ oder } b \precsim a) \quad \text{(Totalität)}$$

Die Menge M heißt dabei partiell bzw. total geordnet.

$\boxed{\text{Bsp}}$ 1) $\mathbb{N} = \{1, 2, 3, \dots\}$ mit $\leq$. Aber auch $\geq$

– beides totale Ordnung.

2) $\mathbb{N}$, $a \precsim b \overset{\text{Def}}{\Longleftrightarrow} a : b$

$a \vdots a$ ✓

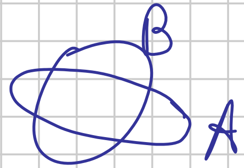
$a \vdots b,\ b \vdots a \implies a = b$ ✓ — part. Ordnung

$a \vdots b,\ b \vdots c \implies a \vdots c$ ✓ nicht total!

3) Sei M eine Menge. Dann ist $\mathcal{P}(M)$ part. geordnet durch

$$A \leq B \overset{\text{Def}}{\iff} A \subset B$$

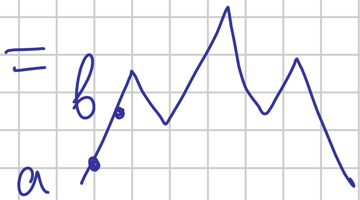
Achtung: nicht total geordn. i. A.:



Aber auch „$\supset$"

Ü 4) Im Allg. gilt: $\leq$ part. (totale) Ordnung

$\iff \geq$ part. (totale) Ordnung.

5) $M :=$ 

$a \precsim b \overset{\text{Def.}}{\Longleftrightarrow}$ (a und b liegen auf einer strecke) und (b liegt höher als a oder gleich hoch)

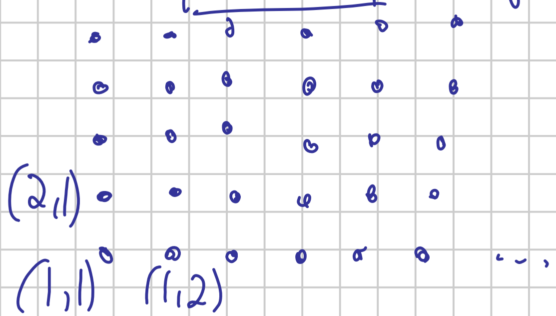
– partielle, keine totale Ordnung.

$\boxed{\text{Bem.}}$ Sei $\precsim$ eine totale Ordnung. Dann gilt $\forall a, b$:

entweder $a \prec b$, oder $b \prec a$, oder $a = b$

(Trichotomie – Warum?)

$\boxed{\text{Bem.}}$ Auf $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ $\exists$ mehrere natürliche (Halb)Ordnungen:



1) $(n_1, n_2) \precsim (m_1, m_2)$, wenn $n_1 \leq m_1$, $n_2 \leq m_2$

– part. Ordnung, nicht total

2) $(n_1, n_2) \preceq (m_1, m_2)$, wenn
$(n_1 < m_1)$ oder $(n_1 = m_1$ und $n_2 \leq m_2)$.
– lexikographische Ordnung (total): Ü

Dasselbe auch für $\mathbb{N}^d$.

$\boxed{\text{Def. 2.21}}$ Sei $\preceq$ eine part. Ordnung auf M. Dann heißt ~~$m \in M$~~ ein Element:

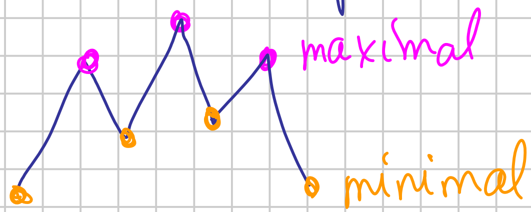
- maximal, wenn $\forall a \in M$
  $m \preceq a \Rightarrow m = a$
- das größte Element, wenn $\forall a \in M$ $a \preceq m$
- minimal, wenn $\forall a \in M$
  $a \preceq m \Rightarrow m = a$

- das <u>kleinste Element</u>, wenn $\forall a \in M$ $m \preceq a$.

<u>Bem.</u> 1) Das größte Element $\Rightarrow$ maximal
($\forall a \in M$ $m \succeq a$ und $\underbrace{a \succeq m}_{m \text{ größtes El.}} \Rightarrow a = m$)

–"– kleinste –"– $\Rightarrow$ minimal (warum?)

2) Die Umkehrung gilt i. A. nicht:

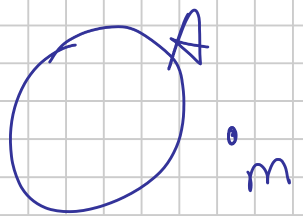
<u>Bsp</u>: 

$\nexists$ größtes, kleinstes Element!

Hörsaalübung (Achtung: für totale Ordnungen gilt maximal $\Leftrightarrow$ das größte El.
minimal $\Leftrightarrow$ das kleinste El
(Warum?)

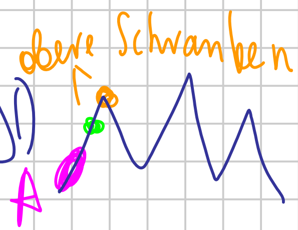
3) Max. und minimale Elemente sind i. A. nicht eindeutig, das größte und das kleinste El. aber schon.

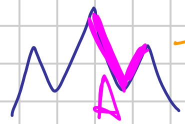
$\boxed{\text{Def. 2.22}}$ Sei $\preceq$ eine part. Ordnung auf M, $A \subset M$ und $m \in M$. Dann heißt m eine obere (bzw. untere) Schranke für A, wenn



$$\forall a \in A \quad a \preceq m \quad (\text{bzw. } m \preceq a)$$

$\boxed{\text{Bsp}}$ 1)





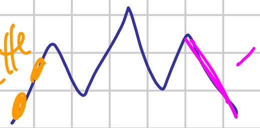
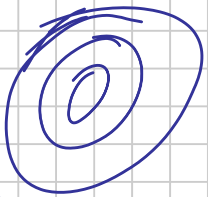
– $\nexists$ obere Schranke.

2) $M = [0, 2] := \{x : 0 \leq x \leq 2\}$,

$A = (0, 1) := \{x : 0 < x < 1\}$ – $\forall$ obere Schranke liegt nicht in A.

3) $\mathcal{P}(M)$ mit „$\subset$". M ist eine obere Schranke
und $\emptyset$ –„– untere –„– $\forall A \subset \mathcal{P}(M)$

$\boxed{\text{Def. 2.23}}$ Sei $(M, \preceq)$ wie oben. Dann heißt $A \subset M$ eine Kette, wenn A total geordnet bzgl. $\preceq$ ist, d.h.,
$\forall a, b \in A$ $(a \preceq b$ oder $b \preceq a)$.

$\boxed{\text{Bsp}}$ 1) Kette  -Kette 2) $(\mathcal{P}(M), \subset)$: 

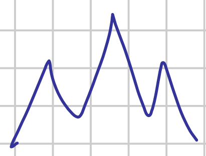
Bem. Es sind äquivalent (ohne Beweis)

(i) A' Axiom

(ii) Wohlordnungssatz: $\forall$ Menge M $\exists$ totale Ordnung auf M s.d. $\forall A \subset M, A \neq \emptyset$ ein kleinstes

Element hat. (wie $\mathbb{N}, \leq$)

(iii) Lemma von Zorn: Sei $\preceq$ eine part. Ordnung auf einer Menge M s.d. $\forall$ Kette eine obere Schranke besitzt. Dann hat M ein (mindestens) maximales Element.



Bem. Ä'Relationen verallgemeinern „="
Ordnungsrelationen —"— „$\leq$" bzw. „$\geq$"

3. Natürliche Zahlen und Induktion, ganze und rationale Zahlen.

Bezeichnung: $\mathbb{N} := \{1, 2, 3, \dots\}$ – die Menge der natürlichen Zahlen

$$\mathbb{N}_0 := \{0, 1, 2, 3, \dots\}$$

(Achtung: in manchen Büchern: $0 \in \mathbb{N}$)

Bem. $\mathbb{N}$ ist durch den Anfang 1 und die Operation „+1" eindeutig bestimmt: $2 = 1+1$ (Nachfolger von 1)

$3 = 2+1 = 1+1+1$ (– " – 2)

$$1 \xrightarrow{+1} 2 \xrightarrow{+1} 3 \xrightarrow{+1} 4 \dots$$

Daraus ergibt sich:

Beweismethode: (vollständige) Induktion

Sei $n_0 \in \mathbb{N}_0$. Wie zeigt man Aussagen $A(n)$ $\forall\, n \geq n_0$?

Es reicht z.z. – zu zeigen:

Induktionsanfang (IA) 1) $A(n_0)$

Induktionsschritt (IS) 2) $\underbrace{A(n)}_{\text{Induktionsvoraus. (IV)}} \Longrightarrow A(n+1) \quad \forall n \geq n_0$.

(oder: 2^*) $A(n_0), \ldots, A(n) \Longrightarrow A(n+1)$)

und

$\boxed{\text{Bsp}}$ $\forall n \in \mathbb{N}$ gilt: $1+2+\ldots+n \overset{?}{=} \frac{n(n+1)}{2}$

Beweis Vollst. Induktion nach n:

IA: $n=1$: $1 = \frac{1(1+1)}{2}$ ✓

IS: $(n \to n+1)$

Ang.: $1+2+\dots+n = \frac{n(n+1)}{2}$; (IV)

z.z.: $1+2+\dots+(n+1) = \frac{(n+1)(n+2)}{2}$

Es gilt:

$$\underbrace{1+\dots+n}_{= \frac{n(n+1)}{2} \text{ nach IV}} + (n+1) = \frac{n(n+1)}{2} + (n+1)$$

$$= \frac{(n+1)}{2}(n+2) \checkmark$$

$\blacksquare$

$\boxed{\text{Bsp}}$ $\forall n \in \mathbb{N}$ gilt $|\mathcal{P}(\{1,\dots,n\})| = 2^n$.

<u>Beweis</u> Vollst. induktion nach n.

- IA: $n=1$: $|\mathcal{P}(\{1\})| = |\{\emptyset, \{1\}\}| = 2$ ✓
- IS: $n \rightsquigarrow n+1$:

  Ang.: die Aussage stimmt für n. (IV)

Wir haben:

$$\mathcal{P}(\{1,\dots,n,n+1\}) = \underbrace{\mathcal{P}(\{1,\dots,n\})}_{\text{hat } 2^n \text{ Elemente nach IV}} \,\dot{\cup}\, \underbrace{\{A \subset \{1,\dots,n+1\} \mid n+1 \in A\}}_{\text{—"— da so ein } A = A_1 \,\dot{\cup}\, \{n+1\},\ A_1 \subseteq \{1,\dots,n\} \text{ beliebig}}$$

disjunkte Vereinigung

→ hat insgesamt $2^n + 2^n = 2^{n+1}$. ✓ $\blacksquare$

Induktive Definitionen

Sei M eine Menge und $n_0 \in \mathbb{N}_0$. Def. Elemente $a(n) \in M$ für alle $n \geq n_0$ wie folgt:

- Def. $A(n_0)$
- Für $n \geq n_0$ gib eine Vorschrift an, wie man $a(n+1)$ aus $a(n_0), \dots, a(n)$ bekommt/berechnet

Bsp 1) <u>Fakultät</u>

- $0! := 1$
- $(n+1)! := (n+1) \cdot n!$

Es gilt also: $n! = n \cdot (n-1)! = n(n-1)(n-2)! = \ldots = n \cdot (n-1) \cdot \ldots \cdot 1$

2) <u>Endliche Summen und Produkte</u>

Für reelle Zahlen $a_1, a_2, \ldots$ def.

$$\sum_{k=1}^{n} a_k := a_1 + \ldots + a_n \quad \text{und} \quad \prod_{k=1}^{n} a_k := a_1 \cdot \ldots \cdot a_n$$

wie folgt:

- $\sum_{k=1}^{1} a_k := a_1$
- $\sum_{k=1}^{n+1} a_k := \sum_{k=1}^{n} a_k + a_{n+1}$

Analog: $\prod_{k=1}^{n}$, $\sum_{k=n}^{m}$ und $\prod_{k=n}^{m}$ für $m \geq n$ (z.B. $\sum_{k=17}^{100} a_k$)

Bis jetzt haben wir nur die Operation „+1" verwendet.

Es gibt auf $\mathbb{N}$ bzw. $\mathbb{N}_0$ die Operationen

$$+ , \cdot , \underbrace{\div \text{ mit Rest}}_{\text{nur auf } \mathbb{N}}$$

und die (totale) Ordnung $\leq$

Die Verknüpfungen $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ und $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ „respektieren" einander und die Ordnung $\leq$: Es gelten

$$\left.\begin{aligned} &\bullet\ (a+b)\cdot c = a\cdot c + b\cdot c \\ &\bullet\ c\,(a+b) = c\cdot a + c\cdot b \end{aligned}\right\} \ \underline{\text{Distributivgesetze}}$$

$\forall a, b, c$

- $a \le b \Rightarrow a+c \le b+c \quad \forall a,b,c$

Außerdem bildet $(\mathbb{N}, +)$ eine <u>kommutative Halbgruppe</u>, d.h., erfüllt:

- $(a+b)+c = a+(b+c) \quad \forall a,b,c$ – <u>Assoziativgesetz</u>
- $a+b = b+a \quad \forall a,b$ – <u>Kommutativität</u>.

Auch $(\mathbb{N}, \cdot)$, $(\mathbb{N}_0, +)$, $(\mathbb{N}_0, \cdot)$ sind komm. Halbgruppen.

<u>Bem.</u> Dabei hat $(\mathbb{N}_0, +)$ ein <u>neutrales Element</u> 0:

- $a+0 = 0+a = a \quad \forall a$

Analog: $(\mathbb{N}, \cdot)$ und 1.
Aber: $(\mathbb{N}, +)$ hat kein neutr. Element.

und: $(\mathbb{N},+)$ und $(\mathbb{N}_0,+)$ sind keine Gruppen

(Gruppe = Halbgruppe mit der Eigenschaft

$\forall a \ \exists x$ mit $a+x=x+a=0$

(x heißt das inverse Element zu a, ist eindeutig und wird mit $(-a)$ bezeichnet.))

Die Gleichung $x+1=0$ ist in $\mathbb{N}_0$ nicht lösbar

Def. $\mathbb{Z} := \{\ldots,-2,-1,0,1,2,\ldots\}$ – Menge der ganzen Zahlen

Darauf haben wir Verknüpfungen $+, \circ, - : \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$

(def. $a-b := a+(-b)$, wobei $-b$ das inverse Element zu b bzgl. $+$ ist)

und „$\leq$"

$(\mathbb{Z},+)$ ist eine Gruppe : $x+a=0$ ist lösbar $\forall a$.

Aber $(\mathbb{Z},\cdot)$ ist keine Gruppe, auch $(\mathbb{Z}\setminus\{0\},\cdot)$ keine Gruppe

$ax=1$ ist nur für $a=\pm 1$ lösbar

Def. $\mathbb{Q} := \left\{ \frac{p}{q} : p\in\mathbb{Z},\ q\in\mathbb{N} \right\}$

$= \left\{ \frac{p}{q} : \text{—"—},\ \underbrace{(p,q)}_{ggT(p,q)}=1 \right\}$

Hörsaalübung: inkl. Def. von $+,\cdot,\leq$

Man kann $\mathbb{Q}$ als $\mathbb{Z}\times\mathbb{N}/\sim$ für die Ä'Rel. $\sim$ def. durch

$$(p_1,q_1)\sim(p_2,q_2) \overset{\text{Def}}{\Longleftrightarrow} p_1\cdot q_2 = q_1\cdot p_2$$

$\mathbb{Q}$ ist ein Körper, d.h., erfüllt:

- $(\mathbb{Q},+)$ komm. Gruppe
- $(\mathbb{Q}\setminus\{0\},\cdot)$ komm. Gruppe
- Distributivgesetze von oben

Aber: z.B. die Gleichung $x^2=2$ ist in $\mathbb{Q}$ nicht lösbar.

4. Reelle Zahlen und Vollständigkeit

Bezeichne: $\mathbb{R} := \{\text{reelle Zahlen}\}$ – Menge der reellen Zahlen

$\mathbb{R}_+ := [0,\infty) := \{x\in\mathbb{R} : x \geq 0\}$ – Menge der pos. reellen Zahlen

$\mathbb{R}_- := (-\infty,0] := \{x\in\mathbb{R} : x\leq 0\}$ – " – negat. – " –

$[a,b] := \{x \in \mathbb{R} : a \leq x \leq b\}$ – das abgeschlossene Intervall a, b,

$(a,b) := \{x \in \mathbb{R} : a < x < b\}$ – das offene Intervall

$\left.\begin{array}{l} (a,b] := \{x \in \mathbb{R} : a < x \leq b\} \\ [a,b) := \{ \quad " \quad : a \leq x < b\} \end{array}\right\}$ halboffene Intervalle

für $a \leq b$, $a, b \in \mathbb{R}$

Manche Bücher benutzen $]a,b[$ statt (a,b) bzw. $]a,b]$ statt $(a,b]$ usw.

$\exists$ mehrere Def. / Konstruktionen der reellen Zahlen – kommt später.

Zuerst: $\xrightarrow[0]{\hspace{3cm}} \mathbb{R}$ $\mathbb{R}$ besitzt Verknüpfungen: $+$, $\cdot$ und die Ordnung $\leq$.

$(\mathbb{R}, +, \cdot)$ ist auch ein Körper (wie $\mathbb{Q}$)

Aus den Körperaxiomen folgen Rechenregeln:

Hörsaalübung

$$0 \cdot a = a \cdot 0 = 0$$

$$(-1) \cdot a = -a$$

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

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

$$a \cdot b = 0 \Rightarrow (a = 0 \text{ oder } b = 0),$$

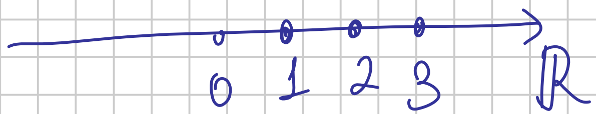
wobei $(-a)$ das inverse Element zu a bzgl. $+$ ist, d.h., x mit $a + x = 0$.

Außerdem ist $\mathbb{R}$ ein <u>geordneter Körper</u> (wie $\mathbb{Q}$); d.h., die totale Ordnung $\leq$ „respektiert" $+$ und $\cdot$:

$$\left.\begin{array}{ll} (O1) & a \leq b \Rightarrow a + c \leq b + c \\ (O2) & (a \geq 0 \text{ und } b \geq 0) \Rightarrow a \cdot b \geq 0. \end{array}\right\} \forall a, b, c$$

Daraus folgen:
- $(a \geq 0$ und $b \geq 0) \Rightarrow a + b \geq 0$ (Warum?)
- $a \leq b,\ c \geq 0 \Rightarrow ac \leq bc$ – (Hörsaalübung)

Außerdem gilt
(O3) $\forall a \in \mathbb{R}\ \exists n \in \mathbb{N}$ mit $n > a$.
Archimedisches Axiom



Bem. (O3) impliziert:
$$\forall x \in \mathbb{R}\ \exists!\ n \in \mathbb{Z} \text{ mit } x \in [n, n+1).$$ Ü

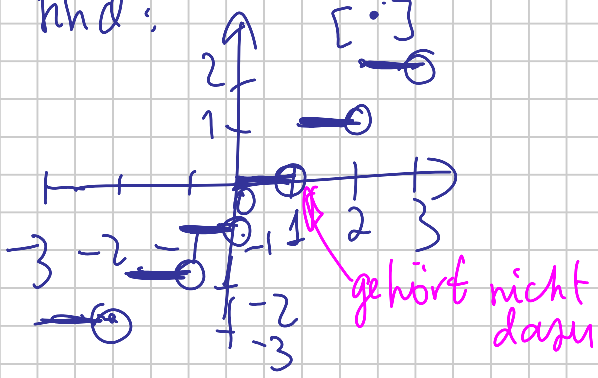
Die Zahl $x - n \in [0,1)$ heißt der Bruchteil von x (schreibe $\{x\}$) und dieses n heißt Ganzteil von x (schreibe $[x]$ oder $\lfloor x \rfloor$)
Gaußklammer

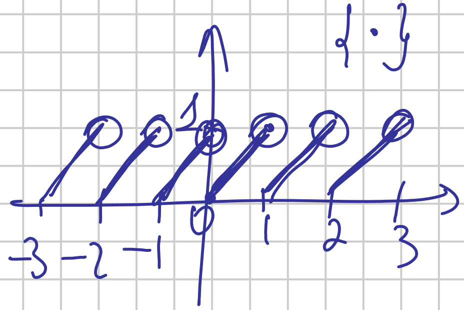
$\boxed{\text{Bsp}}$ $[1{,}6] = 1$ $\quad [-1{,}6] = -2$

$\{1{,}6\} = 0{,}6$ $\quad \{-1{,}6\} = 0{,}4$

$[\cdot]$ und $\{\cdot\}$ sind Funktionen $: \mathbb{R} \to \mathbb{R}$

Graphen sind:

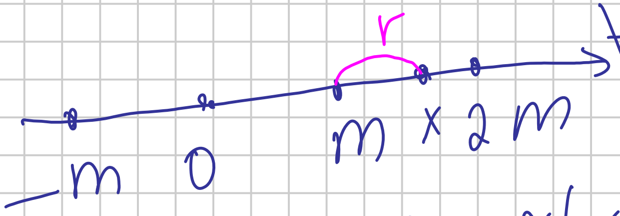




$[x] + \{x\} = x$

Analog: Division mit Rest:

Sei $m \in \mathbb{N}$. Dann gilt (Warum?)



$\forall x \in \mathbb{R} \ \exists! \, n \in \mathbb{Z} \ \exists! \, r \in [0, m)$ mit $x = n \cdot m + r$

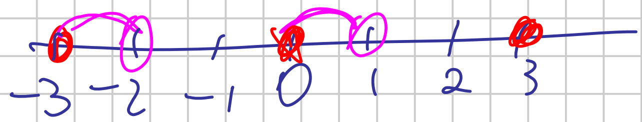
Wir schreiben $x = r \mod m$

Insbesondere gilt $x = \{x\} \mod 1$

Wir schreiben $a = b \mod m$, wenn $a - b = n \cdot m$ für ein $n \in \mathbb{Z}$, d.h., $m \mid a - b$.

(für beliebige $a, b \in \mathbb{R}$)

$\boxed{\text{Bsp}}$ $-2 = 1 \mod 3$



$\boxed{\text{Lemma 4.1}}$ (Bernoullische Ungleichung)

$\forall x \in \mathbb{R}$ mit $x > -1$, $x \neq 0$ und $\forall n \in \{2, 3, \dots\}$

gilt:

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

Beweis: Ü (Induktion nach n)

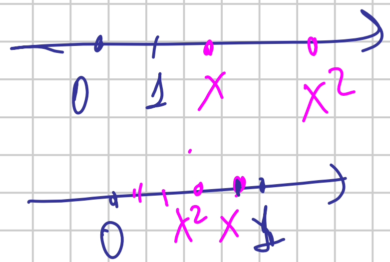
$\boxed{\text{Folgerung 4.2}}$ Sei $x > 0$.

(a) Ist $x > 1$, so gilt:

„egal, wie groß" $\forall R \in \mathbb{R} \ \exists n \in \mathbb{N}: x^n > R$

(d.h.: x^n wird beliebig groß)

(b) Ist $x < 1$, so gilt



„egal, wie klein"

$\forall \varepsilon > 0 \; \exists n \in \mathbb{N} : x^n < \varepsilon$

(d.h., x^n wird beliebig klein)