Operationen auf Mengen

Mengen A, B

$A \cap B$, $A \cup B$, $A \setminus B$, $A \Delta B$

$A \subseteq U : U \setminus A := \complement A = \complement_U A$

↑ Komplement

Satz (De Morgansche Regel)

Seien $A, B \subseteq U$. Dann gilt

$$\complement_U (A \cap B) = (\complement_U A) \cup (\complement_U B)$$

Beweis "$\subseteq$":

Sei $x \in \complement_U (A \cap B)$ z.z. $x \in (\complement_U A) \cup (\complement_U B)$

Dann gilt $x \in U$ und $x \notin A \cap B$

Es gilt also nicht, dass $x \in A$ und $x \in B$.

Also gilt $x \notin A$ oder $x \notin B$. so wie $\neg(A \wedge B) \equiv \neg A \vee \neg B$

1. Fall: $x \notin A$: Dann gilt $x \in \complement_U A$, also $x \in (\complement_U A) \cup (\complement_U B)$.

2. Fall: $x \notin B$: Dann gilt $x \in \complement_U B$, also $x \in (\complement_U A) \cup (\complement_U B)$.

$(A \cap B) \subseteq A$

"$\supseteq$":

Sei $x \in (\complement_U A) \cup (\complement_U B)$. z.z. $x \in \complement_U (A \cap B)$

Es gilt dann $x \in \complement_U A$ oder $x \in \complement_U B$

1. Fall: $x \in \complement_U A$: Dann gilt $x \in U$ und $x \notin A$

Da $x \notin A$, gilt auch $x \notin A \cap B$. Folglich gilt $x \in \complement_U (A \cap B)$.

2. Fall $x \in C_U B$: Dann gilt $x \in U$ und $x \in B$.
Also $x \notin A \cap B$, und somit $x \in C_U(A \cap B)$.

$\emptyset$ auch im Skript

Für jede Menge A gilt: $\emptyset \subseteq A$
Wäre $\emptyset$ keine Teilmenge von A, dann gäbe es $x \in \emptyset$ mit $x \notin A$. Da $x \in \emptyset$ falsch ist, kann es so ein x nicht geben.

$A \setminus A = \emptyset$

$A \Delta B$ siehe Skript s. 29.

Es gilt $(A \Delta B) \Delta C = A \Delta (B \Delta C)$

Beweis (2) Wann gilt $x \in (A \Delta B) \Delta C$?

$x \in (A \Delta B) \Delta C \iff (x \in A \Delta B \wedge x \notin C) \vee (x \in C \wedge x \notin A \Delta B)$

$\iff (((x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)) \wedge x \notin C) \vee$
$(x \in C \wedge (x \notin A \vee x \in B) \wedge (x \notin B \vee x \in A))$

$\iff (x \in A \wedge x \notin B \wedge x \notin C) \vee (x \in B \wedge x \notin A \wedge x \notin C)$
$\vee (((x \notin A \wedge x \in C) \vee (x \in B \wedge x \in C)) \wedge (x \notin B \vee x \in A))$
(Distributg.)

$\iff (x \in A \wedge x \notin B \wedge x \notin C) \vee (x \in B \wedge x \notin A \wedge x \notin C) \vee$
$\{(x \notin A \wedge x \in C \wedge x \notin B) \vee (x \notin A \wedge x \in C \wedge x \in A)$
$\vee (x \in B \wedge x \in C \wedge x \notin B) \vee (x \in B \wedge x \in C \wedge x \in A)$
(* Rückseite; F.A. F.A.)

$\iff (x \in A \wedge x \notin B \wedge x \notin C) \vee (x \in B \wedge x \notin A \wedge x \notin C) \vee *^2$
$\vee F \vee F \vee (x \in B \wedge x \in C \wedge x \in A)$
$*^2 \ldots \vee (x \notin A \wedge x \in C \wedge x \notin B) \ldots$

$x \in A \triangle (B \triangle C) \Leftrightarrow$ ... wir kommen auf den gl. Ausdruck

→ geht auch mit Wahrheitstafel!

Potenzmenge S. 30 unten

$P(A) = \{\{3\}, \{4\}, \{5\}, \{3,4\}, \{3,5\}, \{4,5\}, \{3,4,5\}, \emptyset\}$

Satz 3.13

$*^3$ skript : Induktionsschritt :

gehört mit skript ein!!!

Wir zeigen nun, dass für alle $n \in \mathbb{N}_0$ gilt:
Wenn $\{1,2,\dots n\}$ genau 2^n Teilmengen hat, so hat $\{1,2,\dots,n,n+1\}$ genau 2^{n+1} Teilmengen.

Sei $n \in \mathbb{N}_0$

Wir nehmen an, dass $\{1,\dots n\}$ genau 2^n Teilmengen hat.

Z.z. Die Menge $\{1,2,\dots n+1\}$ hat genau 2^{n+1} Teilmengen (*)

$P(\{1,2,\dots n,n+1\}) = \{B \mid B \subseteq \{1,\dots,n,n+1\}\}$

$= \{B \mid B \subseteq \{1,\dots,n,n+1\}$ und $n+1 \in B\} \cup$
$\{B \mid B \subseteq \{1,\dots n,n+1\}$ und $n+1 \notin B\} =$

$\{B \cup \{n+1 \mid B \in P(\{1,\dots,n\})\} \cup P(\{1,\dots,n\})$

Laut Annahme hat jede Menge 2^n Elemente.
Da diese beiden Mengen „disjunkt" sind, also leeren Schnitt haben, hat ihre Vereinigung $2^n + 2^n = 2 \cdot 2^n$
$= 2^{n+1}$ Elemente. Also ist (*) gezeigt.

Also gilt für alle $n \in \mathbb{N}_0$, dass $\{1,\dots,n\}$ genau 2^n Teilmengen hat.

Mächtigkeit einer Menge

$\{1,2,3\}$, $\emptyset$, $\mathcal{P}(\{1,2,3,4\})$ — endl. Mengen

$\mathbb{N}$, $\mathbb{R}$ — unendl.

Wenn A genau n verschiedene Elemente hat (mit $n \in \mathbb{N}_0$), so schreiben wir $|A| = n$ (oder $\#A = n$). Wenn es kein solches $n \in \mathbb{N}_0$ gibt, so schreiben wir $|A| = \infty$

Satz 3.15) Seien $A, B, A_1, \ldots$ endl. Mengen

(1) Wenn $A \cap B = \emptyset$, so gilt $|A \cup B| = |A| + |B|$

(2) Wenn für alle $i,j \in \{1,\ldots,n\}$ mit $i \neq j$ gilt, dass $A_i \cap A_j = \emptyset$, so gilt $|A_1 \cup \ldots \cup A_n| = |A_1| + |A_2| + \ldots + |A_n|$

(3) $|A \cup B| = |A| + |B| - |A \cap B|$

Wir beweisen (3) (siehe Skript)

Da $A \setminus B$ disjunkt, gilt

$$|A \cup B| = |(A \setminus B) \cup B| = |A \setminus B| + |B|$$

Außerdem gilt

$$|A| = |(A \setminus B) \cup (A \cap B)| \overset{\text{disj.}}{=} |A \setminus B| + |A \cap B|$$

Also: $|A \cup B| = |A| - |A \cap B| + |B|$

FRAGESTUNDE 24.10.

2.12) 6)

stimmt, weil bei oder nur eines stimmen muss

$p: \exists x \in \mathbb{R} : A(x) \vee B(x)$ $\quad q = (\exists x \in \mathbb{R} : A(x)) \vee (\exists x \in \mathbb{R} : B(x))$

1) • "$\Leftarrow$" Ann. q gilt

1.1) Annahme: $a \in \mathbb{R}$, sodass $A(a)$ gilt

Daher gilt q (Da wir eine Aussage haben)

p gilt, da $a \in \mathbb{R}$, sodass $A(a)$ gilt

1.2) analog für B

"$\Rightarrow$" Ann.: p gilt. Daher ~~gilt~~ gibt es $a \in \mathbb{R}$, sodass $A(a)$ oder $B(a)$ gilt.

Ann: $A(a)$ gilt, dann gilt q.

Ann: $B(a)$ gilt. Dann gilt q.

7) $\nexists \to \forall$

"$\Rightarrow$": Sei $a \in \mathbb{R}$. Dann gilt $A(a)$ oder $B(a)$.

Annahme

7) $\forall x \in \mathbb{N} : (\text{"}x \text{ ist gerade"} \vee \text{"}x \text{ ist ungerade"})$

$(\forall x \in \mathbb{N} : \text{"}x \text{ ist g."}) \vee (\overset{\forall x \in \mathbb{N}:}{\text{"}x \text{ ist ungerade"}})$

Gegenbsp

Beweis fertig

Diskrete Mathe vo

13.11.

Vereinigungen

$$\bigcup \{\{1,2,3\},\{3,4,5\}\} = \{1,2,3,4,5\}$$

Def: Sei $\mathcal{A}$ eine Menge, deren Elemente alle Mengen sind. Mit $\bigcup \mathcal{A}$ oder $\bigcup_{A \in \mathcal{A}} A$ bezeichnen wir die Menge

$$\{x \mid \exists A \in \mathcal{A} : x \in A\}$$

Bsp: siehe Skript S. 32

$$\bigcap_{A \in \mathcal{A}} A = \bigcap \mathcal{A} = \{x \mid \forall A \in \mathcal{A} : x \in A\}$$

$\bigcap \mathcal{A}$ ist nur def., wenn $\mathcal{A} \neq \emptyset$.

$$\bigcup \emptyset = \emptyset$$
$$\bigcup \{\emptyset\} = \emptyset$$

evtl. sinnlos nicht schreiben:

$$\bigcup \{A\} = A$$
$$\bigcup_{x \in A} \{x\} = A$$

geordnete Paare:

$$\mathbb{R} \underset{\text{kreuz}}{\times} \mathbb{R} = \{(x,y) \mid x \in \mathbb{R} \text{ und } y \in \mathbb{R}\}$$

kartesischen Koord.

$$A \times B = \{(a,b) \mid a \in A \text{ und } b \in B\}$$

$$(1,-3) \neq (-3,1)$$
$$\{1,-3\} = \{-3,1\}$$

geordnete Paare siehe S. 33

$(a,b) = \{\{a\}, \{a,b\}\} = \{\{b,a\}, \{a\}\}$

$(1,-3) = \{\{1\}, \{1,-3\}\}$

$(-3,1) = \{\{-3\}, \{-3,1\}\}$

$(2,2) = \{\{2\}, \{2,2\}\} = \{\{2\}\{2\}\} = \{\{2\}\}$

Satz 3.2.1.

Für alle a,b,c,d gilt : $(a,b) = (c,d) \Leftrightarrow a=c \wedge b=d$

z.z. $\{\{a\}, \{a,b\}\} = \{\{c\}, \{c,d\}\} \Leftrightarrow a=c \wedge b=d$

"$\Leftarrow$" : Annahme : $a=c \wedge b=d$

z.z. $\{\{a\}, \{a,b\}\} = \{\{c\}, \{c,d\}\}$

Sei $x \in \{\{a\}, \{a,b\}\}$, so gilt $x \in \{a\}$ oder $x \in \{a,b\}$

1. Fall $x = \{a\}$: Da $a=c$ gilt $x = \{c\}$ & somit $x \in \{\{c\}, \{c,d\}\}$

2. Fall ⋮

$\{\{a\}\{a,b\}\} = \{\{c\}\{c,d\}\}$ wenn $a=c$ & $b=d$ offensichtl. gleich

"$\Rightarrow$" Annahme : $\{\{a\}, \{a,b\}\} = \{\{c\}, \{c,d\}\}$

z.z. $a=c$ & $b=d$

1. Fall $a \neq b$: Da $\{c\} \in \{\{a\}, \{a,b\}\}$, gilt $\{c\} = \{a\}$ oder $\{c\} = \{a,b\}$.

Wegen $a \neq b$ gilt $\{a\} = \{c\}$ Da $a \in \{a\}$, gilt $a \in \{c\}$, und somit $a=c$.

Also gilt $\{\{a\},\{a,b\}\} = \{\{a\},\{a,d\}\}$
Somit gilt $\{a,b\} = \{a\}$ oder $\{a,b\} = \{a,d\}$
Da $a \neq b$, gilt $\{a\} \neq \{a,b\}$. Also gilt
$\{a,b\} = \{a,d\}$. Somit gilt $b \in \{a,d\}$.
Da $b \neq a$ gilt $b = d$.

2. Fall: $a = b$: Dann gilt $\{\{a\}\} = \{\{c\},\{c,d\}\}$
Somit $\{c,d\} = \{a\}$, & somit $c = d = a$
Somit $a = c$ & $b = d$.
↑ weil Fallannahme

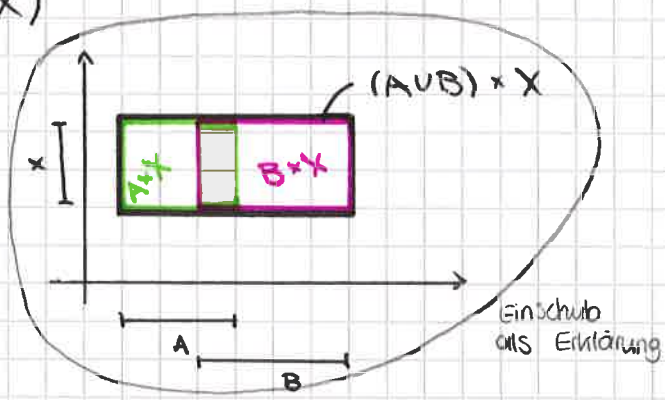
∎

$A \times B := \{(a,b) \mid a \in A \text{ und } b \in B\}$

ReRe siehe S. 34

Beweis 1) Sei $x \in (A \cup B) \times X$. Dann gibt es
$u \in A \cup B$ und $v \in X$, sodass $x = (u,v)$.
Es gibt also: $u \in A$ oder $u \in B$
1. Fall: $u \in A$: Dann gilt $(u,v) \in A \times X$, also
$(u,v) \in (A \times X) \cup (B \times X)$

2. Fall: $u \in B$: .... (analog)



Wir zeigen nun $(A \times X) \cup (B \times X) \subseteq (A \cup B) \times X$

Sei $e \in (A \times X) \cup (B \times X)$

z.z. $e \in (A \cup B) \times X$

Da $e \in (A \times X) \cup (B \times X)$, gilt $e \in A \times X$ oder $e \in B \times X$

1. Fall: $e \in A \times X$: Dann gibt es $a \in A$ und $x \in X$, sodass $e = (a, x)$.
Da $a \in A$, gilt $a \in A \cup B$. Somit gilt $e = (a, x) \in (A \cup B) \times X$

2. Fall: $e \in B \times X$: Dann gibt es $b \in B$ und $x \in X$, sodass $e = (b, x)$
(nicht anders gl. x wie Fall 1)
Da $b \in B$, gilt $b \in A \cup B$. Somit $(b, x) \in (A \cup B) \times X$

■

Teil 2 Kapitel 4

$\mathbb{N}$

$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$

$\mathbb{N}_0 = \{0, 1, 2, 3, 4, \ldots\}$

Axiome über $\mathbb{N}$ siehe Skript 4.1. S. 36

(2) (Für jede Zahl a ist $a+1$ der Nachfolger von a)

$a + 1 = a^+$

(9) $1 \in \mathbb{N}$

$\forall a \in \mathbb{N} \cdot a^+ \in \mathbb{N}$

$\forall a, b \in \mathbb{N} : a^+ = b^+ \Leftrightarrow a = b$

Diskrete Mathe VO

14.11.

$\mathbb{N}$ bedeutet die Menge der positiven ganzen Zahlen, a^+ ist der Nachfolger von a.

1) $1 \in \mathbb{N}$
6) $\forall a \in \mathbb{N} : a^+ \in \mathbb{N}$
8) $\forall a \in \mathbb{N} : a^+ \neq 1$
7) $\forall a,b \in \mathbb{N} : a = b \iff a^+ = b^+$
9) Für alle Mengen K, die $1 \in K \wedge \forall x \in K : x^+ \in K$ erfüllen, gilt $\mathbb{N} \subseteq K$

$1, 1^+, (1^+)^+ = 1^{++}, \ldots$

Peanos Definition der Addition:

$a + 1 :=$ Nachfolger von $a = a^+$

2) $a + (b^+) := (a+b)^+$

BSP: $\overbrace{1^+}^{2} + \overbrace{1^{+++}}^{4}$

$= (1^+ + 1^{++})^+$ ← Regel 2

$= ((1^+ + 1^+)^+)^+$

$= (((1^+ + 1)^+)^+)^+ = \overbrace{1^{++++++}}^{6}$

Andere Erklärung $a + S(b) = S(a+b)$ (Nachfolger von b; Regeln: $a+1 = S(a)$)

$\underbrace{S(1)}_{a} + \underbrace{S(S(S(1)))}_{b}$

$= \underbrace{S(S(1))}_{a} + \underbrace{S(S(1))}_{b}$

$= S(S(S(1) + S(1)))$

$= S(S(S(\underbrace{S(1) + 1}_{= S(S(1))})))$

$= S(S(S(S(S(1)))))$

$3 + 4$

$1^{++} + 1^{+++}$ (a: 1^{++}, b: 1^{+++})

$= (1^{++} + 1^{++})^{+}$ (b: 1^{++})

$= ((1^{++} + 1^{+})^{+})^{+}$

$= (((1^{++} + 1)^{+})^{+})^{+} = 1^{+++++++}$

$1^{++} = (1^{+})^{+}$

Grundregel: 3 + Nachfolger von 2 = Nachfolger von 3+2

von Neumanns Konstruktion von $\mathbb{N}$:

Def: Sei x eine Menge. Der Nachfolger von x ist def. durch $x^{+} := x \cup \{x\}$

Bsp: $A = \{3,7\}$

$A^{+} = \{3,7,\{3,7\}\}$

Def.: $0 := \emptyset$, $1 := 0^{+}$, $2 := 1^{+}$

ReRe $\emptyset \cup A = A$

1 hat ein Element, 2 hat 2 Elemente, 3 hat 3 El. ...

$0 = \emptyset$

$1 = \emptyset^{+} = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\}$ $\{0,1\}$

$2 = 1^{+} = \{\emptyset\}^{+} = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$

$3 = 2^{+} = \{\emptyset, \{\emptyset\}\}^{+} = \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

$= \{0,1,2\}$

Unendlichkeitsaxiom: Nun fordert man, dass es eine Menge U gibt, die $\emptyset \in U$ und $\forall u \in U : u^{+} \in U$ erfüllt.

$\mathbb{N}_0$ ist der Durchschnitt aller Teilmengen von U, die 0 enthalten und mit jedem Element auch dessen Nachfolger.

1) unhandlich

[3 braucht 15 Symbole
[n -"- $2^{n+1} - 1$ Symbole

[$3 = 0^{+++}$ ... 4 Symbole
[n ... n + 1 Symbole

n braucht im Stellenwertsystem $\lfloor \log_{10}(n) \rfloor + 1$ Symb.

Def: Für $x \in \mathbb{R}$ ist $\lfloor x \rfloor := \max \{ n \in \mathbb{Z} \mid n \leq x \}$

$\lfloor \pi \rfloor = 3$

$\lfloor -\frac{1}{2} \rfloor = -1$

$\lfloor -\pi \rfloor = -4$

$\lfloor -2 \rfloor = -2$

Floor-Fkt

$\lceil \pi \rceil = 4$ (ceiling-Fkt)

$\lceil -2 \rceil = -2$

$\lceil 7{,}5 \rceil = 8$

2) Ungewöhnl. Gleichheiten

z.B. $\{0\} = 1$

$2 = 1 \cup \{\emptyset, \emptyset\}$

↳ $2 = \{\emptyset \{\emptyset\}\}$

$1 \cup (\emptyset, \emptyset) = \underbrace{\{\emptyset\}}_{1} \cup \{\{\emptyset\}, \{\emptyset, \emptyset\}\}$

$= \{\emptyset\} \cup \{\emptyset, \{\emptyset\}\}$

3) anzweifelbare Axiome

Vorteile

1) keine neuen Objekte erforderlich, Mengen reichen aus
2) keine Axiome für $\mathbb{N}$; man verwendet nur die Axiome der Mengenlehre. reduzierte Widerspr. gefahr
3) Ordnung: $x \leq y \Leftrightarrow x \subseteq y$
4) siehe Skript

$\mathbb{N}_0 \quad \mathbb{N}_0^+ = \mathbb{N}_0 \cup \{\mathbb{N}_0\}$

$\omega^+ = \omega \cup \{\omega\}$ (omega)

also $0, 1, 2, \ldots \omega, \omega^+, \omega^{++}$

→ lässt sich erweitern (Ordinal-, Kardinalzahlen, ...)

Satz: Es gilt

1) $0 \in \mathbb{N}_0$
2) $\forall n \in \mathbb{N}_0 : n^+ \in \mathbb{N}_0$
3) es gibt kein $n \in \mathbb{N}_0$ mit $n^+ = 0$
4) $\forall n, m \in \mathbb{N}_0 : n^+ = m^+ \Rightarrow n = m$ (Umkehrung gilt aber auch!)

$n^+ = n \cup \{n\}$
$= m \cup \{m\} = m^+$

Beweis (1), (2) ergibt sich aus der Def. von $\mathbb{N}_0$

(3) Nehmen wir an, $n \in \mathbb{N}_0$ ist so, dass $n \cup \{n\} = \emptyset$ ($n^+ = 0$)
Da $n \in n \cup \{n\}$ und $n \notin \emptyset$, können diese beiden Mengen nicht gleich sein

Ann.: $A \cup \{A\} = B \cup \{B\}$
z.z. $A = B$

Wir versuchen 4) zu zeigen:
Seien $n, m \in \mathbb{N}_0$ so, dass $n^+ = m^+$
z.z. $n = m$
Wir wissen: $n \cup \{n\} = m \cup \{m\}$ z.z. $n = m$

Sei $x \in n$ z.z. $x \in m$
Da $x \in n$, gilt $x \in n \cup \{n\}$. Also $x \in m \cup \{m\}$

Somit $x \in m$ oder $x \in \{m\}$

1. Fall] $x \in m$ ✓

2. Fall] $x \in \{m\}$ Also $x = m$

Nun finden wir keinen Grund für $x \in m$.

$\{a_1, a_2, \dots, a_n\} := \{x \mid x = a_1 \vee x = a_2 \vee \dots \vee x = a_n\}$

$\{a\} = \{x \mid x = a\}$

$x \in \{m\}$ Also $x = m$

Satz] Für alle Teilmengen S von $\mathbb{N}_0$ gilt:
Wenn $0 \in S$ und $\forall n \in S : n^+ \in S$ gilt,
so gilt: $S = \mathbb{N}_0$

Diskrete Mathe 10

20. Nov

Neumanns Modell für die Peano-Axiome

$A^+ := A \cup \{A\}$, $0 := \emptyset$

Unendlichkeitsaxiom:

Axiom: es gibt eine Menge U, die 0 enthält, und die $\forall u \in U : u^+ \in U$ erfüllt

$[\{\emptyset, \emptyset^+, \emptyset^{++}, \dots\} \subseteq U]$

Def. $\mathbb{N}_0$ ist der Durchschnitt aller Teilmengen T von U, die $0 \in T$ und $\forall t \in T : t^+ \in T$ erfüllen

Satz Für alle $S \subseteq \mathbb{N}_0$ gilt: Wenn $0 \in S$ und $\forall n \in S : n^+ \in S$ gilt, so gilt $S = \mathbb{N}_0$

Beweis: S ist eine Teilmenge von U, die $0 \in S$ und $\forall n \in S : n^+ \in S$ erfüllt. Also ist S eine der Mengen, die bei der Bildung von $\mathbb{N}_0$ geschnitten wurden. Also $\mathbb{N}_0 \subseteq S$.
Insgesamt: $S = \mathbb{N}_0$.

Satz (Peano-Axiom 7):
Für alle $m, n \in \mathbb{N}_0$ mit $n^+ = m^+$ gilt $n = m$

Lemma Für alle $i, x \in \mathbb{N}_0$: $x \in i \Rightarrow x \subseteq i$

$0 = \emptyset$

$1 = \{\emptyset\}$

$2 = \{\emptyset, \{\emptyset\}\}$ (× über $\{\emptyset\}$)

$3 = \{\emptyset, \{\emptyset\}, \{\emptyset\{\emptyset\}\}\}$

Bsp: $\{\emptyset\}$ ist Element von $\{\emptyset, \{\emptyset\}\} = 2$
Der Satz behauptet, dass $\{\emptyset\}$ auch eine Teilmenge von $\{\emptyset, \{\emptyset\}\}$ ist.
D.h. $\forall x \in \{\emptyset\} : x \in \{\emptyset, \{\emptyset\}\}$

Beweis des Lemmas:

Wir zeigen, dass die Menge $S := \{i \in \mathbb{N}_0 \mid \forall x \in \mathbb{N}_0: x \in i \Rightarrow x \subseteq i\}$ die Eigenschaft $0 \in S$ und $\forall i \in S: i^+ \in S$ erfüllt.

$0 \in S$: z.z.: $\forall x \in \mathbb{N}_0: x \in 0 \Rightarrow x \subseteq 0$

z.z. $\forall x \in \mathbb{N}_0: \underbrace{x \in \emptyset}_{\text{f., somit gilt Implikation (weil aus falschem folgt beliebiges)}} \Rightarrow x \subseteq \emptyset$

Klausur: eigenständigen Beweis finden nicht, nur leichte Beweis

Nun zeigen wir:
$\forall i \in S: i^+ \in S$
Sei dazu $i \in S$. z.z.: $i^+ \in S$

Diesen Beweis wiedergeben kann aber schon kommen!

z.z. $\forall x \in \mathbb{N}_0: x \in i^+ \Rightarrow x \subseteq i^+$

Ev. Lückentext (sehr nicht) kann aber sein

Sei dazu $x \in \mathbb{N}_0$. Wir nehmen an, dass $x \in i^+$.
z.z. ist $x \subseteq i^+$
Da $x \in i^+ = i \cup \{i\}$, gilt $x \in i$ oder $x \in \{i\}$

1. Fall) $x \in i$: Da $i \in S$, gilt $x \subseteq i$. Da $i \subseteq i \cup \{i\} = i^+$ gilt dann auch $x \subseteq i^+$

2. Fall) $x \in \{i\}$. Dann gilt $x = i$. Also gilt $x \subseteq i$, und somit $x \subseteq i^+$

Folglich erfüllt S die Eigenschaften $0 \in S$ und $\forall i \in S \Rightarrow i^+ \in S$
Also gilt $S = \mathbb{N}_0$, somit gilt das Lemma

Nun zeigen wir Satz PA 7) (werden das Lemma brauchen)

Beweis d. Satzes PA 7

Seien $n, m \in \mathbb{N}_0$ so, dass $n^+ = m^+$

Z.Z. $n = m$

Wir nehmen an, dass $n \neq m$.

Da $n \in n \cup \{n\}$, gilt $n \in n^+$. Also gilt $n \in m^+$, und somit $n \in m \cup \{m\}$

1. Fall) $n \in m$: Dann gilt (lt. Lemma) $n \subseteq m$.

2 Fall) $n = m$: Dieser Fall kann nicht eintreten (weil Annahme)

Außerdem gilt (mit der gleichen Überlegung) auch $m \subseteq n$.

Es gilt also $n \subseteq m$ und $m \subseteq n$, also $m = n$, im Widerspruch zur Annahme $m \neq n$.

* also $A \in A \cup \{A\} = A^+$

$\{x \mid X = A\}$ // weil $A \in \{A\}$ * gilt $A \in A \cup \{A\}$

$A^+ = A \cup \{A\}$

omega $\omega := \mathbb{N}_0$

$\omega^+ = \{1, 2, \ldots, \omega\} = \omega \cup \{\omega\}$

Satz) Sei $n \in \mathbb{N}$. Dann gibt es $x \in \mathbb{N}_0$ mit $x^+ = n$.

Beweis: Sei $S := \{n \in \mathbb{N}_0 \mid n = 0 \text{ oder } \exists x \in \mathbb{N}_0 : x^+ = n\}$

Wir zeigen nun: $S = \mathbb{N}_0$

Dazu zeigen wir: $0 \in S$ und $\forall n \in S : n^+ \in S$.

$0 \in S$ gilt ✓ (siehe $S \to n = 0$ oder...)

Sei $n \in S$ (neue Variable) (beliebig aber fix). Z.Z. $n^+ \in S$ (von n wissen wir es schon)

Z.Z.: $n^+ = 0 \vee \exists x \in \mathbb{N}_0 : x^+ = n^+$

Da $n^+ = n^+$ (wir setzen n ein), gibt es ein $x \in \mathbb{N}_0$ mit $x^+ = n^+$, nämlich $x := n$.

Also gilt $n^+ \in S$.

Satz) Sei $A(n)$ eine Aussageform, die für alle $n \in \mathbb{N}_0$ definiert ist.

Wir nehmen an, dass $A(0)$ gilt, und dass $\forall n \in \mathbb{N}_0 : (A(n) \Rightarrow A(n+1))$ gilt.

Dann gilt: $\forall m \in \mathbb{N}_0 : A(m)$.

Beweis) $S := \{m \in \mathbb{N}_0 \mid A(m) \text{ gilt}\}$

erfüllt $0 \in S$ und $\forall m \in S : \underbrace{m+1}_{m^+} \in S$

Also $S = \mathbb{N}_0$

Anstatt $\forall m \in \mathbb{N}_0 : A(m)$ kann ich also $A(0)$ und $\forall m \in \mathbb{N}_0 : A(m) \Rightarrow A(m+1)$ beweisen

Beweis von $\forall m \in \mathbb{N}_0 : A(m)$ durch „vollständige Induktion"

Satz 3.16)

Def: $m! := \prod_{i=1}^{m} i = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot m$, $0! := 1$

$$\binom{70}{2} = \frac{70!}{2!\,68!} = \frac{70 \cdot 69}{1 \cdot 2} = 2415$$

$70! = 70 \cdot 69 \cdot (68!)$

$$n^{\underline{i}} = \underbrace{n \cdot (n-1) \cdot (n-2) \cdots (n-i+1)}_{i \text{ Faktoren}}$$

$$\binom{n}{i} = \frac{n^{\underline{i}}}{i!}$$

$\binom{0}{0}$

$\binom{1}{0}$ $\binom{1}{1}$

$\binom{2}{0}$ $\binom{2}{1}$ $\binom{2}{2}$

$\binom{3}{0}$ $\binom{3}{1}$ $\binom{3}{2}$ $\binom{3}{3}$

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

* Skript nach „dem beweist (33)

Wir zeigen nun mit Induktion nach n, dass für alle $n \in \mathbb{N}$ gilt: $\forall i \in \{0, \ldots, n\}$ hat jede n-elementige Menge genau $\binom{n}{i}$ i-elem. Teilmengen.

$=: P(n)$

Induktionsanfang: $n = 1$

1 elementige Menge

$\{a\}$ $P(\{a\}) = \{\emptyset, \{a\}\}$

$$\binom{1}{0} = \frac{1!}{0!\,1!} = 1 \qquad \binom{1}{1} = 1$$

$\{a\}$ hat genau eine 0-elementige & eine einelementige Menge.

Wir zeigen nun, dass $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n+1)$ gilt.
Sei dazu $n \in \mathbb{N}$. Wir nehmen an, dass
Induktionsannahme: $P(n)$ gilt.

normalerweise wird das bei Induktion beim nicht gesagt, aber eig wichtig

z.z.
Induktionsbehauptung: $P(n+1)$ gilt.

wollen zeigen: B hat genau $\binom{n+1}{i}$ Teilmengen mit i Elementen.

Sei nun B eine $n+1$-elementige Menge. Sei $i \in \{0, \dots, n+1\}$. ⊗ B hat genau eine 0-el. Teilmenge (nämlich $\emptyset$) und genau eine $n+1$-elementige Teilmenge (nämlich B).

⊗ 1. Fall $i = 0 \vee i = n+1$

2. Fall: $i \in \{1, \dots, n\}$:
$M = \{T \subseteq B \mid \#T = i\}$. Ziel ist, zu zeigen, dass
(T: Teilmengen T)
M genau $\binom{n+1}{i}$ Elemente hat.
Sei $a \in B$
$M = \{T \subseteq B \mid \#T = i \text{ und } a \in T\} \cup \{T \subseteq B \mid \#T = i \text{ und } a \notin T\}$
$= \{S \cup \{a\} \mid S \subseteq B \setminus \{a\} \text{ und } \#S = i-1\} \cup \{T \subseteq B \setminus \{a\} \mid \#T = i\}$

$B \setminus \{a\}$ hat n Elemente. Wegen der Induktionsannahme hat $B \setminus \{a\}$ genau $\binom{n}{i}$ i-elementige Teilmengen.

$B \setminus \{a\}$ hat genau $\binom{n}{i-1}$ Teilmengen mit $i-1$ Elementen (wegen der Induktionsannahme).

Also: $|M| = \binom{n}{i-1} + \binom{n}{i} = \binom{n+1}{i}$ ■

5* Sei $n := m+1$

Dann gilt: $\forall i \in \{1, \dots, m\}: \binom{m+1}{i} = \binom{m}{i} + \binom{m}{i-1}$

Diskrete V0

21. Nov

Vollständige Induktion

Um $\forall n \in \mathbb{N}_0 : A(n)$ zu beweisen, genügt es
$A(0)$ und $\forall n \in \mathbb{N}_0 : A(n) \Rightarrow A(n+1)$ zu zeigen

Genauso genügt es
$A(0)$ und $\forall n \in \mathbb{N}_0 : \left((\forall k \in \{0,1,\dots,n\} : A(k)) \Rightarrow A(n+1) \right)$

$\forall n \in \mathbb{N}_0 : A(n) \Rightarrow A(n+1) \equiv \forall m \in \mathbb{N} : A(m-1) \Rightarrow A(m))$

Rekursive Definitionen

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

$5! = (4+1)! = 5 \cdot 4! = 5 \cdot 4 \cdot 3! = 5 \cdot 4 \cdot 3 \cdot 2! =$
$= 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 0! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 = \underline{\underline{120}}$

—

$F_0 = 0 \qquad F_1 = 1$

$F_n = F_{n-1} + F_{n-2}$ für $n \geq 2$ Fibonacci-Zahlen

$F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$,
$F_6 = 8$, $F_7 = 13$ (immer die 2 vorigen Zsm. zählen)

Satz) (Definitionsmethode Rekursion)
Sei X eine Menge, sei $a \in X$, sei $f : X \to X$.
Dann gibt es genau eine Fkt $u : \mathbb{N}_0 \to X$ mit
$u(0) = a$ und $u(n+1) = f(u(n))$

Bsp: $X := \mathbb{R} \qquad f : \mathbb{R} \to \mathbb{R}, \; x \mapsto 2x \qquad a := 1$

$u(0) = 1$

$u(n+1) = 2 \cdot u(n)$

$u(1) = 2 \qquad u(2) = 4 \qquad u(x) = 2^x$

(wenn $a := 7 \rightarrow u(0) = 7 \qquad u(1) = 14$)

Bsp: $u(0) = 15 \qquad u(n+1) = 2 \cdot u(n) - 1 \qquad$ für $n \in \mathbb{N}_0$

$u(0) = 15 \qquad u(1) = 2 \cdot u(0) - 1 = 2 \cdot 15 - 1 = 29$

$u(2) = 2 \cdot u(1) - 1 = 2 \cdot 29 - 1 = 57$

$u(3) = 2 \cdot 57 - 1 = 113$

16 − 1	15	$u(0)$
32 − 3	29	$u(1)$
64 − 7	57	$(u(2))$
128 − 15	113	$u(3)$

Vermutung: $u(n) = 2^{n+4} - (2^{n+1} - 1)$ (*1)

Sei $u: \mathbb{N}_0 \rightarrow \mathbb{N}_0$ geg. durch $u(0) = 15$ und $u(n+1) = 2 \cdot u(n) - 1$. für $n \in \mathbb{N}_0$

Zeigen Sie: $\forall m \in \mathbb{N}_0 : \underbrace{u(m) = 2^{m+4} - 2^{m+1} + 1}_{A(m)}$ (1)

Wir beweisen (1) durch vollständige Induktion.

Wir zeigen also $u(0) = 2^{0+4} - 2^{0+1} + 1$ und (2)

$\forall m \in \mathbb{N}_0 : u(m) = 2^{m+4} - 2^{m+1} + 1 \Rightarrow u(m+1) = 2^{m+5} - 2^{m+2} + 1$ (3)

(Klammer wurde aufgelöst *1)

(2) „Induktionsanfang"

$15 = 16 - 2 + 1$. Daher gilt (2)

(3) „Induktionsschritt"

Sei $m \in \mathbb{N}_0$ (vorrangig wird neu gewählt). Wir nehmen an, dass $u(m) = 2^{m+4} - 2^{m+1} + 1$.

Allquantor wird „aufgelöst"

z.z. $U(m+1) = 2^{m+5} - 2^{m+2} + 1$ z.B. $2^1 \cdot 2^1 = 2^2 = 4$ Potenzregeln (Hochzahlen addieren)

W.w.: (steht ganz oben)

$$U(m+1) = 2 \cdot U(m) - 1 \overset{\text{II. Annahme Ind.}}{=} 2 \cdot (2^{m+4} - 2^{m+1} + 1) - 1 =$$

$$= 2^{m+5} - 2^{m+2} + 2 - 1$$

$$= 2^{m+5} - 2^{m+2} + 1$$

Somit gilt (3).

Also gilt (1).

3.2. Aufbau der Arithmetik

Def Für jedes $m \in \mathbb{N}_0$ definieren wir eine Fkt $a_m : \mathbb{N}_0 \to \mathbb{N}_0$ rekursiv durch $a_m(0) := m$ und $a_m(x^+) := (a_m(x))^+$ für alle $x \in \mathbb{N}_0$

z.B. $a_2(\overset{x}{0^{++}}) = (a_2(\overset{x}{0^{+}}))^+ = ((a_2(0))^+)^+ = 2^{++}$

$2 = 0^{++}$

$$a_3(\overset{x}{0^{++}}) = \underbrace{(a_3(0^+))^+}_{(a_3(0))^+} = (a_3(0))^{++} = 3^{++} = 0^{+++++}$$

[Nun definieren wir $x + y := a_x(y)$ für $x, y \in \mathbb{N}_0$

- $\forall x \in \mathbb{N}_0 : x + 0 = x$

Bew.) $x + 0 = a_x(0) = x$

Satz) Für alle $x \in \mathbb{N}_0$ gilt: $0 + x = x$

Bew) $0 + x = a_0(x) = ??$

Wir beweisen das durch Induktion

Wir zeigen zuerst $0 + 0 = 0$ und

$\forall x \in \mathbb{N}_0 : 0 + x = x \Rightarrow 0 + x^+ = x^+$

$0 + 0 = a_0(0) = 0$. ✓ (Indukt. anfang)

Sei $x \in \mathbb{N}_0$. Wir nehmen an, dass $0 + x = x$ ($\forall x \; 0 + x = x$ ↑ wissen wir noch nicht, denen dürfen wir für das x nicht einfach etwas einsetzen)

z.z. $0 + x^+ = x^+$

$0 + x^+ = a_0(x^+)$ weil Def. Addition

$= (a_0(x))^+ = (0 + x)^+$ ($0 + x = x$)

Def von +: $a_0(x) = 0 + x$, $x + y = a_x(y)$

$= x^+$

↳ Ind. annahme $0 + x = x$

$(a+b)^2 = a^2 + 2ab + b^2$ richtiger logischer Schluss | $x = 7$, $y + 7 = 7$ } kein richtiger log. Schluss

$(2+x)^2 = 4 + 4x + x^2$

w.W. $\forall a,b \in \mathbb{R} : (a+b)^2 = a^2 + 2ab + b^2$

Es ist erlaubt, von $\forall x : A(x)$ auf $A(7)$ zu schließen
Von $A(x)$ kann man nicht auf $A(7)$ schließen.

(42) $(\forall x \in \mathbb{N}_0)$ $\quad x^+ \neq x$

$S := \{x \in \mathbb{N}_0 \mid x^+ \neq x\} = \mathbb{N}_0$

$\rightarrow \forall x \in S \subset \mathbb{N}_0 \quad x^+ \neq x$

$\neg (\forall x \in S \subset \mathbb{N}_0 : x^+ \neq x)$

$\Leftrightarrow \exists x \in S \subset \mathbb{N}_0 : x^+ = x$

Annahme) $S \neq \mathbb{N}_0$, $S \subseteq \mathbb{N}_0$

D.h. es existiert ein $x \in \mathbb{N}_0$ für das gilt

$x \notin S$. x ist nicht in $S \rightarrow$

Daher $x^+ = x$

Mit Satz 4.2 (3) ist $y^+ \neq 0$ für alle (weil es keines gibt) $y \in \mathbb{N}_0$. Insbesondere $x = x^+ \neq 0$ d.h. $x \neq 0$.

1. Fall) $x^+ \in S$, dann gilt $(x^+)^+ \neq x^+$ (*)

(lt. Def. von S)

2. Fall) $x^+ \notin S$, dann gilt $(x^+)^+ = x^+$

Struktur $x^+ = y^+ \Rightarrow x = y$ } Peano Pkt 4

Mit Peano 4.2 (4) ist $x^+ = x$

D.h. $x \notin S$

(2) (X) Annahme: $S \neq \mathbb{N}_0$ $\quad S \subsetneq \mathbb{N}_0$, $x \notin S$ und daher $x^+ = x$

Da $x \neq 0$ (4.2 (3)), d.h. $0 \in S$ (lt. Axiom)

Dann verwenden wir 4.2 (5)

z.z. $0 \in S$ und $(\forall x \in S)\ x^+ \in S$ (*)

Dann sagt der Satz $S = \mathbb{N}_0$

Z.Z. $\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$ $\forall n \in \mathbb{N}$ Übung → anal. Bsp

Anfang: $n=1$: $1 = \frac{1 \cdot 2}{2}$ ✓

Hypothese: $\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$

Behauptung: $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$

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

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

$* \quad \frac{n \cdot (n+1) + 2 \cdot (n+1)}{2} = \frac{(n+1)(n+2)}{2}$

---

41) $B(y) := y = 3 \iff$

$\exists z \, \forall x \quad x \cdot (y-3) = z$

$\Rightarrow$: $z = 0$

$\Leftarrow$: Annahme $y \neq 3$, $z \in \mathbb{R}$ beliebig

1 Fall) $\underline{x(y-3)} = z = (x+1)(y-3) = \underline{x(y-3)} + (y-3)$

$0 = y - 3 \iff y = 3$ ↯ Wid zur Annahme

2 Fall) analog

Diskrete Mathe VO

27.11.

$(\mathbb{N}_0, x \mapsto x^+)$ $\quad a_m(0) := m$, $a_m(x^+) = (a_m(x))^+$ für $x \in \mathbb{N}_0$

$x + y := a_x(y)$ $\quad$ Ziel: Beweis von $\forall x, y \in \mathbb{N}_0 : x + y = y + x$

Lemma 1 Für alle $x \in \mathbb{N}_0 : x + 0 = 0 + x = x$ (am Termin davor bewiesen)

Lemma 2 Für alle $u, v \in \mathbb{N}_0 : (v+u)^+ = v^+ + u$ (nach Def. $= v + u^+$; Erklärung warum + bei v später)

Wir zeigen dieses Lemma durch Induktion nach u.

Wir zeigen also: $\forall u \in \mathbb{N}_0 : A(u)$, wobei

$A(u) :\Leftrightarrow \forall v \in \mathbb{N}_0 : (v+u)^+ = v^+ + u$

Ind. anfang: Wir zeigen $A(0)$.

z.z. $\forall v \in \mathbb{N}_0 : (v+0)^+ = v^+ + 0$

Sei $v \in \mathbb{N}_0$. Dann gilt $(v+0)^+ = v^+ = v^+ + 0$.

Ind. schritt: Wir zeigen:

$\forall u \in \mathbb{N}_0 : A(u) \Rightarrow A(u^+)$.

Sei dazu $u \in \mathbb{N}_0$. Wir nehmen an, dass $A(u)$ gilt.

z.z. $A(u^+)$

Annahme: $\forall v \in \mathbb{N}_0 : (v+u)^+ = v^+ + u$

z.z. $\forall v \in \mathbb{N}_0 : (v+u^+)^+ = v^+ + u^+$

Sei dazu $v \in \mathbb{N}_0$.

$(v+u^+)^+ = (a_v(u^+))^+ \overset{\text{def. } a_v}{=} ((a_v(u))^+)^+ = ((v+u)^+)^+$ (siehe Annahme)

Nach Ind. ann. ist der letzte Ausdruck gleich

$(v^+ + u)^+ = (a_{v^+}(u))^+ = a_{v^+}(u^+) = v^+ + u^+$

↳ d.h. Lemma sagt, ich kann + dazu ziehen wo ich will! (bei u oder bei v)

Satz) Für alle $x, y \in \mathbb{N}_0$ gilt $x + y = y + x$
(Kommutativgesetz)

Bew: Wir zeigen

$\forall y \in \mathbb{N}_0 \; (\forall x \in \mathbb{N}_0 : x + y = y + x) \equiv \forall y \in \mathbb{N}_0 : A(y)$ (*)

durch Induktion nach y.

Ind.anfang: z.z. $A(0)$, also

$\forall x \in \mathbb{N}_0 : x + 0 = 0 + x$

Das gilt nach Lemma 1

Einschub: $x + 0 = a_x(0) = x$

$x = y \wedge y = z \Rightarrow x = z$

Induktionsschritt:

z.z. $\forall y \in \mathbb{N}_0 : A(y) \Rightarrow A(y^+)$

Sei dazu $y \in \mathbb{N}_0$. Wir nehmen an, dass $A(y)$ gilt.

z.z. $A(y^+)$

Ann.: $\forall x \in \mathbb{N}_0 : x + y = y + x$

z.z.: $\forall x \in \mathbb{N}_0 : x + (y^+) = (y^+) + x$

Sei dazu $x \in \mathbb{N}_0$.

$$x + y^+ = (x + y)^+ \overset{\text{ind. annahme}}{=} (y + x)^+ \overset{\text{Lemma 2}}{=} y^+ + x$$

Somit gilt (*).

Peano definiert nun

$x - y$ (falls $x \geq y$), $x \cdot y$

und beweist $\forall a,b,c \in \mathbb{N}_0 : a \cdot (b+c) = a \cdot b + a \cdot c$, ...

Dann: $\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, \dots \}$

In $\mathbb{Z}$ gilt:

$\forall x,y,z \in \mathbb{Z} : (x+y)+z = x+(y+z)$ + ist assoziativ

⋮

alle ReRe siehe S. 43 4.9.

Ein Ring ist ein Tripel $(R, +, \cdot)$ (Bsp.), wobei

R ist eine nichtleere Menge,

$+ : R \times R \to R$ (+ ist eine Fkt von $R \times R$ nach R),

$\cdot : R \times R \to R$ ($\cdot$ ist Fkt von $R \times R$ nach R)

es gelten bestimmte Rechengesetze (Assoz. von +, ...)

Bsp: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}^{2\times 2}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$ sind Ringe

Division & Teilbarkeit

Def: Für $x,y \in \mathbb{Z}$ def. wir

$$x \mid y :\Leftrightarrow \exists z \in \mathbb{Z} : x \cdot y = z$$

x teilt y, oder y ist ein Vielfaches von x

Bsp: $12 \mid 60$, $12 \nmid 59$, $(-12) \mid 60$

$5 \mid 0$, $0 \nmid 5$, $0 \mid 0$ ($\frac{0}{0}$ obwohl def ist nicht)

jede Zahl teilt 0
0 teilt nur sich selbst

$$723 : 16 = 45$$
$$083$$
$$03\ R.$$

$$\vdots$$

↳ $\underbrace{723}_{\text{Dividend}} = \underbrace{45}_{\text{Quotient}} \cdot \underbrace{16}_{\text{Divisor}} + \underbrace{3}_{\text{Rest}}$

Satz) Seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}$. Dann gibt es genau ein Paar $(q, r) \in \mathbb{Z} \times \mathbb{N}_0$, sodass $a = n \cdot q + r$ und $r \in \{0, 1, \dots, n-1\}$

$A \times B = \{(a,b) \mid a \in A, b \in B\}$ — kartesisches Produkt

Induktionsbeweis siehe Skript

$a = 723 \quad n = 16 \quad 723 = 16 \cdot 45 + 3 \quad q = 45, r = 3$

$$-723 = (-45) \cdot 16 + (-3)$$
$$= (-46) \cdot 16 + 13$$
$$q = -46 \ ; \ r = 13$$

Den Rest bezeichnet man oft mit $r = a \bmod n$.

$723 \bmod 16 = 3 \qquad (-723) \bmod 16 = 13$

Diskrete vo

28.11.

Teilbarkeit : $t \mid a \iff \exists z \in \mathbb{Z} : a = z \cdot t$

t ist ein Teiler von a

Def: Seien $a, b \in \mathbb{Z}$ (nicht beide 0). Dann ist ggT(a,b) die größte Zahl in $\mathbb{N}$, für die $t \mid a$ und $t \mid b$ gilt.

ggT (30, 12)

pos. Teiler von 30 $\{$ $T_{30}^+ = \{1, 2, 3, 5, 6, 10, 15, 30\}$

$T_{12}^+ = \{1, 2, 3, 4, 6, 12\}$

gemeinsame Teiler $= T_{30}^+ \cap T_{12}^+ = \{1, 2, 3, 6\}$

ggT (12, 30) $= \max\{1, 2, 3, 6\} = 6$.

Satz Seien $a, b \in \mathbb{Z}$, nicht beide 0, und sei $z \in \mathbb{Z}$. Dann gilt ggT(a,b) = ggT(a + zb, b)

ggT (30, 12) $\overset{30 + 2 \cdot 12}{=}$ (ggT (54, 12)) — nicht so / so

$= ggT(\overset{30 + (-2) \cdot 12}{6}, 12) = ggT(12, 6) =$

$= ggT(0, 6) = 6$

Beweis : Wir zeigen als erstes:

$\{t \in \mathbb{N} : t \mid a \text{ und } t \mid b\} = \{t \in \mathbb{N} : t \mid a + bz \text{ und } t \mid b\}$

„$\subseteq$" Sei $t \in \mathbb{N}$ ($\mathbb{Z}$ stimmt auch) so, dass $t \mid a$ und $t \mid b$.

z.z. $t \mid a + zb$ und $t \mid b$

Da $t \mid b$, gilt $t \mid b$. Somit bleibt zu zeigen, dass $t \mid a + z \cdot b$

Da $t|a$, gibt es $a_1 \in \mathbb{Z}$ mit $a = a_1 \cdot t$ lt. Def. der Teilbarkeit

Da $t|b$, gibt es ein $b_1 \in \mathbb{Z}$ mit $b = b_1 \cdot t$

Insgesamt gilt dann

$a + z \cdot b = a_1 \cdot t + z \cdot b_1 \cdot t = (a_1 + z \cdot b_1) \cdot t$, und somit gilt $t | a + b \cdot z$.

"$\supseteq$" Sei $t \in \mathbb{N}$ so, dass $t|a + z \cdot b$ und $t|b$

z.z. $t|a$ und $t|b$ wir wollen auf das hin

[$a = \underbrace{(a + z \cdot b)}_{t| \text{ vielfaches}} - z \cdot \underbrace{b}_{t|}$, und somit ist a ein

ausführlich

Vielfaches von t.

Da $t | a + zb$, gibt es $c \in \mathbb{N}$, sodass $t \cdot c = a + z \cdot b$

Da $t|b$, gibt es $d \in \mathbb{N}$, sodass $t \cdot d = b$.

schreibe ich, damit ich verifizieren kann, dass $t|b$

$a = (a + \textcircled{z \cdot b}) - \textcircled{z \cdot b} = t \cdot c - ztd = t \cdot (c - zd)$,

und somit gilt $t|a$.

Aufgrund dieser Mengengleichheit gilt

$\max \{ t \in \mathbb{N} : t|a \text{ und } t|b \} = \max \{ t \in \mathbb{N} : t|a + zb \text{ und } t|b \}$

Also $ggT(a,b) = ggT(a + zb, b)$

$ggT(147,33) = ggT(147 - \textcircled{4}33, 33)$ zam teilen, Rest hinschreiben usw.

$= ggT(15,33) = ggT(33,15) =$

$= ggT(33 - \textcircled{2} \cdot 15, 15) = ggT(3,15)$

$= ggT(15,3) = ggT(15 - \textcircled{5}3, 3) =$

$= ggT(0,3) = \underline{\underline{3}}$

	147	33
147	1	0
33	0	1
15	1	-4
3	-2	9
0		

$1-2\cdot(-4)=9$

$147 = 1\cdot 147 + 0\cdot 33$

$33 = 0\cdot 147 + 1\cdot 33$

$15 = 1\cdot 147 + -4\cdot 33$

$3 = (-2)\cdot 147 + 9\cdot 33$

$a = 561 \qquad b = 112$

	561	112	
561	1	0	I
112	0	1	II
1	1	-5	I − 5·112
0			

eukliol'scher Algorythmus

googeln weil wichtig!

$ggT(561, 112) = 1$

$= 1\cdot 561 + (-5)\cdot 112$

$a = 123 \qquad b = 428$

	123	428	
123	1	0	
428	0	1	II
123	1	0	III
← 59	-3	1	IV = II − 3·III
5	7	-2	V = III − 2·IV
4	-80	23	VI = IV − 11·V
← 1	87	-25	
0			

Rest von 428:123

123 steckt 3× in 428

5−4

$1-(-2\cdot-3)$

$ggT(123, 428) = 1$

$= 87\cdot 123 - 25\cdot 428$

ggT ist das vielfache jedes gem. Teilers

Satz) Seien $a, b \in \mathbb{Z}$ (nicht beide 0) . Dann gibt es $u, v \in \mathbb{Z}$, sodass $ggT(a,b) = u \cdot a + v \cdot b$

(u, v: Kofaktoren)

Erweiterter Euklidscher Algorithmus

Satz) Seien $a, b \in \mathbb{Z}$, nicht beide 0, und sei $t \in \mathbb{Z}$ so, dass $t \mid a$ und $t \mid b$. Dann gilt auch $t \mid ggT(a,b)$.

Beweis] Aufgrund des Euklidschen Algorithmus gibt es $u, v \in \mathbb{Z}$, sodass $ggT(a,b) = u \cdot a + v \cdot b$

[Da $t \mid a$ und $t \mid b$, gilt $t \mid ua$ und $t \mid vb$ und somit $t \mid ua + vb$, also $t \mid ggT(a,b)$.

[Da $t \mid a$ und $t \mid b$, gibt es $z_1 \in \mathbb{Z}$ und $z_2 \in \mathbb{Z}$, sodass $a = z_1 \cdot t$ und $b = z_2 \cdot t$. Also
$ggT(a,b) = ua + vb = z_1 \cdot t \cdot u + z_2 \cdot t \cdot v =$
$= t(uz_1 + vz_2)$

---

a, b sind <u>teilerfremd</u> oder <u>relativ prim</u> $:\Leftrightarrow ggT(a,b) = 1$

Satz Seien $a, b, c \in \mathbb{N}$. Wir nehmen an, dass $a \mid b \cdot c$ und $ggT(a,b) = 1$. Dann gilt $a \mid c$.

Beweis] Da ggT $(a,b) = 1$, gibt es $u,v \in \mathbb{Z}$, sodass

$1 = u \cdot a + v \cdot b$ multipl. mit c

Also $c = \underbrace{uac}_{a\text{l}.} + \underbrace{vbc}_{a\text{l}.}$ } ein Vielfaches von a

Also gilt $a \mid c$

Def: Seien $a,b \in \mathbb{Z} \setminus \{0\}$

$kgV(a,b) := \min \{ v \in \mathbb{N} : a \mid v \text{ und } b \mid v \}$

$kgV(a,b) \leq |a| \cdot |b|$

Satz Seien $a,b \in \mathbb{Z} \setminus \{0\}$, sei $s \in \mathbb{Z}$ so, dass $a \mid s$ und $b \mid s$

Dann gilt $kgV(a,b) \mid s$.

Bew] $s = q \cdot kgV(a,b) + r$ mit $q \in \mathbb{Z}$ und $r \in \{0, \dots, kgV(a,b) - 1\}$

$r = s - q \cdot kgV(a,b)$. Dann ist r Vielfaches von a und von b. Somit $r = 0$.