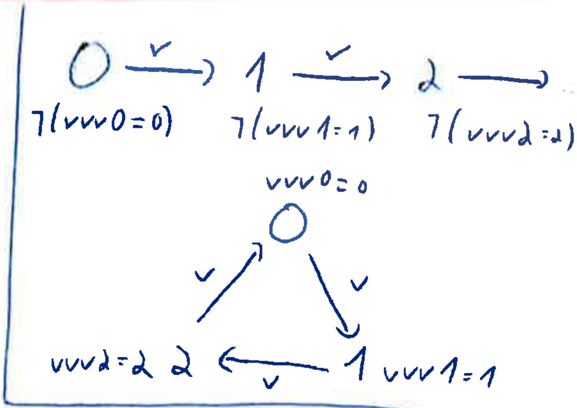
Vorlesung 5, 22. Okt. 2018

"Die natürlichen Zahlen I"



Peano (1888): "Was sind und was sollen die Zahlen?"

Idee: Auch die natürliche Zahlen, und alle ihre Eigenschaften, sollen über die Mengenlehre definiert werden.

Vorsicht: Obwohl Sie alle schon wissen, was die natürliche Zahlen sind, wollen wir diese rein axiomatisch einführen.

Definition (Peano Axiome)

Die natürlichen Zahlen (mit Null) bilden eine Menge $\mathbb{N}_0$ für die es ein Element $\boxed{0 \in \mathbb{N}_0}$ und eine Funktion

$$\boxed{\nu : \mathbb{N}_0 \longrightarrow \mathbb{N} = \mathbb{N}_0 \setminus \{0\}}$$

so gilt, dass

Nachfolgerfunktion
$\nu(n)$ = Nachfolger von n

$\boxed{PA1:}$ ν ist injektiv

$\boxed{PA2:}$ $N \subset \mathbb{N}_0$ so, dass $0 \in N$ und $(\forall n \in N) \Rightarrow (\nu(n) \in N)$ gilt. Dann ist $N = \mathbb{N}_0$

Dies ist das Induktionsaxiom.

Proposition 5.1 ν ist bijektiv

Tippfehler: bijective auf N (nicht N_0)

Beweis: Es sei $N = \{ n \in \mathbb{N}_0 \mid \exists n' \in \mathbb{N}_0 \text{ mit } \nu(n') = n \} \cup \{0\}$

Dann ist $N = \mathrm{im}(\nu) \cup \{0\}$ und wegen PA2 folgt $N = \mathbb{N}_0$. $\Rightarrow \mathrm{im}(\nu) = \mathbb{N}$, also ist ν surjektiv.

ν ist injektiv per Definition. $\square$

Bemerkung 5.2 Wir kommen in der letzten Vorlesung darauf zurück, aber man muss eigentlich zeigen, dass $\mathbb{N}$ existiert. Siehe aus [AE06, Bemerkungen 5.2]

Beispiel 5.3 Schreibe $0 = \emptyset$ und setze $\underset{\nu(n)}{\overset{\shortparallel}{n+1}} = \{0, \dots, n\}$ ~~$n+1 = \{\dots\}$~~. Dann ist für alle [illegible]

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

$$\emptyset \quad \{\emptyset\} \quad \{\emptyset, \{\emptyset\}\} \quad \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \quad \dots$$

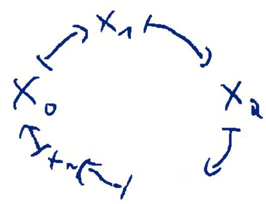
Wir schreiben $1 = \nu(0)$, $2 = \nu(\nu(0))$, $3 = \nu(\nu(\nu(0)))$ etc.

Proposition 5.4 $\mathbb{N}_0$ ist nicht endlich

Beweis: Angenommen $\mathbb{N}_0 = \{ \underset{0}{\overset{\shortparallel}{x_0}}, \dots, x_n \}$ und

$$x_0 \overset{\nu}{\longmapsto} x_1 \longmapsto \dots \overset{\nu}{\longmapsto} x_n$$

Dann muss $\nu(x_n) = x_0$ sein, da ν injektiv ist.

$\rightsquigarrow$ 

Aber das ist ein Widerspruch dazu, dass $\nu : \mathbb{N}_0 \longrightarrow \mathbb{N}$ gilt. $\square$

Theorem 5.5 (Peano)

Auf $\mathbb{N}$ gibt es zwei eindeutige Verknüpfungen $+$ (Addition), $\cdot$ (Multiplikation) und eine Ordnung $\leq$ (natürliche oder Zählordnung) so, dass:

a) $+$ ist assoziativ, kommutativ und 0 ist Einheit

b) $\cdot$ ist assoziativ, kommutativ und 1 ist Einheit

c) Es gilt $\forall\, l, m, n \in \mathbb{N}_0 \quad (l+m) \cdot n = l \cdot n + m \cdot n$ "Distributiv"

d) $0 \cdot n = 0$

e) $(\mathbb{N}_0, \leq)$ ist total geordnet mit $0 = \min(\mathbb{N}_0)$

f) Für $n \in \mathbb{N}_0$ $\nexists\, k \in \mathbb{N}_0$ so, dass $n < k < n+1$.

g) $\forall\, m, n \in \mathbb{N}_0$: $\quad m \leq n \iff \exists\, d \in \mathbb{N}_0$ mit $m + d = n$
$\quad m < n \iff \exists\, d \in \mathbb{N}$ mit $m + d = n$

d ist eindeutig und heißt Differenz.

h) $\forall\, m, n \in \mathbb{N}_0$: $\quad m \leq n \iff m + l \leq n + l$
$\quad m < n \iff m + l < n + l \quad \forall\, l \in \mathbb{N}_0$

i) Für $m, n \in \mathbb{N}$ ist $m \cdot n \in \mathbb{N}$ $\quad (m \cdot n = 0 \iff (m=0) \vee (n=0))$

j) $\forall\, m, n \in \mathbb{N}_0$: $\quad m \leq n \iff m \cdot l \leq n \cdot l$
$\quad m < n \iff m \cdot l < n \cdot l \quad \forall\, l \in \mathbb{N}$

Beweis: Wir beweisen nur a), für alle anderen siehe z.B. die Referenz in [AE06, Theorem 5.5].

Der Punkt ist alles hinzuschreiben, ohne die verbotenen Regeln zu verwenden ☺

i) Angenommen $\circledast : \mathbb{N}_0 \times \mathbb{N}_0 \longrightarrow \mathbb{N}_0$ ist eine kommutative Verknüpfung, welche

$0 \otimes 0 = 0 \quad , \quad n \otimes 1 = \nu(n) \; ; m \otimes \nu(m) = \nu(m \otimes m)$
$\forall m,n \in \mathbb{N}_0$ erfüllt. Betrachte (*)

$$N = \{ n \in \mathbb{N}_0 \mid 0 \otimes n = n \}$$

Dann gilt $0 \in N$, und $n \in N \Rightarrow 0 \otimes \nu(n) = \nu(0 \otimes n) = \nu(n)$
Also ist $\nu(n) \in N \overset{PA2}{\Longrightarrow} N = \mathbb{N}_0$, d.h. $0 \otimes n = n \quad \forall n \in \mathbb{N}_0$

ii) Sei $\boxed{*}$ eine weitere kommutative Verknüpfung, welche (*) erfüllt. Setze für $n \in \mathbb{N}_0$ fest

$$M_n = \{ m \in \mathbb{N}_0 \mid m \otimes n = m \boxed{*} n \}$$

Es folgt $0 \in M_n$, und sei $m \in M_n$. Dann

$$\nu(n \otimes m) = \nu(m \boxed{*} n) = \nu(n \boxed{*} m)$$

also

$$\nu(m) \otimes n = n \otimes \nu(m) = n \boxed{*} \nu(m) = \nu(m) \boxed{*} n$$

$\Rightarrow \nu(m) \in M_n \overset{PA2}{\Longrightarrow} M_n = \mathbb{N}_0 \quad \forall n \in \mathbb{N}_0$ ~~also~~

Also $\otimes = \boxed{*}$, da $n \in \mathbb{N}_0$ beliebig war.

Es gilt nur eine kommutative Verknüpfung mit (*) (☆)

iii) Konstruiere $+ : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ mit (*) welche kommutativ ist. Dazu setze

$$N = \{ n \in \mathbb{N}_0 \mid \exists \varphi_n : \mathbb{N}_0 \to \mathbb{N}_0 \text{ mit } \varphi_n(0) = \nu(n) \text{ und } \varphi_n(\nu(m)) = \nu(\varphi_n(m)) \; \forall m \in \mathbb{N}_0 \}$$

Mit $\varphi_0 = \nu$ folgt $0 \in N$. Sei nun $n \in N$, dann setze

$$\psi : \mathbb{N}_0 \to \mathbb{N}_0 \quad , \quad m \longmapsto \nu(\varphi_n(m))$$

Dann gilt $\psi(0) = \nu(\varphi_n(0)) = \nu(\nu(n))$ und

$\varphi(v(m)) = v(\varphi_n(v(m))) = v(v(\varphi_n(m))) = v(\varphi(m))$ $\forall m \in \mathbb{N}_0$

Also $(n \in N) \Rightarrow (v(n) \in N) \overset{PA2}{\Rightarrow} N = \mathbb{N}_0$.

φ_n ist eindeutig: Sei ψ_n eine weitere Abbildung mit denselben Eigenschaften. Dann kann man ~~mit~~ für $M_n = \{m \in \mathbb{N}_0 \mid \varphi_n(m) = \psi_n(m)\}$ und PA2, dass $M_n = \mathbb{N}_0$ gilt. Das bedeutet $\varphi_n = \psi_n$

Tippfehler: "mittels PA2 zeigen"

Also: Für alle $n \in \mathbb{N}_0$ $\exists!$

$\varphi_n : \mathbb{N}_0 \to \mathbb{N}_0$ mit $\varphi_n(0) = v(n)$ und $\varphi_n(v(m)) = v(\varphi_n(m))$ $\forall m \in \mathbb{N}_0$

Definiere

$$+ : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0, \quad n + m = \begin{cases} n, & \text{falls } m = 0, (\square) \\ \varphi_n(m'), & \text{falls } m = v(m'). \end{cases}$$

Dann erfüllt + (*), denn

$$n + 0 = n, \quad n + 1 = n + v(0) = \varphi_n(0) = v(n) = v(n+0)$$

$$n + v(m) = \varphi_n(m) = \varphi_n(v(m')) = v(\varphi_n(m')) = v(n+m)$$

für $n \in \mathbb{N}_0$, $m \in \mathbb{N}$ und $m = v(m')$. Dann ist auch 0 die Einheit bezüglich (+), weil $(\square)$ gilt.

iv) Sei $N_{l,m} = \{n \in \mathbb{N}_0 \mid (l+m)+n = l+(m+n)\}$ für $l, m \in \mathbb{N}_0$ fest. Dann $0 \in N_{l,m}$ und für $n \in N$

$(l+m)+v(n) = v((l+m)+n) = v(l+(m+n)) = l + v(m+n)$

$= l + (m + v(n))$. Also folgt $v(n) \in N \overset{PA2}{\Rightarrow} N = \mathbb{N}_0$

$\Rightarrow$ Assoziativität, da l, m beliebig waren.

v) Kommutativität: Betrachte

$$N = \{ n \in \mathbb{N}_0 \mid n+1 = 1+n \}$$

Wie vorher folgt $0 \in N$ und für $n \in N$

$$\nu(n)+1 = \nu(\nu(n)) = \nu(n+1) = \nu(1+n) = 1+\nu(n)$$

Also $\nu(n) \in N \overset{PA2}{\Rightarrow} N = \mathbb{N}_0$.

Dasselbe Argument funktioniert für

$$M_n = \{ m \in \mathbb{N}_0 \mid m+n = n+m \}$$

für alle $n \in \mathbb{N}_0$. Daraus folgt dann Kommutativität.

Zusammengefasst: $\exists$ die Addition durch (iii), welche Assoziativ ist bei (iv) und kommutativ bei (v). 0 ist Einheit, durch Konstruktion und + ist eindeutig durch (☆). $\boxed{\text{q.e.d.}}$

Beispiel 5.6

+ = die vertraute Addition

$\cdot$ = die vertraute Multiplikation (schreibe auch $mn = m \cdot n$)

$\leq$ = die vertraute Ordnung, bestimmt durch $n < n+1 = \nu(n) \; \forall n \in \mathbb{N}_0$

$$0 < 1 < \nu(1) = 2 < \nu(2) = 3 < \ldots$$

Proposition 5.7 Für $m, n \in \mathbb{N}_0$, $k \in \mathbb{N}$ mit $mk = nk$ gilt $m = n$ "Kürzen"

Beweis Wegen (j) von Theorem 5.5 $\square$

$m \in \mathbb{N}$ heißt Teiler von n, falls es $k \in \mathbb{N}$ gibt so, dass $mk = n$. Schreibe in diesem Fall $m | n$. k heißt in diesem Fall Quotient und wird mit n/m bezeichnet.

Theorem 5.8 (Division mit Rest, aka Euklids Algorithmus)
Zu $m \in \mathbb{N}$ und $n \in \mathbb{N}_0$ $\exists !$ $k \in \mathbb{N}$ und $l \in \mathbb{N}$ mit

$$n = km + l \quad \text{für } l < m$$

Tippfehler: Beide, k und l, sind aus N_0

Beweis i) Existenz. Setze

$$N = \{n \in \mathbb{N}_0 \mid \exists k, l \text{ mit } n = km + l, \; l < m\}$$

Wegen $0 = 0 \cdot m + 0$ ist $0 \in N$. Also sei $n \in N$, und wähle k, l mit $n = km + l$, $l < m$. Also $n + 1 = km + (l+1)$. Ist $l + 1 < m$, so folgt $n + 1 \in N$. Ist $l + 1 = m$, dann ist $n + 1 = (k+1)m$ und $n + 1 \in N$. Wegen PAα folgt $N = \mathbb{N}_0$.

ii) Eindeutigkeit. Seien k, k', l, l' gegeben so, dass

$$km + l = k'm + l' \qquad l, l' < m$$

Angenommen $l \leq l'$, dann $k'm + l' = km + l \leq km + l'$, also $k'm \leq km$, also $k' \leq k$. Aber wegen $l' < m$ folgt

$$km \leq k'm + l < k'm + m = (k'+1)m \implies k < k' + 1$$

Tippfehler: l' nicht l

$\implies$ Wegen $k' \leq k$ folgt also $k = k'$ und damit $l = l'$ $\square$