Wiederholung

Satz 0.8: $\forall m, n \in \mathbb{N}$ gilt genau eine der folgenden drei Aussagen:

(i) $m = n$

(ii) $\exists!\, l \in \mathbb{N}^+$ sodass $m = n + l$

(iii) $\exists!\, l \in \mathbb{N}^+$ sodass $n = m + l$

Beweis: „höchstens eine" - Aufgabe

„mindestens eine": Es sei M die Menge aller Zahlen a sodass mindestens eine der drei Aussagen gilt für $n = a$.

Es ist $0 \in M$, da wenn $m = 0$ gilt (i)
wenn $m \neq 0$ gilt (ii) mit $l = m$.

Es sei $a \in M$

Dann gilt mindestens einer der drei Fälle

Fall 1: $m = a$

Dann ist $a^* = m^* = m + 1$ (L 0.2 (i))

und für $n = a^*$ gilt (iii) mit $l = 1$.

Fall 2: $\exists!\, k \in \mathbb{N}^+$ sodass $m = a + k$

Es gibt ein $l \in \mathbb{N}$ sodass $k = l^*$ (S 0.1)

und $a^* + l = a + l^*$ (K 0.4)

$= a + k = m$

Wenn $l \neq 0$:
Die Eindeutigkeit von l folgt aus K 0.7

und so gilt (ii) für $n = a^*$

Wenn $l = 0$, gilt (i) für $n = a^*$

Fall 3: $\exists!\, k \in \mathbb{N}^+$ sodass $a = m + k$

Dann ist $a^* = (m+k)^*$

$= m + k^*$ $\quad (A_2)$

und $k^* \in \mathbb{N}^+$ $\quad (P_3)$

die Eindeutigkeit von $l = k^*$ folgt aus K 0.7

also gilt (iii) für $n = a^*$ mit $l = k^*$.

In allen Fällen ist $a^* \in M$, also ist $M = \mathbb{N}$ (P_5) $\square$

Multiplikation

Def: Wir definieren die binäre Operation $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ rekursiv durch

(M_1) $m \cdot 0 := 0$ $\quad \forall m \in \mathbb{N}$

(M_2) $m \cdot n^* := (m \cdot n) + m$ $\quad \forall m, n \in \mathbb{N}$

Eigenschaften der Multiplikation:

Satz 0.9: $\forall\, l, m, n \in \mathbb{N}$ gilt

(i) $0 \cdot n = n \cdot 0 = 0$

(ii) $1 \cdot n = n \cdot 1 = n$

(iii) $(l \cdot m) \cdot n = l \cdot (m \cdot n)$ (Assoziativität)

(iv) $(l + m) \cdot n = (l \cdot n) + (m \cdot n)$ (Distributivität)

(v) $m \cdot n = n \cdot m$ (Kommutativität)

(vi) Wenn $n \neq 0$ und $l \cdot n = m \cdot n$, dann ist $l = m$ (Kürzungsregel)

(vii) Wenn $m \cdot n = 0$, dann ist $m = 0$ oder $n = 0$

Beweis: (Übungs-)Aufgabe

Die natürliche Ordnungsrelation

Def: Wir definieren die binäre Relation „$\leq$" auf $\mathbb{N} \times \mathbb{N}$ durch

$$m \leq n \Leftrightarrow \exists\, l \in \mathbb{N} \text{ sodass } n = m + l$$

wir sagen $m < n \Leftrightarrow m \leq n$ und $m \neq n$

wir sagen $m \geq n$ (bzw. $m > n$) $\Leftrightarrow n \leq m$ (bzw. $n < m$).

Lemma 0.10: $\forall\, m, n \in \mathbb{N}$ gilt

$$m < n \Leftrightarrow \exists\, l \in \mathbb{N}^+ \text{ sodass } n = m + l$$

Beweis: Aufgabe

Satz 0.11: $\forall\, m, n \in \mathbb{N}$ gilt genau eine der folgenden drei Aussagen:

(i) $m = n$

(ii) $m < n$

(iii) $m > n$

Beweis: Mit Hilfe des Lemmas 0.10 folgt das direkt aus Satz 0.8 $\square$

„$\leq$" ist eine partielle Ordnung (Satz 0.12)

Aus Satz 0.11 folgt, dass „$\leq$" sogar eine lineare Ordnung ist.

Satz 0.12: $\forall\, l, m, n \in \mathbb{N}$ gilt

(i) $n \leq n$ (reflexiv)

(ii) $m \leq n$ und $n \leq m \Rightarrow m = n$ (anti-symmetrisch)

(iii) $l \leq m$ und $m \leq n \Rightarrow l \leq n$ (transitiv)

Beweis: Aufgabe.

Bemerkung: (iii) lässt sich auch mit „<" formulieren (i) und (ii) aber nicht.

Wie verhält sich „≤" (bzw. „<") mit „+" und „·"?

Satz 0.13: $\forall k, l, m, n \in \mathbb{N}$ gilt

(i) $n \leq n+m$	Wenn $m \neq 0$ ist $n < n+m$
(ii) $0 \leq n$	$0 < n \iff n \neq 0$
(iii) $l \leq m \iff l+n \leq m+n$	$l < m \iff l+n < m+n$
(iv) $l \leq m \Rightarrow l \cdot n \leq m \cdot n$	$l < m$ <u>und</u> $n \neq 0 \Rightarrow l \cdot n < m \cdot n$
(v) Wenn $n \neq 0$ gilt $l \cdot n \leq m \cdot n \Rightarrow l \leq m$	$l \cdot n < m \cdot n \Rightarrow l < m$

Beweis: Aufgabe (meist ganz einfach)

Der folgende Satz ist für uns so „offensichtlich", dass wir seine Notwendigkeit leicht übersehen können.

Satz 0.14: $\forall n \in \mathbb{N} \; \nexists m \in \mathbb{N}$ mit $n < m < n+1$

Bemerkung: „$x < y < z$" ist eine Abkürzung von „$x < y$ und $y < z$"

Analog sind „$x \leq y \leq z$", „$x \leq y < z$" und „$x < y \leq z$".

Beweis: Angenommen es gäbe ein solches m.

Dann existieren $k, l \in \mathbb{N}^+$ sodass $m = n + k$

$n+1 = m + l$

Also ist $n + 1 = (n+k) + l$

$= n + (k+l)$ (S 0.3)

$\Rightarrow \quad 1 = k + l$ (K 0.7)

Da $k, l \in \mathbb{N}^+$, $\exists\, i, j \in \mathbb{N}$ sodass $k = i^*$, $l = j^*$ (S 0.1)

Also ist $1 = i^* + j^*$

$0^* = (i^* + j)^*$ (A_2)

$= (i + j^*)^*$ (K 0.4)

$= ((i+j)^*)^*$ (A_2)

$\Rightarrow \quad 0 = (i+j)^*$ (P_4)

$\lightning$ (P_3) $\square$

Der folgende Satz ist eine sehr nützliche Form des Prinzips der vollständigen Induktion

Satz 0.15 (Satz des kleinsten Elements):

Sei $M \subseteq \mathbb{N}$ eine beliebige nichtleere Teilmenge

Dann besitzt M ein <u>kleinstes Element</u>,

d.h. $\exists\, a \in M$ sodass $\forall n \in M$ gilt $a \leq n$.

Beweis: Angenommen es gäbe <u>kein</u> kleinstes Element

Sei $L = \{ m \in \mathbb{N}$ sodass $m \leq n \quad \forall n \in M \}$ ← schlaue Zeile

Dann ist $L \cap M = \emptyset$ (ein Element in $L \cap M$ wäre ein kleinstes Element in M)

Aber $0 \in L$ $(\leq 0.13\ (ii))$

und angenommen $k \in L$, dann ist $k \notin M$

also gilt $\forall n \in M$, $k \leq n$ <u>und</u> $k \neq n$

d.h. $k < n$

also gilt auch $n \not< k+1$ (≤ 0.14)

Daher gilt $k+1 = n$ <u>oder</u> $k+1 < n$ (≤ 0.11)

d.h. $k+1 \leq n$

also ist $k^* = k+1 \in L$ und es ist $L = \mathbb{N}$ (P_5)

Aber da $L \cap M = \emptyset$, ist dann M leer $\lightning$ $\square$

Bemerkung: Das kleinste Element ist auch eindeutig (Beweis mit Hilfe des Satzes 0.12 (ii)).

Erweiterte Zahlenmengen

Die ganzen Zahlen

Def: Die Menge $\mathbb{Z}$ der ganzen Zahlen ist die Menge der Äquivalenzklassen in $\mathbb{N} \times \mathbb{N}$ bezüglich der Relation

$$(k,\ell) \sim_{\mathbb{Z}} (m,n) \iff k+n = m+\ell$$

Intuition: (m,n) entspricht $m-n$

Aufgabe: Überzeugen Sie sich, dass „$\sim_{\mathbb{Z}}$" tatsächlich eine Äquivalenzrelation ist, d.h.

(i) $x \sim_{\mathbb{Z}} x \quad \forall x \in \mathbb{N}^2$ (reflexiv)

(ii) $x \sim_{\mathbb{Z}} y \Rightarrow y \sim_{\mathbb{Z}} x$ (symmetrisch)

(iii) $x \sim_{\mathbb{Z}} y$ und $y \sim_{\mathbb{Z}} z \Rightarrow x \sim z$ (transitiv)

Def: wir bezeichnen mit $\overline{(m,n)}$ die Äquivalenzklasse

$$\{(k,\ell) \in \mathbb{N} \times \mathbb{N} : (k,\ell) \sim_{\mathbb{Z}} (m,n)\}$$

also ist $\mathbb{Z} = \{\overline{(m,n)} : m,n \in \mathbb{N}\}$

Wie erweitern wir Addition und Multiplikation?

Def: wir definieren Addition und Multiplikation auf $\mathbb{Z}$ durch

(i) $\overline{(k,\ell)} + \overline{(m,n)} := \overline{(k+m, \ell+n)}$

(ii) $\overline{(k,\ell)} \cdot \overline{(m,n)} := \overline{((k\cdot m)+(\ell\cdot n), (k\cdot n)+(\ell\cdot m))}$

Aufgabe: Überzeugen Sie sich, dass Addition und Multiplikation auf $\mathbb{Z}$ wohl-definiert sind. Welche Eigenschaften von „+" und „·", die wir für $\mathbb{N}$ bewiesen haben, gelten auch in $\mathbb{Z}$?

Die rationellen Zahlen

Def: $\mathbb{Z}^\times := \mathbb{Z} \setminus \{\overline{(0,0)}\}$

Def: Die Menge $\mathbb{Q}$ der rationellen Zahlen ist die Menge der Äquivalenzklassen in $\mathbb{Z} \times \mathbb{Z}^\times$ bezüglich der Relation

$$(p,q) \sim_{\mathbb{Q}} (r,s) \Leftrightarrow p \cdot s = r \cdot q$$

Intuition: (p,q) entspricht p/q

Def: Wir bezeichnen mit $\widehat{(p,q)}$ die Äquivalenzklasse

$$\{(r,s) \in \mathbb{Z} \times \mathbb{Z}^\times : (r,s) \sim_{\mathbb{Q}} (p,q)\}$$

also ist $\mathbb{Q} = \{\widehat{(p,q)} : p \in \mathbb{Z},\ q \in \mathbb{Z}^\times\}$

Bemerkung: Um z.B. $\frac{-2}{3}$ zu bezeichnen, schreiben wir

$$\widehat{\left(\overline{(0,2)}, \overline{(3,0)}\right)}$$

deswegen würden wir sobald möglich Notationsabkürzungen definieren.