1.8 Vollständige Induktion

Die Menge der natürlichen Zahlen ist wie folgt definiert.

(1) $0 \in \mathbb{N}$

(2) $\forall\, n \in \mathbb{N} : n' \in \mathbb{N}$

(3) $\forall\, n \in \mathbb{N} : n' \neq 0$

(4) $\forall\, n, m \in \mathbb{N} : (n' = m' \implies n = m)$

(5) $\forall\, X : (0 \in X \wedge \forall\, n \in \mathbb{N} : (n \in X \implies n' \in X)) \implies \mathbb{N} \subseteq X$

Hierbei bezeichnet n' den Nachfolger von $n \in \mathbb{N}$.
Hieraus leitet sich das Prinzip der vollständigen Induktion ab. Falls nun

- Die Aussage $A(0)$ wahr ist und
- Für jedes $n \in \mathbb{N}$ gilt: $A(n)$ ist wahr $\implies$ $A(n+1)$ ist wahr,

so ist $A(n)$ wahr für jedes $n \in \mathbb{N}$.

Satz 1.1. *für alle $n \in \mathbb{N}$ ist die Summe der ersten n ungeraden Zahlen n^2:*

$$\sum_{i=1}^{n} (2i - 1) = n^2$$

Beweis mittels vollständiger Induktion: Induktionsanfang ($n = 0$):

$$\sum_{i=1}^{0} (2i - 1) = 0 = 0^2$$

gilt.
Induktionsschluss ($n \to n + 1$):
Für ein beliebiges, aber festes $n \in \mathbb{N}$ gelte $\sum_{i=1}^{n}(2i - 1) = n^2$. Daraus folgt

$$\begin{aligned} \sum_{i=1}^{n+1} (2i - 1) &= \sum_{i=1}^{n} (2i - 1) + 2(n + 1) - 1 \\ &= n^2 + 2n + 1 \\ &= (n + 1)^2 \end{aligned}$$

□

Satz 1.2. *Für alle $n \in \mathbb{N}$ und $q \in \mathbb{R} \setminus \{1\}$ ist die geometrische Summe*

$$\sum_{i=0}^{n-1} q^i = \frac{q^n - 1}{q - 1}$$

Beweis mittels vollständiger Induktion: Induktionsanfang ($n = 0$):

$$\sum_{i=0}^{-1} q^i = 0 = \frac{q^0 - 1}{q - 1}$$

Induktionsschluss ($n \to n+1$):
Für ein beliebiges, aber festes $n \in \mathbb{N}$ gelte

$$\sum_{i=0}^{n-1} q^i = \frac{q^n - 1}{q - 1}$$

Dann gilt:

$$\begin{aligned}
\sum_{i=0}^{n} q^i &= \sum_{i=0}^{n-1} q^i + q^n \\
&= \frac{q^n - 1}{q - 1} + q^n \\
&= \frac{q^n - 1}{q - 1} + \frac{q^n(q-1)}{q - 1} \\
&= \frac{q^n - 1 + q^{n+1} - q^n}{q - 1} \\
&= \frac{q^{n+1} - 1}{q - 1}
\end{aligned}$$

□

1.9 Verallgemeinerte Induktion

(i) Es sei $n_0 \in \mathbb{Z}$ und für jede ganze Zahl $n \geq n_0$ sei $A(n)$ eine Aussage, die wahr oder falsch ist. Falls nun

- die Aussage $A(n_0)$ wahr ist und
- für alle $n \geq n_0$ gilt $A(n)$ ist wahr $\implies$ $A(n+1)$ ist wahr,

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

(ii) Induktionsprinzip zweiter Art („starke Induktion“): Es sei $n_0 \in \mathbb{Z}$ und für jede ganze Zahl $n \geq n_0$ sei $A(n)$ eine Aussage, die wahr oder falsch ist. Falls nun

- die Annahme $A(n_0)$ wahr ist und
- Für alle $n \geq n_0$ gilt:

$$\big(A(k) \text{ ist wahr } \forall\, n_0 \leq k \leq n \implies A(n+1) \text{ ist wahr}\big)$$

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

Satz 1.3. *Jede nicht-leere Teilmenge $X \subseteq N$ enthält ein kleinstes Element.*

Beweis. Es sei $X \subseteq \mathbb{N}$ und X enthalte kein kleinstes Element. Wir zeigen mittels Induktionsprinzip 2. Art, dass $X = \emptyset$, d. h. $n \notin X \; \forall n \in \mathbb{N}$
Induktionsanfang ($n = 0$): $0 \notin X$, da sonst 0 kleinstes Element von X.
Induktionsschluss ($n \to n+1$): Für ein beliebiges, aber festes $n \in \mathbb{N}$ gelte: $k \notin X \; \forall k \leq n$.
Dann ist $n + 1 \notin X$, da sonst $(n+1)$ kleinstes Element von X wäre. □

2 Darstellung ganzer Zahlen

2.1 Modulo-Rechnung

Satz 2.1. *Zu* $a \in \mathbb{Z}$ *und* $m \in \mathbb{N}_{\geq 1}$ *gibt es eindeutig bestimmte Zahlen* $p \in \mathbb{Z}$ *und* $q \in \{0, \dots, n-1\}$ *mit*

$$a = p \cdot m + q$$

Die Zahl q ist der Rest bei Division von a durch m. Wir schreiben

$$q = a \mod m$$

Beweis. Existenz: Setze $p := \lfloor \frac{a}{m} \rfloor \in \mathbb{Z}$ und $q := a - p \cdot m \in \{0, \dots, m-1\}$.
Eindeutigkeit: Es seien $p, p' \in \mathbb{Z}$ und $q, q' \in \{0, \dots, m-1\}$ mit

$$a = p \cdot m + q = p' \cdot m + q'$$

$$\implies \underbrace{(p - p')}_{\in \mathbb{Z}} \cdot m = \underbrace{(q' - q)}_{\in \{-m+1, \dots, m-1\}} \implies q - q' = 0, p - p' = 0$$

□

Die Modulo-Operation ist mit Addition und Multiplikation verträglich, d. h. für $a, b \in Z$ und $m \in \mathbb{N}_{\geq 1}$ gilt

$$(a + b) \mod m = \big((a \mod m) + (b \mod m)\big) \mod m$$

und

$$(a \cdot b) \mod m = \big((a \mod m) \cdot (b \mod m)\big) \mod m$$

Beweis. schreibe $a = p \cdot m + q, b = p' \cdot m + q'$ mit $q, q' \in \{0, \dots, m-1\}$. Dann gilt

$$(a + b) \mod m = \big((p + p') \cdot m + (q + q')\big) \mod m$$

Analog für Multiplikation. □

Bemerkung. Die Menge $\{0, 1, \dots, m-1\}$ bildet gemeinsam mit Addition und Multiplikation mod m den Ring $\mathbb{Z}_m$. Ist m prim, so ist $\mathbb{Z}_m$ sogar ein Körper.

2.2 Zahldarstellung

Satz 2.2. *es seien $b \in \mathbb{N}_{\geq 2}$ und $n \in \mathbb{N}_{\geq 1}$. Für $\ell := \lfloor \log_b n + 1 \rfloor$ existieren eindeutig bestimmte Zahlen $z_i \in \{0, \dots, b-1\}$ für $i = 0, \dots, \ell - 1$ mit*

$$n = \sum_{i=0}^{\ell-1} z_i \cdot b^i \text{ und } z_{\ell-1} \neq 0$$

Bemerkung. Das Wort $z_{\ell-1} \dots z_0$ heißt die b-adische Darstellung von n. Man schreibt manchmal auch

$$n = (n_{\ell-1} \dots z_0)_b$$

Beispiel. $(24)_{10} = (11000)_2 = (220)_3 = (120)_4 = (44)_5 = (40)_6 = (33)_7 = (30)_8$
$(986)_{10} = (3\ 13\ 10)_{16} = 0x3da$

Beweis zur Existenz der b-adischen Darstellung. Induktionsanfang: Für $n \in \{1, \dots, b-1\}$ gilt $\sum_{i=0}^{0} z_i b^i$ mit $z_0 := n \neq 0$
Induktionsschritt: Für ein beliebiges, aber festes $n \in \mathbb{N}_{\geq b-1}$ gebe es für alle $k \leq n$ eine solche Darstellung. Konstruiere damit Darstellung für $n+1$:
Es sei $k := \lfloor \frac{n+1}{b} \rfloor \leq n$ und $\ell' := \lfloor \log_b k \rfloor + 1$. Also gibt es Darstellung

$$k = \sum_{i=0}^{\ell'-1} z_i' b^i$$

mit $z_i' \in \{0, \dots, b-1\}$ und $z_{\ell-1}' \neq 0$. Dann ist $\ell := \lfloor \log_b(n+1) \rfloor + 1 = \ell' + 1$
Setze $z_i := z_{i-1}'$ für $i = 1, \dots, \ell - 1$ und $z_0 := (n+1) \mod b$. Dann ist $n + 1 = k \cdot b + z_0 = \sum_{i=0}^{\ell'-1} z_i' b^{i+1} + z_0$. □