

Ein fundamentales mathematisches Beweisprinzip ist die *vollständige Induktion*:

Sei $p : \mathbb{N}_0 \rightarrow \mathbb{B}$ ein totales Prädikat.

Falls

1. $p(0)$ (*Induktionsanfang*) und
2. für beliebiges $n \in \mathbb{N}_0$ gilt der *Induktionsschluss*:
“Falls $p(n)$ (Induktionsvoraussetzung), dann $p(n + 1)$.”

Dann: $p(n)$ für alle $n \in \mathbb{N}_0$.

Die vollständige Induktion (“nach n ”) ermöglicht es zu beweisen, dass eine Aussage (“ p ”) für alle $n \in \mathbb{N}_0$ gilt.

Beispiel:

- Sei $p(n) : \Leftrightarrow \sum_{i=0}^n i = \frac{n \cdot (n+1)}{2}$
- Zu beweisen: Gültigkeit von $p(n)$ für alle $n \in \mathbb{N}_0$
- Induktionsanfang:

- Zu zeigen, dass $p(0)$, d.h. $\sum_{i=0}^0 i = \frac{0 \cdot (0+1)}{2}$

$$\sum_{i=0}^0 i = 0 \qquad \frac{0 \cdot (0+1)}{2} = 0 \quad \checkmark$$

- Für den Induktionsschluss können wir für $n \in \mathbb{N}_0$ als Induktionsvoraussetzung $p(n)$, d.h. $\sum_{i=0}^n i = \frac{n \cdot (n+1)}{2}$ annehmen.
- Zu zeigen ist die Gültigkeit von $p(n+1)$, d.h.

$$\sum_{i=0}^{n+1} i = \frac{(n+1) \cdot (n+1+1)}{2}$$

Beweis (unter Verwendung der Induktionsvoraussetzung):

$$\begin{aligned}\sum_{i=0}^{n+1} i &= 0 + 1 + \dots + n + (n + 1) \\ &= \sum_{i=0}^n i + (n + 1) \\ &= \frac{n \cdot (n + 1)}{2} + n + 1 \\ &= \frac{n \cdot (n + 1) + 2 \cdot (n + 1)}{2} \\ &= \frac{(n + 1) \cdot (n + 2)}{2} \\ &= \frac{(n + 1) \cdot (n + 1 + 1)}{2} \quad \checkmark\end{aligned}$$

Warum ist dieses Beweisprinzip gültig?

Wie kann man sicher sein, dass p für alle Zahlen aus \mathbb{N}_0 gilt, wenn $p(0)$ gilt und man für ein beliebiges festes $n \in \mathbb{N}_0$ von $p(n)$ auf $p(n + 1)$ schließen kann?

Die Menge \mathbb{N}_0 lässt sich durch folgende Regeln *induktiv definieren*:

1. $0 \in \mathbb{N}_0$
2. Ist $n \in \mathbb{N}_0$ dann ist auch $n + 1 \in \mathbb{N}_0$.
3. Außer den Elementen gemäß Regeln 1 und 2 enthält \mathbb{N}_0 keine weiteren Objekte.

Die Elemente der Menge \mathbb{N}_0 werden gemäß dieser induktiven Definition der Reihe nach “konstruiert”:

- Zunächst wird 0 gemäß Regel 1 als Element von \mathbb{N}_0 festgelegt.
- Wegen Regel 2 ist dann $0 + 1 = 1$ Element von \mathbb{N}_0 .
- Erneute Anwendung von Regel 2 ergibt $1 + 1 = 2$ als Element von \mathbb{N}_0 usw.

“ $n + 1$ ” können wir auch die *Nachfolger-Funktion* nennen:

$$\begin{array}{l} \text{successor :} \quad \mathbb{N}_0 \quad \rightarrow \quad \mathbb{N}_0 \\ \text{mit} \quad \quad \quad n \quad \mapsto \quad n + 1 \end{array}$$

Jede Zahl aus \mathbb{N}_0 wird erzeugt durch endlich-oft-malige Anwendung von *successor* auf 0, z.B.:

$$3 = \text{successor}(\text{successor}(\text{successor}(0))), \text{ also gilt: } 3 \in \mathbb{N}_0$$

- Dieser “induktive Aufbau” der Menge \mathbb{N}_0 ist der Grund für die Gültigkeit des Beweisprinzips der vollständigen Induktion.
- Das Prinzip der vollständigen Induktion vollzieht genau diesen Erzeugungsmechanismus der Menge \mathbb{N}_0 nach:
 - Der Induktionsanfang verifiziert $p(0)$.
 - Mit dem Induktionsschluss, angewendet auf $n = 0$, erhält man $p(0 + 1)$, d.h. $p(1)$.
 - Mit einem weiteren Induktionsschluss, angewendet auf $n = 1$, erhält man $p(1 + 1)$, d.h. $p(2)$ usw.
- Da \mathbb{N}_0 nur Elemente enthält, die gemäß der induktiven Definition von \mathbb{N}_0 konstruiert sind, gilt dann also p tatsächlich für alle Zahlen aus \mathbb{N}_0 .

- Eine weitere Konsequenz der induktiven Definition von \mathbb{N}_0 ist die Ermöglichung der *rekursiven Definition* von Abbildungen von \mathbb{N}_0 .
- Die rekursive Definition einer Funktion f mit Definitionsbereich \mathbb{N}_0 bedeutet intuitiv:
 - $f(0)$ wird explizit festgelegt.
 - $f(n + 1)$ für ein beliebiges $n \in \mathbb{N}_0$ wird auf $f(n)$ “zurückgeführt”, d.h. in Abhängigkeit von $f(n)$ definiert.
 - Die Werte der Funktion $f(0), f(1), f(2)$ usw. sind dann wie zuvor erzeugbar, was $f(m)$ für alle $m \in \mathbb{N}_0$ festlegt.

- Die Fakultäts-Funktion $! : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ ist rekursiv definiert wie folgt:
 - $0! = 1$
 - $(n + 1)! = (n + 1) \cdot (n !)$
- Oft wird äquivalent statt der Rückführung von $n + 1$ auf n der Fall $n \neq 0$ auf $n - 1$ zurückgeführt:

$$n! = \begin{cases} 1, & \text{falls } n = 0, \\ n \cdot (n - 1)! & \text{sonst.} \end{cases}$$

- Die Summen-Formel aus dem obigen Beispiel zum Beweis durch vollständige Induktion lässt sich ebenfalls rekursiv definieren:

$$\sum_{i=0}^n i = \begin{cases} 0, & \text{falls } n = 0, \\ \sum_{i=0}^{n-1} i + n & \text{sonst.} \end{cases}$$

- Das Beweisprinzip der vollständigen Induktion eignet sich besonders gut, wenn in der zu beweisenden Aussage rekursiv definierte Abbildungen auftreten.

- Unabhängig von der Gestalt des Summanden lässt sich eine Summenformel grundsätzlich immer rekursiv definieren.
- Sei $a : \mathbb{N} \rightarrow \mathbb{N}$.

$$\sum_{i=0}^n a(i) = \begin{cases} 0, & \text{falls } n = 0, \\ \sum_{i=0}^{n-1} a(i) + a(n) & \text{sonst.} \end{cases}$$

- Folgen haben wir vorher als n -Tupel definiert, also als Elemente aus M^* .
- Hierbei gilt offensichtlich, dass eine Folge der Länge 1 (a) $\in M$ mit ihrem einzigen Element $a \in M$ identisch ist.
- Unter Ausnutzung dieser Eigenschaft können wir Folgen auch induktiv definieren.

- Hilfsfunktionen hierzu ermöglichen das Anfügen eines Elements $a \in M$ an eine Folge $x \in M^*$:
$$\text{postfix} : M^* \times M \rightarrow M^*$$
mit $\text{postfix}(x, a) = x \circ (a)$
- Analog: Das Anfügen einer Folge $x \in M^*$ an ein Element $a \in M$:
$$\text{prefix} : M^* \times M \rightarrow M^*$$
mit $\text{prefix}(a, x) = (a) \circ x$

- Damit kann eine Folge $x \in M^*$, $x = (x_1, \dots, x_n)$ schrittweise aufgebaut werden.
- Ausgehend von der leeren Folge $()$ werden die Elemente x_1, x_2, \dots, x_n angefügt:

$$\begin{aligned}x &= postfix(\dots postfix(postfix(), x_1), x_2), \dots, x_n) \\ &= () \circ (x_1) \circ (x_2) \circ \dots \circ (x_n)\end{aligned}$$

Induktive Definition von M^* :

1. $() \in M^*$
2. Ist $x \in M^*$ und $a \in M$, dann ist *postfix* $(x, a) \in M^*$.

Analoge Definition unter Verwendung von *prefix*:

1. $() \in M^*$
2. Ist $a \in M$ und $x \in M^*$, dann ist *prefix* $(a, x) \in M^*$.

- Da nun Folgen induktiv definiert sind, liegt es nahe, dass wir sehr einfach rekursive Abbildungen über Folgen definieren können.
- $first : M^+ \rightarrow M$ mit $first(prefix(a, x)) = a$
- $rest : M^+ \rightarrow M^*$ mit $rest(prefix(a, x)) = x$
- Die Bedeutung dieser Funktionen ist offensichtlich. Für eine nicht leere Folge (x_1, \dots, x_n) gilt:

$$first(x_1, x_2, \dots, x_n) = x_1$$

$$rest(x_1, x_2, \dots, x_n) = (x_2, \dots, x_n)$$

Die *Projektion* auf Folgen

$$\pi : M^n \times I_n \rightarrow M.$$

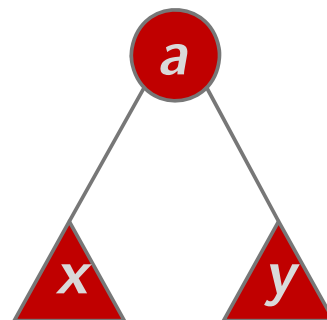
mit $\pi(x, i) = x_i$ können wir nun auch rekursiv definieren, z.B.:

$$\pi(x, i) = \begin{cases} \textit{first}(x), & \text{falls } i = 1, \\ \pi(\textit{rest}(x), i - 1) & \text{sonst.} \end{cases}$$

- Die induktive Struktur von Folgen lässt sich leicht verallgemeinern.
- Jede nicht-leere Folge ist zusammengesetzt aus einem Element $a \in M$ und einer anderen Folge x :
$$y = \text{prefix}(a, x)$$
- Abstrahiert von der konkreten Funktion *prefix*, ist y durch das Paar (a, x) bestimmt, wobei x selbst wieder derartig bestimmt ist.
- Eine Verallgemeinerung kann darin bestehen, dass wir Objekte einführen, die aus einem Element a und mehreren "Resten" bestehen: (a, x, y)
- Hierbei gilt induktiv, dass die "Reste" x und y selbst von der gleichen Art sind.

- Solche Objekte heißen *Binärbäume* (über M).
- Analog zu den Folgen lassen wir den *leeren Baum* zu, den wir mit ε bezeichnen.
- Induktive Definition der Menge $binarytree_M$ über M :
 1. $\varepsilon \in binarytree_M$
 2. Wenn $a \in M$ und $x, y \in binarytree_M$,
dann ist $(a, x, y) \in binarytree_M$.

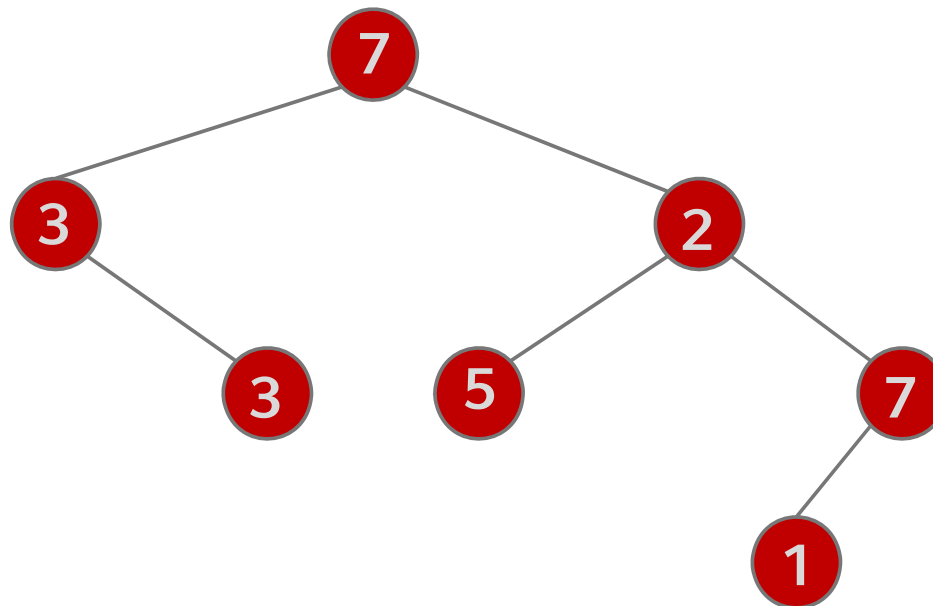
- Hierbei heißt a *Wurzel*, x *linker Teilbaum* und y *rechter Teilbaum* eines Binärbaumes (a, x, y) .
- Ein Binärbaum der Gestalt $(a, \varepsilon, \varepsilon)$ heißt *Blatt*.
- Ein von ε verschiedener Binärbaum heißt *nicht-leer*.
- Es ist auch üblich, Bäume graphisch darzustellen.
Die kanonische Darstellung für (a, x, y) ist:



- Beispiel: Das Objekt
 $(7, (3, \varepsilon, (3, \varepsilon, \varepsilon)), (2, (5, \varepsilon, \varepsilon), (7, (1, \varepsilon, \varepsilon), \varepsilon)))$

ist ein Binärbaum über \mathbb{N}_0 .

- Graphisch:



- Die Wurzel des Baumes und die Wurzeln von Teilbäumen (linker bzw. rechter Unterbaum) sind *Knoten*.

- Entsprechend der induktiven Definition lassen sich auch leicht wieder rekursive Funktionen über Binärbäumen definieren, die auf die einzelnen Elemente zugreifen:
- $root : binarytree_M \setminus \{\varepsilon\} \rightarrow M$
mit $root(a, x, y) = a$
- $left : binarytree_M \setminus \{\varepsilon\} \rightarrow binarytree_M$
mit $left(a, x, y) = x$
- $right : binarytree_M \setminus \{\varepsilon\} \rightarrow binarytree_M$
mit $right(a, x, y) = y$

Damit können wir z.B. die Anzahl der Knoten bestimmen:

$$nodes : binarytree_M \rightarrow \mathbb{N}_0$$

$$nodes(z) = \begin{cases} 0, & \text{falls } z = \varepsilon, \\ 1 + nodes(left(z)) + nodes(right(z)) & \text{sonst.} \end{cases}$$