Sebastian Thomas RWTH Aachen, WS 2016/17
17.11.2016–23.11.2016

Diskrete Strukturen

Vorlesungen 9 und 10 (vorläufig)

8 Induktion und Rekursion

Induktion

Da uns die natürlichen Zahlen vertraut sind, haben wir auch ein intuitives Verständnis für die Gültigkeit des folgenden Satzes:

(8.1) Satz (Peano-Arithmetik)**.** Es sei $s\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto n+1$. Dann gilt:

(a) Es ist s injektiv.

(b) Es ist $1 \notin \operatorname{Im} s$.

(c) *Induktionsprinzip.* Für jede Teilmenge U von $\mathbb{N}$ mit $1 \in U$ und $s(U) \subseteq U$ (d.h. für alle $n \in U$ ist auch $s(n) = n+1 \in U$) gilt $U = \mathbb{N}$.

Die in Satz (8.1) aufgeführten Eigenschaften charakterisieren die natürlichen Zahlen bis auf Bijektion. Mit Hilfe dieser Eigenschaften lassen sich die Addition, die Multiplikation und die Ordnung auf $\mathbb{N}$ konstruieren.
Für uns von besonderem Interesse ist das Induktionsprinzip (8.1)(c) (auch *Prinzip der vollständigen Induktion* genannt), welches sich wie folgt äquivalent umformulieren lässt: Zum Beweis einer Aussage der Form

$$(\forall n \in \mathbb{N} : A(n)) := (\forall n : n \in \mathbb{N} \Rightarrow A(n))$$

können wir zeigen, dass die Aussage der Form

$$A(1) \wedge (\forall n \in \mathbb{N} : A(n) \Rightarrow A(n+1))$$

gültig ist, d.h. dass zum einen die Aussage der Form

$$A(1)$$

und zum anderen für jedes $n \in \mathbb{N}$ die Aussage der Form

$$A(n) \Rightarrow A(n+1)$$

gilt.
Um zu zeigen, dass dieses Beweisprinzip gültig ist, nehmen wir an, dass beide Bedingungen erfüllt sind, also dass die Aussage der Form $A(1)$ gilt und dass für jedes $n \in \mathbb{N}$ die Aussage der Form $A(n) \Rightarrow A(n+1)$ gilt. Ferner setzen wir $U := \{n \in \mathbb{N} \mid \text{die Aussage der Form } A(n) \text{ gilt}\}$. Dann ist die Gültigkeit der Aussage der Form $A(1)$ äquivalent zu $1 \in U$. Für alle $n \in U$ gilt ferner die Aussage der Form $A(n)$. Da für jedes $n \in U$ wegen $U \subseteq \mathbb{N}$ die Aussage der Form $A(n) \Rightarrow A(n+1)$ gilt, haben wir auch die Gültigkeit der Aussage der Form $A(n+1)$, d.h. für jedes $n \in U$ ist auch $n+1 \in U$. Nach dem Induktionsprinzip (8.1)(c) impliziert dies bereits $U = \mathbb{N}$, d.h. die Aussage der Form $A(n)$ gilt für alle $n \in \mathbb{N}$. Mit anderen Worten: die Aussage der Form $\forall n \in \mathbb{N} : A(n)$ ist gezeigt.
Wir illustrieren das Induktionsprinzip an einem Beispiel.

(8.2) Anwendungsbeispiel. Für jede ungerade natürliche Zahl m ist $2^m + 1$ ein Vielfaches von 3.

Beweis. Für jedes ungerade $m \in \mathbb{N}$ gibt es (genau) ein $n \in \mathbb{N}$ mit $m = 2n - 1$. Wir wollen zeigen, dass $2^{2n-1} + 1$ für alle $n \in \mathbb{N}$ ein Vielfaches von 3 ist. Hierzu führen wir Induktion nach n.
Induktionsanfang. Für $n = 1$ ist

$$2^{2n-1} + 1 = 2^{2 \cdot 1 - 1} + 1 = 3 = 1 \cdot 3$$

ein Vielfaches von 3.
Induktionsvoraussetzung. Nun sei $n \in \mathbb{N}$ so gegeben, dass $2^{2n-1} + 1$ ein Vielfaches von 3 ist.
Induktionsschritt. Dann gibt es ein $q \in \mathbb{N}$ mit $2^{2n-1} + 1 = q \cdot 3$. Es folgt $2^{2n-1} = q \cdot 3 - 1$ und somit

$$\begin{aligned} 2^{2(n+1)-1} + 1 &= 2^{2n+2-1} + 1 = 4 \cdot 2^{2n-1} + 1 = 4 \cdot (q \cdot 3 - 1) + 1 = 4q \cdot 3 - 4 + 1 = 4q \cdot 3 - 3 \\ &= (4q - 1) \cdot 3. \end{aligned}$$

Insbesondere ist auch $2^{2(n+1)-1} + 1$ ein Vielfaches von 3.
Nach dem Induktionsprinzip ist $2^{2n-1} + 1$ für alle $n \in \mathbb{N}$ ein Vielfaches von 3. □

Im obigen Beispiel haben wir in der Induktionsvoraussetzung angenommen, dass ein (beliebiges) $n \in \mathbb{N}$ gegeben ist und dass die Aussage für dieses n gilt. Anschließend haben wir im Induktionsschritt gezeigt, dass die Aussage unter dieser Annahme auch für $n + 1$ gilt. Äquivalent hätten wir in der Induktionsvoraussetzung natürlich auch annehmen können, dass ein (beliebiges) $n \in \mathbb{N}$ mit $n \geq 2$ gegeben ist und dass die Aussage für $n - 1$ gilt, um im Induktionsschritt dann die Aussage für n zu zeigen.

Alternativer Beweis. Wir zeigen erneut durch Induktion nach n, dass $2^{2n-1} + 1$ für alle $n \in \mathbb{N}$ ein Vielfaches von 3 ist.
Induktionsanfang. Für $n = 1$ verfahren wir wie oben.
Induktionsvoraussetzung. Nun sei $n \in \mathbb{N}$ mit $n \geq 2$ so gegeben, dass $2^{2(n-1)-1} + 1$ ein Vielfaches von 3 ist.
Induktionsschritt. Dann gibt es ein $q \in \mathbb{N}$ mit $2^{2(n-1)-1} + 1 = q \cdot 3$. Es folgt $2^{2(n-1)-1} = q \cdot 3 - 1$ und somit

$$\begin{aligned} 2^{2n-1} + 1 &= 2^{2(n-1)+2-1} + 1 = 4 \cdot 2^{2(n-1)-1} + 1 = 4 \cdot (q \cdot 3 - 1) + 1 = 4q \cdot 3 - 4 + 1 = 4q \cdot 3 - 3 \\ &= (4q - 1) \cdot 3. \end{aligned}$$

Insbesondere ist auch $2^{2n-1} + 1$ ein Vielfaches von 3.
Nach dem Induktionsprinzip ist $2^{2n-1} + 1$ für alle $n \in \mathbb{N}$ ein Vielfaches von 3. □

Eine Variante des Induktionsprinzips lässt sich wie folgt formulieren. Um eine Aussage der Form $\forall n \in \mathbb{N} : A(n)$ zu beweisen, können wir die Aussage der Form

$$A(1) \wedge (\forall n \in \mathbb{N} : A(1) \wedge \ldots \wedge A(n) \Rightarrow A(n + 1))$$

zeigen, d.h. zum einen die Aussage der Form

$$A(1)$$

und zum anderen für jedes $n \in \mathbb{N}$ die Aussage der Form

$$A(1) \wedge \ldots \wedge A(n) \Rightarrow A(n + 1).$$

Um zu zeigen, dass auch diese Variante gültig ist, nehmen wir an, dass beide Bedingungen erfüllt sind, also dass die Aussage der Form $A(1)$ gilt und dass für jedes $n \in \mathbb{N}$ die Aussage der Form $A(1) \wedge \ldots \wedge A(n) \Rightarrow A(n + 1)$ gilt. Dann gilt nach Beispiel (1.29) für jedes $n \in \mathbb{N}$ aber auch die Aussage der Form

$$A(1) \wedge \ldots \wedge A(n) \Rightarrow A(1) \wedge \ldots \wedge A(n) \wedge A(n + 1),$$

so dass nach dem Induktionsprinzip die Aussage der Form $\forall n \in \mathbb{N} : A(1) \wedge \ldots \wedge A(n)$ gilt. Nach Beispiel (1.28)(a) gilt dann aber insbesondere die Aussage der Form $\forall n \in \mathbb{N} : A(n)$.
Wir wollen auch die Nützlichkeit dieses Induktionsprinzip an Hand eines Beispiels verdeutlichen.

(8.3) Anwendungsbeispiel. Jede natürliche Zahl ist ein Produkt ([1]) von Primzahlen.

[1] Genauer meinen wir hier ein Produkt aus einer endlichen Anzahl an Faktoren, wobei ein Produkt aus null Faktoren per Definition immer gleich 1 ist, vgl. Notation (8.7).

Beweis. Wir wollen zeigen, dass jedes $n \in \mathbb{N}$ ein Produkt aus Primzahlen ist. Hierzu führen wir Induktion nach n.
Induktionsanfang. Es ist $n = 1$ ein Produkt aus 0 Faktoren, vgl. Notation (8.7) unten, also insbesondere ein Produkt aus Primzahlen (bestehend aus null Faktoren).
Induktionsvoraussetzung. Nun sei $n \in \mathbb{N}$ gegeben und es sei angenommen, dass jedes $m \in \mathbb{N}$ mit $m < n$ ein Produkt aus Primzahlen ist.
Induktionsschritt. Wenn n eine Primzahl ist, so ist n insbesondere ein Produkt aus Primzahlen (bestehend aus einem Faktor). Andernfalls ist n zusammengesetzt, d.h. es gibt $l, m \in \mathbb{N}$ mit $l < n$, $m < n$ und $n = lm$. Nach Induktionsvoraussetzung sind l und m Produkte aus Primzahlen. Wegen $n = lm$ ist dann aber auch n ein Produkt aus Primzahlen.
Nach dem Induktionsprinzip ist jedes $n \in \mathbb{N}$ ein Produkt aus Primzahlen. □

Mit Hilfe eines abgewandelten Induktionsprinzips lassen sich auch Aussagen für ganze Zahlen ab einer bestimmten Grenze zeigen – das Beweisprinzip bleibt dasselbe, lediglich der Induktionsanfang bei 1 wird zu einem Induktionsanfang bei irgendeinem gegebenen $n_0 \in \mathbb{Z}$. Präzise formuliert: Um für ein $n_0 \in \mathbb{Z}$ eine Aussage der Form $\forall n \in \mathbb{Z} : n \geq n_0 \Rightarrow A(n)$ zu beweisen, können wir die Aussage der Form

$$A(n_0) \land (\forall n \in \mathbb{Z} : n \geq n_0 \Rightarrow (A(n) \Rightarrow A(n+1)))$$

zeigen, d.h. zum einen die Aussage der Form

$$A(n_0)$$

und zum anderen für jedes $n \in \mathbb{Z}$ mit $n \geq n_0$ die Aussage der Form

$$A(n) \Rightarrow A(n+1).$$

Um zu zeigen, dass auch diese Variante gültig ist, nehmen wir an, dass beide Bedingungen erfüllt sind, also dass die Aussage der Form $A(n_0)$ gilt und dass für jedes $n \in \mathbb{Z}$ mit $n \geq n_0$ die Aussage der Form $A(n) \Rightarrow A(n+1)$ gilt. Da $\mathbb{N} \to \{n \in \mathbb{Z} \mid n \geq n_0\}$, $m \mapsto n_0 - 1 + m$ eine wohldefinierte Bijektion ist, gilt dann die Aussage der Form

$$A(n_0 - 1 + 1)$$

sowie für jedes $m \in \mathbb{N}$ die Aussage der Form

$$A(n_0 - 1 + m) \Rightarrow A(n_0 - 1 + m + 1).$$

Nach dem Induktionsprinzip ist dann aber die Gültigkeit der Aussage der Form $\forall m \in \mathbb{N} : A(n_0 - 1 + m)$ nachgewiesen, so dass aus der Bijektion die Gültigkeit der Aussage der Form $\forall n \in \mathbb{Z} : n \geq n_0 \Rightarrow A(n)$ folgt.
Diese Variante des Induktionsprinzips lässt sich zum Beispiel zum Beweis der folgenden Aussage verwenden.

(8.4) Anwendungsbeispiel. Für jedes $n \in \mathbb{N}$ mit $n \geq 4$ gilt $n^2 > 2n + 7$.

Beweis. Wir führen Induktion nach n.
Induktionsanfang. Für $n = 4$ gilt

$$n^2 = 4^2 = 16 > 15 = 2 \cdot 4 + 7 = 2n + 7.$$

Induktionsvoraussetzung. Nun sei $n \in \mathbb{N}$ mit $n \geq 4$ so gegeben, dass $n^2 > 2n + 7$ gilt.
Induktionsschritt. Dann folgt auch

$$(n+1)^2 = n^2 + 2n + 1 > 2n + 7 + 2n + 1 > 2n + 7 + 2 = 2n + 2 + 7 = 2(n+1) + 7.$$

Nach dem Induktionsprinzip gilt $n^2 > 2n + 7$ für alle $n \in \mathbb{N}$ mit $n \geq 4$. □

Rekursion

Auf Grund des Induktionsprinzips lassen sich Folgen, also Familien über $\mathbb{N}$, rekursiv definieren:

(8.5) Proposition (Rekursionssatz)**.** Für jede Menge X, jede Abbildung $t \colon X \to X$ und jedes $a \in X$ gibt es genau eine Folge $x = (x_n)_{n \in \mathbb{N}}$ in X mit $x_1 = a$ und $x_{n+1} = t(x_n)$ für $n \in \mathbb{N}$.

(8.6) Beispiel. Für jedes $a \in \mathbb{R}$ gibt es genau eine Folge $x = (x_n)_{n \in \mathbb{N}}$ in $\mathbb{R}$ mit $x_1 = a$ und $x_{n+1} = ax_n$ für $n \in \mathbb{N}$.

Beweis. Es sei $a \in \mathbb{R}$ gegeben und es sei $t \colon \mathbb{R} \to \mathbb{R}$, $y \mapsto ay$. Nach dem Rekursionssatz (8.5) gibt es genau eine Folge $x = (x_n)_{n \in \mathbb{N}}$ in $\mathbb{R}$ mit $x_1 = a$ und $x_{n+1} = t(x_n) = ax_n$. □

Produkt- und Summennotation

Mit Hilfe von Rekursion führen wir die Produkt- bzw. Summenschreibweise ein:

(8.7) Notation.

(a) Es sei ein Monoid M gegeben. Für jedes $n \in \mathbb{N}_0$ und alle $x \in M^n$ mit $x_i x_j = x_j x_i$ für $i, j \in [1, n]$ notieren wir rekursiv

$$\prod_{i \in [1,n]} x_i = \begin{cases} 1, & \text{falls } n = 0, \\ (\prod_{i \in [1,n-1]} x_i)\, x_n, & \text{falls } n > 0. \end{cases}$$

(b) Es sei ein abelsches Monoid A gegeben. Für jedes $n \in \mathbb{N}_0$ und alle $x \in A^n$ notieren wir rekursiv

$$\sum_{i \in [1,n]} x_i := \begin{cases} 0, & \text{falls } n = 0, \\ \sum_{i \in [1,n-1]} x_i + x_k, & \text{falls } n > 0. \end{cases}$$

Wie skizzieren einen Beweis für die Wohldefiniertheit des in Notation (8.7)(a) definierten Objekts: Es sei

$$t \colon \dot{\bigcup_{n \in \mathbb{N}_0}} \operatorname{Map}(M^n, M) \to \dot{\bigcup_{n \in \mathbb{N}_0}} \operatorname{Map}(M^n, M)$$

gegeben durch

$$t(f) \colon M^{n+1} \to M,\ x \mapsto f((x_i)_{i \in [1,n]}) \cdot x_{n+1}$$

für $f \in \operatorname{Map}(M^n, M)$, $n \in \mathbb{N}_0$. Nach dem Rekursionssatz (8.5) ([2]) gibt es genau eine durch $\mathbb{N}_0$ indizierte Folge $(p_n)_{n \in \mathbb{N}_0}$ in $\dot{\bigcup}_{n \in \mathbb{N}_0} \operatorname{Map}(M^n, M)$ mit $p_0 \colon M^0 \to M$, $x \mapsto 1$ und mit $p_n = t(p_{n-1})$ für $n \in \mathbb{N}_0$. Nach dem Induktionsprinzip ist dann p_n für jedes $n \in \mathbb{N}_0$ eine Abbildung von M^n nach M. Für $n \in \mathbb{N}_0$, $x \in M^n$ mit $x_i x_j = x_j x_i$ für $i, j \in [1, n]$ schreiben wir

$$\prod_{i \in [1,n]} x_i = p_n(x),$$

dann gilt

$$\prod_{i \in [1,n]} x_i = p_n(x) = \left\{\begin{matrix} 1, & \text{falls } n = 0, \\ (t(p_{n-1}))(x), & \text{falls } n > 0 \end{matrix}\right\} = \left\{\begin{matrix} 1, & \text{falls } n = 0, \\ p_{n-1}((x_i)_{i \in [1,n-1]}) \cdot x_n, & \text{falls } n > 0 \end{matrix}\right\}$$
$$= \begin{cases} 1, & \text{falls } n = 0, \\ (\prod_{i \in [1,n-1]} x_i) \cdot x_n, & \text{falls } n > 0. \end{cases}$$

(8.8) Bemerkung. Es seien ein Monoid M, eine endliche Menge I und ein $x \in M^I$ so gegeben, dass $x_i x_j = x_j x_i$ für $i, j \in I$ gilt. Für Abzählungen $e, e' \colon [1, |I|] \to I$ gilt

$$\prod_{k \in [1,|I|]} x_{e(k)} = \prod_{k \in [1,|I|]} x_{e'(k)}.$$

Beweisidee. Dies folgt aus der Assoziativität von M. □

Die vorangegangene Bemerkung erlaubt uns, die Produkt- und Summenschreibweise auf beliebige endliche Indexmengen zu verallgemeinern:

(8.9) Notation. Es sei eine endliche Menge I gegeben. Wir wählen eine Abzählung $e \colon [1, |I|] \to I$.

(a) Es seien ein Monoid M und ein $x \in M^I$ so gegeben, dass $x_i x_j = x_j x_i$ für $i, j \in I$ gilt. Wir setzen

$$\prod_{i \in I} x_i := \prod_{k \in [1,|I|]} x_{e(k)}.$$

[2] Genau genommen benutzen wir eine Variante für $\mathbb{N}_0$ statt $\mathbb{N}$.

(b) Es seien ein abelsches Monoid A und ein $x \in A^I$ gegeben. Wir setzen

$$\sum_{i \in I} x_i := \sum_{k \in [1,|I|]} x_{e(k)}.$$

(8.10) Notation. Es seien ein Monoid M und eine Menge I gegeben. Wir setzen

$$M^{(I)} := \{x \in M^I \mid \{i \in I \mid x_i \neq 1\} \text{ ist endlich}\}.$$

(8.11) Notation. Es sei eine Menge I gegeben.

(a) Es seien ein Monoid M und ein $x \in M^{(I)}$ so gegeben, dass $x_i x_j = x_j x_i$ für $i, j \in I$ gilt. Wir setzen

$$\prod_{i \in I} x_i := \prod_{\substack{i \in I \\ x_i \neq 1}} x_i := \prod_{i \in \{j \in I \mid x_j \neq 1\}} x_i.$$

(b) Es seien ein abelsches Monoid A und ein $x \in A^{(I)}$ gegeben. Wir setzen

$$\sum_{i \in I} x_i := \sum_{\substack{i \in I \\ x_i \neq 0}} x_i := \sum_{i \in \{j \in I \mid x_j \neq 0\}} x_i.$$

Wir kommen zum Spezialfall, bei welchem alle indizierten Elemente gleich sind:

(8.12) Notation.

(a) Es seien ein Monoid M und $x \in M$ gegeben. Für $k \in \mathbb{N}_0$ setzen wir

$$x^k := \prod_{i \in [1,k]} x.$$

Wenn x invertierbar in M ist, so setzen wir

$$x^{-k} := (x^{-1})^k$$

für $k \in \mathbb{N}$.

(b) Es seien ein abelsches Monoid A und $x \in A$ gegeben. Für $k \in \mathbb{N}_0$ setzen wir

$$kx = k \cdot x := \sum_{i \in [1,k]} x.$$

Wenn x negierbar in A ist, so setzen wir

$$(-k)x := k(-x)$$

für $k \in \mathbb{N}$.

(8.13) Proposition (Potenzgesetze)**.** Es sei ein Monoid M gegeben.

(a) Für $x \in M$, $k, l \in \mathbb{N}_0$ gilt

$$x^k x^l = x^{k+l}.$$

Für $x \in M^\times$, $k, l \in \mathbb{Z}$ gilt

$$x^k x^l = x^{k+l}.$$

(b) Für $x \in M$, $k, l \in \mathbb{N}_0$ gilt

$$(x^k)^l = x^{kl}.$$

Für $x \in M^\times$, $k, l \in \mathbb{Z}$ gilt

$$(x^k)^l = x^{kl}.$$

(c) Es sei M kommutativ. Für $x, y \in M$, $k \in \mathbb{N}_0$ gilt

$$x^k y^k = (xy)^k.$$

Für $x, y \in M^\times$, $k \in \mathbb{Z}$ gilt

$$x^k y^k = (xy)^k.$$

Beweis.

(a) Es seien $x \in M$, $k \in \mathbb{N}_0$ gegeben. Um $x^k x^l = x^{k+l}$ für alle $l \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach l. Für $l = 0$ gilt

$$x^k x^l = x^k x^0 = x^k \cdot 1 = x^k = x^{k+0}.$$

Es sei also $l > 0$ und gelte $x^k x^{l-1} = x^{k+l-1}$. Dann ist auch $k + l \geq l > 0$ und somit

$$x^k x^l = x^k (x^{l-1} x) = (x^k x^{l-1}) x = x^{k+l-1} x = x^{k+l}.$$

Nach dem Induktionsprinzip haben wir $x^k x^l = x^{k+l}$ für alle $l \in \mathbb{N}_0$.

Um $x^k x^l = x^{k+l}$ für alle $x \in M^\times$, $k, l \in \mathbb{Z}$ zu zeigen, unterscheiden wir drei Fälle. Zuerst verifizieren wir die Gleichung für den Spezialfall $x \in M^\times$, $k \in \mathbb{Z}$, $l = 1$, danach für $x \in M^\times$, $k \in \mathbb{Z}$, $l \geq 0$ mittels Induktion nach l, und schließlich für $x \in M^\times$, $k \in \mathbb{Z}$, $l < 0$.

Zum ersten Fall. Es seien $x \in M^\times$, $k \in \mathbb{Z}$, $l = 1$. Für $k \geq 0$ ist $k+1 > 0$ und damit $x^{k+1} = x^{(k+1)-1} x = x^k x$ nach Definition. Für $k < 0$ gilt aber $-k > 0$ und damit ebenfalls

$$\begin{aligned} x^k x^1 &= (x^{-1})^{-k} x = ((x^{-1})^{-k-1} x^{-1}) x = (x^{-1})^{-k-1} (x^{-1} x) = (x^{-1})^{-(k+1)} \cdot 1 = (x^{-1})^{-(k+1)} \\ &= \left. \begin{cases} (x^{-1})^0, & \text{falls } k = -1, \\ x^{-(-(k+1))}, & \text{falls } k < -1 \end{cases} \right\} = \left. \begin{cases} 1, & \text{falls } k = -1, \\ x^{k+1}, & \text{falls } k < -1 \end{cases} \right\} = x^{k+1}. \end{aligned}$$

Zum zweiten Fall. Es seien $x \in M^\times$, $k \in \mathbb{Z}$. Um $x^k x^l = x^{k+l}$ für $l \in \mathbb{Z}$, $l \geq 0$ zu zeigen, führen wir Induktion nach l (wobei dies völlig analog zum Beweis für $x \in M$, $k, l \in \mathbb{N}_0$ geht): Für $l = 0$ gilt

$$x^k x^l = x^k x^0 = x^k \cdot 1 = x^k = x^{k+0}.$$

Es seien also $l > 0$ und es gelte $x^k x^{l-1} = x^{k+l-1}$. Unter Benutzung des ersten Falls erhalten wir dann auch

$$x^k x^l = x^k (x^{l-1} x) = (x^k x^{l-1}) x = x^{k+l-1} x = x^{k+l}.$$

Nach dem Induktionsprinzip haben wir $x^k x^l = x^{k+l}$ für alle $l \geq 0$.

Zum dritten Fall. Schließlich seien $x \in M^\times$, $k, l \in \mathbb{Z}$, $l < 0$. Dann ist $-l > 0$, also

$$x^{k+l} x^{-l} = x^{k+l+(-l)} = x^k$$

nach dem zweiten Fall und damit $x^{k+l} = x^k (x^{-l})^{-1}$. Nun haben wir aber

$$x^{-l} x^l = ((x^{-1})^{-1})^{-l} (x^{-1})^{-l} = (x^{-1})^{-(-l)} (x^{-1})^{-l} = (x^{-1})^l (x^{-1})^{-l} = (x^{-1})^{l+(-l)} = (x^{-1})^0 = 1$$

unter Benutzung des zweiten Falls, also $(x^{-l})^{-1} = x^l$ nach Bemerkung (6.15) und damit auch in diesem Fall

$$x^k x^l = x^k (x^{-l})^{-1} = x^{k+l}.$$

(b) Es seien $x \in M$, $k \in \mathbb{N}_0$ gegeben. Um $(x^k)^l = x^{kl}$ für alle $l \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach l. Für $l = 0$ gilt

$$(x^k)^0 = 1 = x^0 = x^{k \cdot 0}.$$

Es sei also $l > 0$ und gelte $(x^k)^{l-1} = x^{k(l-1)}$. Mit (a) folgt

$$(x^k)^l = (x^k)^{l-1} x^k = x^{k(l-1)} x^k = x^{k(l-1)+k} = x^{kl}$$

Nach dem Induktionsprinzip haben wir $(x^k)^l = x^{kl}$ für alle $l \in \mathbb{N}_0$.

Um $(x^k)^l = x^{kl}$ für alle $x \in M^\times$, $k, l \in \mathbb{Z}$, unterscheiden wir drei Fälle. Zuerst verifizieren wir die Gleichung für $k \geq 0$, $l \geq 0$, danach für $k < 0$, $l \geq 0$, und schließlich für $k \in \mathbb{Z}$, $l < 0$.

Zum ersten Fall. Wir haben bereits bewiesen, dass $(x^k)^l = x^{kl}$ für alle $x \in M$, $k, l \in \mathbb{N}_0$ gilt, also insbesondere für $x \in M^\times$, $k, l \in \mathbb{Z}$, $k \geq 0$, $l \geq 0$.

Zum zweiten Fall. Es seien $x \in M^\times$, $k, l \in \mathbb{Z}$, $k < 0$, $l \geq 0$. Dann ist $-k > 0$ und $-kl > 0$, also

$$(x^k)^l = ((x^{-1})^{-k})^l = (x^{-1})^{(-k)l} = (x^{-1})^{-kl} = x^{kl}$$

nach dem ersten Fall.

Zum dritten Fall. Es seien $x \in M^\times$, $k, l \in \mathbb{Z}$, $k \in \mathbb{Z}$, $l < 0$. Dann ist $-l > 0$, also

$$(x^k)^{-l} = x^{k(-l)}$$

nach dem ersten oder zweiten Fall. Nun ist aber $(x^k)^l\,(x^k)^{-l} = (x^k)^0 = 1$ und $x^{k(-l)} x^{kl} = x^0 = 1$ nach (a), also $((x^k)^{-l})^{-1} = (x^k)^l$ und $(x^{k(-l)})^{-1} = x^{kl}$ nach Bemerkung (6.15). Wir erhalten also auch in diesem Fall

$$(x^k)^l = ((x^k)^{-l})^{-1} = (x^{k(-l)})^{-1} = x^{kl}.$$

(c) Es seien $x, y \in M$ gegeben. Um $x^k y^k = (xy)^k$ für alle $k \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach k. Für $k = 0$ gilt

$$x^k y^k = x^0 y^0 = 1 \cdot 1 = 1 = (xy)^0.$$

Es sei also $k > 0$ und gelte $x^{k-1} y^{k-1} = (xy)^{k-1}$. Dann ist auch

$$x^k y^k = (x^{k-1} x)(y^{k-1} y) = (x^{k-1} y^{k-1})(xy) = (xy)^{k-1}\,(xy) = (xy)^k.$$

Nach dem Induktionsprinzip haben wir $x^k y^k = (xy)^k$ für alle $k \in \mathbb{N}_0$.

Nun seien $x, y \in M^\times$, $k \in \mathbb{Z}$, $k < 0$. Dann ist $-k > 0$, also

$$x^k y^k = (x^{-1})^{-k} (y^{-1})^{-k} = (x^{-1} y^{-1})^{-k} = (y^{-1} x^{-1})^{-k} = ((xy)^{-1})^{-k} = (xy)^k$$

nach Proposition (6.30)(a). □

Jeder Ring R hat eine unterliegende abelsche Gruppe. Folglich haben wir für jedes $x \in R$, $k \in \mathbb{Z}$ den Ausdruck $kx = k \cdot x \in R$ definiert, vgl. Notation (8.12)(b).

(8.14) Notation. Es sei ein Ring R gegeben. Für $k \in \mathbb{Z}$ schreiben wir auch

$$k = k^R := k \cdot 1^R.$$

Wir betonen, dass die vorangegangene Vereinbarung konform mit unserer Notation für das Nullelement und das Einselement in einem Ring R ist. Sie besagt unter anderem, dass wir $2^R = 2 \cdot 1^R = 1^R + 1^R$, $3^R = 3 \cdot 1^R = 2 \cdot 1^R + 1^R = 2^R + 1^R$, etc., setzen.

Hin und wieder werden wir außerdem folgende Schreibweise antreffen:

(8.15) Notation (Kronecker-Delta)**.** Es seien ein Ring R, eine Menge I und $i, j \in I$ gegeben. Das *Kronecker-Delta* ist definiert als

$$\delta_{i,j} := \begin{cases} 1^R & \text{falls } i = j, \\ 0^R & \text{falls } i \neq j. \end{cases}$$

Rekursionsgleichungen

(8.16) Beispiel. Es sei $f \in \mathbb{R}^{\mathbb{N}_0}$ gegeben durch

$$f_k = \begin{cases} 0, & \text{für } k = 0, \\ 1, & \text{für } k = 1, \\ f_{k-2} + f_{k-1}, & \text{für } k \in \mathbb{N}_0 \text{ mit } k \geq 2. \end{cases}$$

Dann gilt

$$f_k = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^k - (\frac{1-\sqrt{5}}{2})^k)$$

für $k \in \mathbb{N}_0$.

Beweis. Wir führen Induktion nach k. Für $k = 0$ gilt

$$f_k = f_0 = 0 = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^0 - (\frac{1-\sqrt{5}}{2})^0).$$

Für $k = 1$ gilt

$$f_k = f_1 = 1 = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^1 - (\frac{1-\sqrt{5}}{2})^1).$$

Für $k \in \mathbb{N}_0$ mit $k \geq 2$ und $f_{k-2} = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-2} - (\frac{1-\sqrt{5}}{2})^{k-2})$ und $f_{k-1} = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-1})$ gilt auch

$$\begin{aligned}
f_k &= f_{k-2} + f_{k-1} = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-2} - (\frac{1-\sqrt{5}}{2})^{k-2}) + \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-1}) \\
&= \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-2} - (\frac{1-\sqrt{5}}{2})^{k-2} + (\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-1}) \\
&= \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-2} + (\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-2} - (\frac{1-\sqrt{5}}{2})^{k-1}) \\
&= \frac{1}{\sqrt{5}}(\frac{2^2(1+\sqrt{5})^{k-2} + 2(1+\sqrt{5})^{k-1}}{2^k} - \frac{2^2(1-\sqrt{5})^{k-2} + 2(1-\sqrt{5})^{k-1}}{2^k}) \\
&= \frac{1}{\sqrt{5}}(\frac{(4 + 2(1+\sqrt{5}))(1+\sqrt{5})^{k-2}}{2^k} - \frac{(4 + 2(1-\sqrt{5}))(1-\sqrt{5})^{k-2}}{2^k}) \\
&= \frac{1}{\sqrt{5}}(\frac{(4 + 2 + 2\sqrt{5})(1+\sqrt{5})^{k-2}}{2^k} - \frac{(4 + 2 - 2\sqrt{5})(1-\sqrt{5})^{k-2}}{2^k}) \\
&= \frac{1}{\sqrt{5}}(\frac{(1 + 2\sqrt{5} + (\sqrt{5})^2)(1+\sqrt{5})^{k-2}}{2^k} - \frac{(1 - 2\sqrt{5} + (\sqrt{5})^2)(1-\sqrt{5})^{k-2}}{2^k}) \\
&= \frac{1}{\sqrt{5}}(\frac{(1+\sqrt{5})^2\,(1+\sqrt{5})^{k-2}}{2^k} - \frac{(1-\sqrt{5})^2\,(1-\sqrt{5})^{k-2}}{2^k}) = \frac{1}{\sqrt{5}}(\frac{(1+\sqrt{5})^k}{2^k} - \frac{(1-\sqrt{5})^k}{2^k}).
\end{aligned}$$

Nach dem Induktionsprinzip gilt $f_k = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^k - (\frac{1-\sqrt{5}}{2})^k)$ für alle $k \in \mathbb{N}_0$. □

(8.17) Beispiel. Es seien ein Monoid M, $a \in M$ und $x \in M^{\mathbb{N}_0}$ mit

$$x_{k+1} = a x_k$$

für $k \in \mathbb{N}_0$ gegeben. Dann ist

$$x_k = a^k x_0$$

für $k \in \mathbb{N}_0$.

Beweis. Wir führen Induktion nach k. Für $k = 0$ gilt

$$x_0 = 1x_0 = a^0 x_0.$$

Für $k \in \mathbb{N}_0$ mit $x_k = a^k x_0$ gilt auch

$$x_{k+1} = ax_k = aa^k x_0 = a^{k+1} x_0.$$

Nach dem Induktionsprinzip gilt also in der Tat $x_k = a^k x_0$ für alle $k \in \mathbb{N}_0$. $\square$

(8.18) Beispiel. Es seien ein Monoid M, $a \in M^{\mathbb{N}}$ und $x \in M^{\mathbb{N}_0}$ mit

$$x_{k+1} = a_{k+1} x_k$$

für $k \in \mathbb{N}_0$ gegeben. Dann ist

$$x_k = (\prod_{i \in [1,k]} a_i) x_0$$

für $k \in \mathbb{N}_0$.

Beweis. Dies sei dem Leser zur Übung überlassen. $\square$

(8.19) Beispiel. Es sei $x \in \mathbb{R}^{\mathbb{N}_0}$ mit

$$x_{k+1} = x_k + k + 1$$

für $k \in \mathbb{N}_0$ gegeben. Dann ist

$$x_k = \frac{(k+1)k}{2} + x_0$$

für $k \in \mathbb{N}_0$.

(8.20) Beispiel. Es sei $x \in \mathbb{R}^{\mathbb{N}_0}$ mit

$$x_{k+1} = 2x_k + 2^{k+1}$$

für $k \in \mathbb{N}_0$ gegeben. Dann ist

$$x_k = 2^k (k + x_0)$$

für $k \in \mathbb{N}_0$.

Beweis. Für $k = 0$ gilt

$$x_0 = 2^0 \cdot (0 + x_0) = 2^k (k + x_0).$$

Für $k \in \mathbb{N}_0$ mit $x_k = 2^k (k + x_0)$ gilt auch

$$\begin{aligned} x_{k+1} &= 2x_k + 2^{k+1} = 2 \cdot 2^k (k + x_0) + 2^{k+1} = 2^{k+1}(k + x_0) + 2^{k+1} = 2^{k+1}(k + x_0 + 1) \\ &= 2^{k+1}(k + 1 + x_0). \end{aligned}$$

Nach dem Induktionsprinzip gilt $x_k = 2^k (k + x_0)$ für alle $k \in \mathbb{N}_0$. $\square$

(8.21) Beispiel. Es sei $x \in \mathbb{R}^{\mathbb{N}_0}$ mit

$$x_k = 2x_{\lfloor \frac{k}{2} \rfloor} + k$$

für $k \in \mathbb{N}$ gegeben. Dann ist

$$x_k = \sum_{i \in [0, \lfloor \log_2(k) \rfloor]} \lfloor \frac{k}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(k) \rfloor + 1} x_0$$

für $k \in \mathbb{N}$.

Beweis. Für $k = 1$ gilt

$$\begin{aligned}\sum_{i \in [0, \lfloor \log_2(k) \rfloor]} \lfloor \frac{k}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(k) \rfloor + 1} x_0 &= \sum_{i \in [0, \lfloor \log_2(1) \rfloor]} \lfloor \frac{1}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(1) \rfloor + 1} x_0 = \sum_{i \in [0,0]} \lfloor \frac{1}{2^i} \rfloor \, 2^i + 2^{0+1} x_0 \\ &= 1 + 2x_0,\end{aligned}$$

also

$$x_k = x_1 = 2x_0 + 1 = \sum_{i \in [0, \lfloor \log_2(k) \rfloor]} \lfloor \frac{k}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(k) \rfloor + 1} x_0.$$

Für $k \in \mathbb{N}$ mit $k > 1$ gilt

$$\begin{aligned}x_k &= 2x_{\lfloor \frac{k}{2} \rfloor} + k = 2(\sum_{i \in [0, \lfloor \log_2(k) \rfloor]} \lfloor \frac{\lfloor \frac{k}{2} \rfloor}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(\lfloor \frac{k}{2} \rfloor) \rfloor + 1} x_0) + k \\ &= 2(\sum_{i \in [0, \lfloor \log_2(k) \rfloor]} \lfloor \frac{k}{2^{i+1}} \rfloor \, 2^i + 2^{\lfloor \log_2(\frac{k}{2}) \rfloor + 1} x_0) + k = \sum_{i \in [0, \lfloor \log_2(k) \rfloor]} \lfloor \frac{k}{2^{i+1}} \rfloor \, 2^{i+1} + 2^{\lfloor \log_2(k) - 1 \rfloor + 1 + 1} x_0 + k \\ &= k + \sum_{i \in [1, \lfloor \log_2(k) \rfloor + 1]} \lfloor \frac{k}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(k) \rfloor + 1} x_0 = \sum_{i \in [0, \lfloor \log_2(k) \rfloor]} \lfloor \frac{k}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(k) \rfloor + 1} x_0.\end{aligned}$$

Nach dem Induktionsprinzip gilt $x_k = \sum_{i \in [0, \lfloor \log_2(k) \rfloor]} \lfloor \frac{k}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(k) \rfloor + 1} x_0$ für alle $k \in \mathbb{N}$. □

(8.22) Beispiel. Es sei $x \in \mathbb{R}^{\mathbb{N}_0}$ mit

$$x_k = 2x_{\lfloor \frac{k}{2} \rfloor} + k$$

für $k \in \mathbb{N}$ gegeben. Dann ist

$$x_{2^l} = 2^l(l + 2x_0 + 1)$$

für $l \in \mathbb{N}_0$. Mit anderen Worten: Für $k \in 2^{\mathbb{N}_0}$ gilt

$$x_k = k(\log_2(k) + 2x_0 + 1).$$

Beweis. Für $k \in \mathbb{N}$ gilt $x_k = 2x_{\lfloor \frac{k}{2} \rfloor} + k$, also insbesondere

$$x_{2k} = 2x_{\lfloor \frac{2k}{2} \rfloor} + 2k = 2x_k + 2k.$$

Für $l \in \mathbb{N}_0$ folgt

$$x_{2^{l+1}} = x_{2 \cdot 2^l} = 2x_{2^l} + 2 \cdot 2^l = 2x_{2^l} + 2^{l+1},$$

und damit

$$x_{2^l} = 2^l(l + x_{2^0}) = 2^l(l + x_1) = 2^l(l + 2x_0 + 1)$$

nach Beispiel (8.20). □

Mache Wertetabelle:

(8.23) Definition (ungefähr gleich schnelles asymptotisches Wachstum)**.** Es seien $x, y \in \mathbb{R}_{\geq 0}^{\mathbb{N}_0}$ gegeben. Wir sagen, dass x *ungefähr so schnell* wie y *wächst*, wenn es $c, d \in \mathbb{R}_{>0}$ und ein $k_0 \in \mathbb{N}_0$ derart gibt, dass für $k \in \mathbb{N}_0$ mit $k \geq k_0$ stets

$$cy_k \leq x_k \leq dy_k$$

gilt.

(8.24) Beispiel. Es seien $x, y \in \mathbb{R}_{\geq 0}^{\mathbb{N}_0}$ mit

$$\begin{aligned} x_k &= 2x_{\lfloor \frac{k}{2} \rfloor} + k, \\ y_k &= k \log_2(k) \end{aligned}$$

für $k \in \mathbb{N}$ gegeben. Dann wächst x ungefähr so schnell wie y.

Beweis. Zunächst zeigen wir durch Induktion nach k, dass für $k \in \mathbb{N}_0$ mit $k \geq 2$ stets $x_k \leq 2(x_0 + 1)y_k$ gilt. Für $k = 2$ gilt

$$\begin{aligned} x_k &= x_2 = 2x_1 + 2 = 2(2x_0 + 1) + 2 = 4x_0 + 4 = 2(x_0 + 1) \cdot 2 = 2(x_0 + 1) \cdot 2 \log_2(2) = 2(x_0 + 1)y_2 \\ &= 2(x_0 + 1)y_k. \end{aligned}$$

Für $k = 3$ gilt

$$\begin{aligned} x_k &= x_3 = 2x_1 + 3 = 2(2x_0 + 1) + 3 = 4x_0 + 5 \leq 6x_0 + 6 = 2(x_0 + 1) \cdot 3 \leq 2(x_0 + 1) \cdot 3 \log_2(3) \\ &= 2(x_0 + 1)y_3 = 2(x_0 + 1)y_k. \end{aligned}$$

Für $k \in \mathbb{N}_0$ mit $k \geq 4$ gilt

$$\begin{aligned} x_k &= 2x_{\lfloor \frac{k}{2} \rfloor} + k \leq 2 \cdot 2(x_0 + 1)y_{\lfloor \frac{k}{2} \rfloor} + k = 4(x_0 + 1)\lfloor \frac{k}{2} \rfloor \log_2(\lfloor \frac{k}{2} \rfloor) + k \leq 4(x_0 + 1)\frac{k}{2} \log_2(\frac{k}{2}) + k \\ &= 2(x_0 + 1)k(\log_2(k) - 1) + k = 2(x_0 + 1)k \log_2(k) - 2(x_0 + 1)k + k = 2(x_0 + 1)y_k - (2x_0 + 1)k \\ &\leq 2(x_0 + 1)y_k. \end{aligned}$$

Nach dem Induktionsprinzip gilt $x_k \leq 2(x_0 + 1)y_k$ für alle $k \in \mathbb{N}_0$ mit $k \geq 2$. $\square$