

# Kapitel 2

## Die natürlichen Zahlen

### 2.1 Peano-Systeme

**Definition 2.1.** Ein Tripel  $(D, S, d)$  mit den Eigenschaften

(P1)  $d \in D$ ,

(P2)  $S: D \rightarrow D$ ,

(P3)  $S(n) \neq d$  für alle  $n \in D$ ,

(P4)  $S$  ist injektiv,

(P5) Ist  $M \subset D$  mit  $d \in M$  und  $(n \in M \implies S(n) \in M)$ , dann ist  $M = D$ ,

heißt ein Peano-System oder ein Modell der natürlichen Zahlen (mit Anfangselement  $d$  und Nachfolgerfunktion  $S$ ).

**Bemerkung 2.2.**  $S$  steht für successor, engl. Nachfolger. Die Eigenschaften (P1)–(P5) sind als Peano-Axiome (G. Peano, 1889) bekannt. Sie lassen sich in komprimierter Form auch wie folgt formulieren:

(P1\*)  $d \in D$ ,

(P2\*)  $S: D \rightarrow D$  ist eine injektive Abbildung mit  $d \notin S(D)$ ,

(P3\*) Ist  $M \subset D$  mit  $d \in M$  und  $S(M) \subset M$ , dann gilt  $M = D$ .

**Bemerkung 2.3.** Bei der Nachfolgerfunktion  $S$  kann man sich von der Vorstellung leiten lassen, dass  $S$  jedem  $n \in D$  einen Nachfolger  $S(n) \in D$  zuordnet. Durch die Funktion  $S$  wird so etwas wie eine Reihenfolge auf  $D$  definiert, nämlich

$$d, S(d), S(S(d)), S(S(S(d))), \dots$$

Eigenschaft (P5) (oder (P3\*)) garantiert, dass auf diese Weise alle Elemente von  $D$  erfasst werden (vgl. Folgerung 2.6).

**Bemerkung 2.4.** Die Eigenschaft (P5) bzw. (P3\*) beinhaltet das Prinzip der vollständigen Induktion, das wir schon in Abschnitt 1.3 als Beweismethode kennen gelernt haben.

Als erstes stellt sich natürlich die Frage, ob es überhaupt Peano-Systeme gibt.

**Satz 2.5.** *Es existiert (mindestens) ein Peano-System  $(D, S, d)$ .*



Giuseppe Peano  
geb. 27.8.1858 in Cuneo, Italien  
gest. 20.4.1932 in Turin

*Beweis.* Das System  $(\mathbb{N}_0, S^+, 0)$  mit  $S^+ : \mathbb{N}_0 \rightarrow \mathbb{N}_0, n \mapsto n^+$  ist nach Satz 1.46 ein Peano-System.  $\square$

Das Peano-System  $(\mathbb{N}_0, S^+, 0)$  bezeichnen wir in Zukunft als Standardmodell der natürlichen Zahlen. Als erste Anwendung des Prinzips der vollständigen Induktion beweisen wir

**Folgerung 2.6.** *Ist  $(D, S, d)$  ein Peano-System, dann gilt  $D = \{d\} \cup S(D)$ .*

*Beweis.* Sei  $M = \{d\} \cup S(D)$ , dann gilt wegen (P1\*) und (P2\*) zunächst  $M \subset D$ . Außerdem ist natürlich  $d \in M$  und (vgl. Lemma 1.31(iv))

$$S(M) \subset S(\{d\}) \cup S(S(D)) \subset S(D) \cup S(D) = S(D) \subset M.$$

Mit (P3\*) folgt deshalb  $M = D$ .  $\square$

Als Verallgemeinerung der Definition einer Folge in Abschnitt 1.4 definieren wir jetzt: Ist  $(D, S, d)$  ein Peano-System und  $A$  eine beliebige Menge, dann heißt eine Abbildung  $T : D \rightarrow A$  auch eine Folge in  $A$ . Für  $T(n) = a$  schreibt man meist  $a_n$  und für die gesamte Folge  $(a_n)_{n \in D}$ .

**Definition durch Rekursion:** Häufig definiert man Folgen durch Rekursion (rekursiv), z. B. definiert man durch

$$(2.1) \quad a_0 := a, \quad a_{n+1} := 2a_n - 2 \quad (n = 0, 1, 2, \dots)$$

eine reelle Zahlenfolge.

Anschaulich wird durch (2.1) jedem  $n$  eine reelle Zahl  $a_n$  zugeordnet. Die Frage ist aber, ob dadurch wirklich eine eindeutig bestimmte Folge, also eine eindeutig bestimmte Abbildung von  $\mathbb{N}_0$  in die reellen Zahlen definiert wird.

**Satz 2.7** (Rekursionstheorem, Dedekind 1899). *Sei  $(D, S, d)$  ein Peano-System,  $X$  eine beliebige Menge,  $a \in X$  und  $f : X \rightarrow X$ , dann gibt es genau eine Folge  $u = (u_n)_{n \in D}$  in  $X$  mit*

$$(2.2) \quad u_d = a, \quad u_{S(n)} = f(u_n) \quad (n \in D).$$



Julius Wilhelm Richard Dedekind  
geb. 6.10.1831 in Braunschweig  
gest. 12.2.1916 in Braunschweig

*Beweis.*

*Eindeutigkeit von  $u$ .* Sei  $v: D \rightarrow X$  eine weitere Folge in  $X$ , die (2.2) erfüllt, d. h.,

$$v_d = a, \quad v_{S(n)} = f(v_n) \quad (n \in D)$$

und sei

$$M := \{n \in D; u_n = v_n\}.$$

Es gilt  $d \in M$  und

$$n \in M \implies u_n = v_n \implies f(u_n) = f(v_n) \implies u_{S(n)} = v_{S(n)} \implies S(n) \in M.$$

Nach dem Induktionsprinzip (P5) ist  $M = D$ , also  $u_n = v_n$  für alle  $n \in D$ .

*Existenz von  $u$ .* Wir betrachten das Mengensystem

$$\mathfrak{C} := \{A \subset D \times X; (d, a) \in A \wedge ((n, x) \in A \implies (S(n), f(x)) \in A)\}$$

Wegen  $D \times X \in \mathfrak{C}$  ist  $\mathfrak{C} \neq \emptyset$  und wir können die Menge

$$u := \bigcap_{A \in \mathfrak{C}} A$$

bilden. Es gilt  $u \in \mathfrak{C}$ , d. h.  $u$  ist Relation von  $D$  nach  $X$ , und wir werden jetzt noch zeigen, dass  $u$  sogar eine Abbildung von  $D$  nach  $X$  ist, die (2.2) erfüllt.

1)  $\text{dom } u = D$ . Wegen  $u \in \mathfrak{C}$  gilt  $\text{dom } u \subset D$  und  $d \in \text{dom } u$ . Ist nun  $n \in \text{dom } u$ , dann existiert ein  $x \in X$  mit  $(n, x) \in u$  und nach Definition von  $\mathfrak{C}$  folgt  $(S(n), f(x)) \in u$ . Also ist auch  $S(n) \in \text{dom } u$ . Mit (P5) folgt  $\text{dom } u = D$ .

2)  $(n, x) \in u \wedge (n, y) \in u \implies x = y$ . Sei diesmal

$$M := \{n \in D; (n, x) \in u \wedge (n, y) \in u \implies x = y\}.$$

Wir zeigen wieder mit (P5), dass  $M = D$  ist.

Wir nehmen an, dass  $d \notin M$  ist. In diesem Fall existiert ein  $b \in X$  mit  $b \neq a$  und  $(d, b) \in u$ . Setzen wir nun

$$\tilde{u} := u \setminus \{(d, b)\},$$

dann ist  $(d, a) \in \tilde{u}$  und

$$(n, x) \in \tilde{u} \xrightarrow{\tilde{u} \subset u} (n, x) \in u \xrightarrow{u \in \mathfrak{C}} (S(n), f(x)) \in u \xrightarrow{S(n) \neq d} (S(n), f(x)) \in \tilde{u}.$$

Damit ist aber  $\tilde{u} \in \mathfrak{C}$  und nach Definition von  $u$  gilt  $u \subset \tilde{u}$ . Dies ist aber ein Widerspruch zur Definition von  $\tilde{u}$ . Also ist  $d \in M$ .

Sei nun  $n \in M$ , dann existiert ein eindeutig bestimmtes  $c \in X$  mit  $(n, c) \in u$  und damit ist auch  $(S(n), f(c)) \in u$ . Angenommen  $S(n) \notin M$ , dann existiert ein  $g \in X$  mit  $g \neq f(c)$  und  $(S(n), g) \in u$ . Wir setzen nun

$$\hat{u} := u \setminus \{(S(n), g)\}$$

und zeigen  $\hat{u} \in \mathfrak{C}$ . Wegen  $(d, a) \in u$  und  $d \neq S(n)$  für alle  $n \in D$  ist  $(d, a) \in \hat{u}$ . Außerdem gilt

$$(m, x) \in \hat{u} \xrightarrow{\hat{u} \subset u} (m, x) \in u \xrightarrow{u \in \mathfrak{C}} (S(m), f(x)) \in u \xrightarrow{?} (S(m), f(x)) \in \hat{u}.$$

Zu ?. Für  $m \neq n$  ist nach (P4) auch  $S(m) \neq S(n)$  und deshalb  $(S(m), f(x)) \neq (S(n), g)$ , d. h.  $(S(m), f(x)) \in u \setminus \{(S(n), g)\} = \hat{u}$ .

Für  $m = n$  ist aber  $(m, x) = (n, x) = (n, c)$  und  $(S(m), f(x)) = (S(n), f(c)) \neq (S(n), g)$ , also ebenfalls  $(S(m), f(x)) \in u \setminus \{(S(n), g)\} = \hat{u}$ .

Damit ist die Implikation mit ? bewiesen und wir haben  $\hat{u} \in \mathfrak{C}$ , was wiederum ein Widerspruch zu den Definitionen von  $u$  und  $\hat{u}$  ist.

Die Relation  $u$  ist somit eine Abbildung von  $D$  nach  $X$ . Wegen  $u \in \mathfrak{C}$  gilt insbesondere  $(d, a) \in u$ , d. h.  $u_d = a$ . Ist nun  $u_n = x$  also  $(n, x) \in u$ , dann gilt nach Definition von  $\mathfrak{C}$

$$(S(n), f(u_n)) = (S(n), f(x)) \in u.$$

Dies bedeutet aber nicht anderes als  $u_{S(n)} = f(u_n)$ , womit auch (2.2) bewiesen ist.  $\square$

Wir formulieren jetzt noch eine etwas allgemeinere Version des Rekursionstheorems. Der Beweis verläuft ganz analog.

**Satz 2.8.** *Sei  $(D, S, d)$  ein Peano-System,  $X$  eine beliebige Menge,  $a \in X$  und  $f_n: X \rightarrow X$ ,  $n \in D$ , eine Folge von Abbildungen von  $X$  in sich, dann gibt es genau eine Folge  $u = (u_n)_{n \in D}$  in  $X$  mit*

$$(2.3) \quad u_d = a, \quad u_{S(n)} = f_n(u_n) \quad (n \in D).$$

Eine Anwendung des Rekursionstheorems, d. h. die Definition einer Folge durch (2.2) oder (2.3) nennt man Definition durch Rekursion. Eine etwas ungewöhnliche Anwendung des Rekursionstheorems ist der Beweis des folgenden Satzes.

**Satz 2.9** (Eindeutigkeit von Peano-Systemen). *Seien  $(D, S, d)$  und  $(D', S', d')$  Peano-Systeme, dann existiert genau eine Abbildung  $\varphi: D \rightarrow D'$  mit*

$$(2.4) \quad \varphi(d) = d', \quad \varphi(S(n)) = S'(\varphi(n)) \quad (n \in D).$$

Die Abbildung  $\varphi$  ist bijektiv.

*Beweis.* Wir wenden das Rekursionstheorem auf  $X = D'$ ,  $a = d'$  und  $f = S'$  an. Damit existiert genau eine Abbildung  $\varphi: D \rightarrow D'$  (Folge in  $D'$ ), die (2.4) erfüllt. Damit sind schon Existenz und Eindeutigkeit von  $\varphi$  bewiesen.

Um die Bijektivität von  $\varphi$  zu zeigen, vertauschen wir die Rollen von  $D$  und  $D'$  und erhalten eine eindeutig bestimmte Abbildung  $\psi: D' \rightarrow D$  mit

$$(2.5) \quad \psi(d') = d, \quad \psi(S'(n)) = S(\psi(n)) \quad (n \in D').$$

Setzt man jetzt  $\Phi := \psi \circ \varphi$ , dann ist  $\Phi: D \rightarrow D$  mit  $\Phi(d) = \psi(\varphi(d)) = \psi(d') = d$  und

$$\Phi(S(n)) = \psi(\varphi(S(n))) \stackrel{(2.4)}{=} \psi(S'(\varphi(n))) \stackrel{(2.5)}{=} S(\psi(\varphi(n))) = S(\Phi(n)) \quad (n \in D),$$

also

$$(2.6) \quad \Phi(d) = d, \quad \Phi(S(n)) = S(\Phi(n)) \quad (n \in D).$$

Nach dem Rekursionstheorem mit  $X = D$ ,  $a = d$ ,  $f = S$  ist  $\Phi$  die einzige Abbildung von  $D$  in sich, die (2.6) erfüllt. Andererseits hat aber auch die Identität  $I_D$  die Eigenschaft (2.6), d. h., es muss  $\Phi = \psi \circ \varphi = I_D$  gelten. Analog erhält man  $\varphi \circ \psi = I_{D'}$ . Nach Lemma 1.39b ist damit  $\varphi$  bijektiv und die gesuchte Abbildung von  $D$  nach  $D'$ .  $\square$

Nach Satz 2.9 sind alle Peano-Systeme gleichberechtigt. Deshalb benutzen wir im Folgenden das Standardmodell  $(\mathbb{N}_0, S^+, 0)$  stellvertretend für alle anderen. Für  $(\mathbb{N}_0, S^+, 0)$  schreiben wir in der Regel einfach  $\mathbb{N}_0$  und sprechen wie schon in Abschnitt 1.3 von der Menge der natürlichen Zahlen (einschließlich der 0). Wir werden aber ausschließlich die in Satz 1.46 enthaltenen Eigenschaften von  $\mathbb{N}_0$  benutzen und nicht solche, die aus der speziellen Konstruktion mittels  $n^+ = n \cup \{n\}$  folgen. Die Eigenschaften aus Satz 1.46 sind ja genau die, die in Definition 2.1 für ein Peano-System gefordert werden.

Als eine weitere Anwendung des Rekursionstheorems beweisen wir jetzt den Satz von Schröder-Bernstein (Satz 1.73).

**Beweis von Satz 1.73.** Wir müssen nur noch die Implikation „ $\implies$ “ zeigen. Dazu beweisen wir zunächst einen

**Hilfssatz.** *Ist  $A$  eine Menge,  $f: A \rightarrow A$  injektiv und  $B$  eine weitere Menge mit  $f(A) \subset B \subset A$ , dann ist  $A \sim B$ .*

*Beweis des Hilfssatzes.* Mithilfe des Rekursionstheorems definieren wir zwei Folgen in  $\mathfrak{P}(A)$  durch

$$\begin{aligned} A_0 &:= A, & A_{S^+(n)} &:= f(A_n) \quad (n \in \mathbb{N}_0) \\ B_0 &:= B, & B_{S^+(n)} &:= f(B_n) \quad (n \in \mathbb{N}_0). \end{aligned}$$

Setzen wir noch  $C := \bigcup_{n \in \mathbb{N}_0} (A_n \setminus B_n)$ , dann ist

$$C \subset A, \quad A \setminus C \subset B, \quad B = (A \setminus C) \cup (B \cap C).$$

Wir definieren jetzt eine Abbildung  $g: A \rightarrow B$  durch

$$g(x) := \begin{cases} f(x), & x \in C \\ x, & x \in A \setminus C. \end{cases}$$

Der Hilfssatz ist bewiesen, wenn wir zeigen können, dass  $g$  bijektiv ist.

Aus der Injektivität von  $f$  folgt zunächst, dass (vgl. Lemma 1.37)

$$x \in A_n \setminus B_n \implies g(x) = f(x) \in f(A_n \setminus B_n) = f(A_n) \setminus f(B_n) = A_{S^+(n)} \setminus B_{S^+(n)}.$$

Damit ist  $g|_C = f|_C$  eine injektive Funktion von  $C$  in sich und man sieht ganz leicht, dass auch  $g$  injektiv ist.

Um die Surjektivität von  $g$  zu zeigen, wählen wir ein  $y \in B = (A \setminus C) \cup (B \cap C)$ . Ist  $y \in A \setminus C$ , dann ist  $g(y) = y$ , also  $y \in g(A)$ . Ist dagegen  $y \in B \cap C$ , dann existiert ein  $n \in \mathbb{N}_0$  mit  $y \in A_n \setminus B_n$ . Wegen  $y \in B$  und  $A_0 \setminus B_0 = A \setminus B$  muss aber  $n \neq 0$  sein, d. h. es existiert ein  $m \in \mathbb{N}_0$  mit  $n = S^+(m)$  und es folgt

$$y \in A_{S^+(m)} \setminus B_{S^+(m)} = f(A_m) \setminus f(B_m) = f(A_m \setminus B_m) \subset f(C) = g(C) \subset g(A).$$

In jedem Fall gilt also  $y \in g(A)$ . Damit ist  $B = g(A)$  und der Hilfssatz ist bewiesen.  $\square$

Der Beweis des Satzes von Schröder-Bernstein wird nun auf diesen Hilfssatz zurückgeführt. Wegen  $X \preceq Y$  und  $Y \preceq X$  existieren zwei injektive Abbildungen  $\varphi: X \rightarrow Y$  und  $\psi: Y \rightarrow X$ . Im Hilfssatz wählen wir jetzt

$$A := X, \quad B := \psi(Y) \subset A, \quad f := \psi \circ \varphi: A \rightarrow A.$$

$f$  ist als Zusammensetzung injektiver Abbildungen ebenfalls injektiv und wegen  $f(A) = \psi(\varphi(X)) \subset \psi(Y) = B$  sind alle Voraussetzungen des Hilfssatzes erfüllt. Wir erhalten deshalb  $X \sim \psi(Y)$ . Da  $\psi$  injektiv ist gilt natürlich  $\psi(Y) \sim Y$  also auch  $X \sim Y$ .  $\square$

## 2.2 Die algebraische Struktur der natürlichen Zahlen

### 2.2.1 Arithmetik

In diesem Paragraphen wenden wir das Rekursionstheorem 2.8 auf  $(\mathbb{N}_0, S^+, 0)$  an, um eine Addition, eine Multiplikation und eine Anordnung einzuführen. Grundlage ist die folgende aus der Algebra bekannte Definition.

**Definition 2.10.** Eine nicht leere Menge  $H$  mit einer inneren Verknüpfung (Abbildung)

$$H \times H \rightarrow H, \quad (a, b) \mapsto a \cdot b,$$

heißt *Halbgruppe*, wenn das Assoziativgesetz

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad (a, b, c \in H)$$

gilt. Man nennt  $H$  *abelsch*, wenn das Kommutativgesetz

$$a \cdot b = b \cdot a \quad (a, b \in H)$$

gilt, und man sagt, dass in der Halbgruppe  $H$  die Kürzungsregel gilt, wenn für alle  $a, b, c \in H$  aus  $a \cdot b = a \cdot c$  oder  $b \cdot a = c \cdot a$  stets  $b = c$  folgt.

Eine Halbgruppe  $H$  heißt *Monoid*, wenn  $H$  ein neutrales Element  $e$  besitzt, d. h. wenn ein  $e \in H$  existiert mit

$$e \cdot a = a \cdot e = a \quad (a \in H).$$

Ein Monoid  $H$  heißt *Gruppe*, wenn jedes  $a \in H$  ein inverses Element  $b \in H$  besitzt, d. h. wenn zu jedem  $a \in H$  ein  $b \in H$  existiert mit

$$a \cdot b = b \cdot a = e.$$

Man nennt die Halbgruppe (bzw. Gruppe)  $H$  *zyklisch*, wenn ein  $a \in H$  existiert, so dass für jede Halbgruppe (bzw. Gruppe)  $H' \subset H$  mit  $a \in H'$  bereits  $H' = H$  gilt. Man schreibt dann auch  $H = \langle a \rangle$  und sagt, dass  $H$  von  $a$  erzeugt wird.

Das neutrale Element  $e$  und die inversen Elemente in Definition 2.10 sind, sofern sie existieren, eindeutig bestimmt (Algebra).

Wir benutzen nun wie angekündigt Satz 2.8, um auf  $\mathbb{N}_0$  eine Addition zu definieren. Dazu definieren wir zunächst für  $m \in \mathbb{N}_0$  eine Abbildung  $\varphi_m: \mathbb{N}_0 \rightarrow \mathbb{N}_0$  durch

$$(2.7) \quad \varphi_m(0) := m, \quad \varphi_m(S^+(n)) := S^+(\varphi_m(n)).$$

Wendet man Satz 2.7 auf  $X = \mathbb{N}_0$ ,  $a = m$  und  $f = S^+$  an, so folgt, dass  $\varphi_m$  durch (2.7) eindeutig bestimmt ist. Daher können wir jetzt mit Hilfe von  $\varphi_m$  eine innere Verknüpfung auf  $\mathbb{N}_0$  definieren.

**Definition 2.11.** Sei  $\varphi_m$  durch (2.7) definiert. Die Abbildung  $+: \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \mathbb{N}_0$ ,  $(m, n) \mapsto m + n := \varphi_m(n)$  heißt Addition auf  $\mathbb{N}_0$ . Dabei heißen  $m$  und  $n$  Summanden, und  $m + n$  heißt die Summe von  $m$  und  $n$ .

**Bemerkung 2.12.** Man beachte, dass es in der Definition der Addition zumindest zunächst auf die Reihenfolge der Summanden ankommt.

Aus (2.7) folgt zunächst  $m + 0 = \varphi_m(0) = m$  und wegen  $1 = S^+(0)$  (vgl. (1.1)) gilt

$$m + 1 = \varphi_m(1) = \varphi_m(S^+(0)) = S^+(\varphi_m(0)) = S^+(m).$$

Wir können deshalb im Folgenden das Symbol  $S^+$  meistens durch  $+ 1$  ersetzen, z. B.

$$m + (n + 1) = \varphi_m(n + 1) = \varphi(S^+(n)) = S^+(\varphi_m(n)) = S^+(m + n) = (m + n) + 1$$

Die Addition erfüllt also die beiden Gleichungen

$$(2.8) \quad m + 0 = m, \quad m + (n + 1) = (m + n) + 1 \quad (m, n \in \mathbb{N}_0).$$

Die algebraischen Eigenschaften der Addition auf  $\mathbb{N}_0$  sind enthalten in

**Satz 2.13.**  $\mathbb{N}_0$  ist bezüglich der Addition eine abelsche Halbgruppe, in der die Kürzungsregel gilt.  $\mathbb{N}_0$  ist ein Monoid mit neutralem Element 0.

*Beweis.* Aus der Definition folgt, dass die Addition eine innere Verknüpfung auf  $\mathbb{N}_0$  ist.

a) *Assoziativgesetz:* Für alle  $k, m, n \in \mathbb{N}_0$  gilt  $(k + m) + n = k + (m + n)$ .

Wir beweisen dies durch Induktion nach  $n$ . Man beachte, dass wegen  $S^+(n) = n + 1$  der Induktionsschluss  $n \rightarrow S^+(n)$  ab jetzt die bekannte Form  $n \rightarrow n + 1$  hat.

Für  $n = 0$  folgt die Aussage unmittelbar aus (2.8), denn

$$(k + m) + 0 = k + m = k + (m + 0).$$

Gilt das Assoziativgesetz für  $n \in \mathbb{N}_0$ , so hat man

$$\begin{aligned} (k + m) + (n + 1) &\stackrel{(2.8)}{=} ((k + m) + n) + 1 \stackrel{\text{I.V.}}{=} (k + (m + n)) + 1 \\ &\stackrel{(2.8)}{=} k + ((m + n) + 1) \stackrel{(2.8)}{=} k + (m + (n + 1)). \end{aligned}$$

Dabei verweist I.V. auf die Induktionsvoraussetzung.

b) *Kommutativgesetz:* Für alle  $m, n \in \mathbb{N}_0$  gilt:  $m + n = n + m$ .

Wir beweisen zunächst durch vollständige Induktion nach  $m$  die Spezialfälle

$$(2.9) \quad m + 0 = 0 + m \quad (m \in \mathbb{N}_0),$$

$$(2.10) \quad m + 1 = 1 + m \quad (m \in \mathbb{N}_0).$$

Bei (2.9) ist der Induktionsanfang  $m = 0$  unmittelbar klar und hinsichtlich  $m \rightarrow m + 1$  gilt

$$(m + 1) + 0 \stackrel{(2.8)}{=} m + 1 \stackrel{(2.8)}{=} (m + 0) + 1 \stackrel{\text{I.V.}}{=} (0 + m) + 1 \stackrel{\text{a)}}{=} 0 + (m + 1).$$

Bei (2.10) ist der Induktionsanfang  $m = 0$  in (2.9) enthalten, und der Induktionsschluss ist durch

$$(m + 1) + 1 \stackrel{\text{I.V.}}{=} (1 + m) + 1 \stackrel{\text{a)}}{=} 1 + (m + 1)$$

gegeben.

Jetzt können wir das Kommutativgesetz  $m + n = n + m$  in der allgemeinen Form durch Induktion nach  $n$  beweisen. Der Induktionsanfang  $n = 0$  ist dabei durch (2.9) bereits bewiesen und aus der Induktionsvoraussetzung  $m + n = n + m$  erhält man

$$\begin{aligned} m + (n + 1) &\stackrel{\text{a)}}{=} (m + n) + 1 \stackrel{\text{I.V.}}{=} (n + m) + 1 \\ &\stackrel{\text{a)}}{=} n + (m + 1) \stackrel{(2.10)}{=} n + (1 + m) \stackrel{\text{a)}}{=} (n + 1) + m. \end{aligned}$$

c) *Kürzungsregel:* Für alle  $k, m, n \in \mathbb{N}_0$  folgt aus  $m + k = n + k$  stets  $m = n$ .

Wir verwenden eine Induktion nach  $k$ . Der Induktionsanfang  $k = 0$  ist klar. Nehmen wir jetzt an, dass aus  $m + k = n + k$  bereits  $m = n$  folgt, und setzen  $m + (k + 1) = n + (k + 1)$  voraus, dann ergibt sich mit dem Assoziativgesetz daraus

$$S^+(m + k) = (m + k) + 1 = m + (k + 1) = n + (k + 1) = (n + k) + 1 = S^+(n + k).$$

Die Injektivität von  $S^+$  impliziert jetzt  $m + k = n + k$  und aus der Induktionsvoraussetzung folgt  $m = n$ .

d) *Neutrales Element:*  $m + 0 = 0 + m = m$ .

Dies folgt unmittelbar aus (2.8) und der Kommutativität der Addition.  $\square$

**Lemma 2.14.** a) Sind  $m, n \in \mathbb{N}_0$  mit  $m + n = 0$ , dann gilt  $m = n = 0$ .

b) Sind  $m, n \in \mathbb{N}_0$  mit  $m + n = 1$ , dann gilt  $m = 0$  und  $n = 1$  oder  $m = 1$  und  $n = 0$ .

*Beweis.* a) Angenommen  $m \neq 0$ , dann existiert wegen  $\mathbb{N}_0 = \{0\} \cup S^+(\mathbb{N}_0)$  (vgl. Folgerung 2.6) ein  $k \in \mathbb{N}_0$  mit  $m = S^+(k) = k + 1$ . Damit folgte dann

$$0 = m + n = (k + 1) + n = (k + n) + 1 = S^+(k + n),$$

was ein Widerspruch zu (P3) ist. Also muss  $m = 0$  sein und ebenso zeigt man  $n = 0$ .

b) Wegen  $1 = S^+(0) \neq 0$  (vgl. (P3)) muss  $m \neq 0$  oder  $n \neq 0$  sein. Sei  $m \neq 0$ , dann gilt wie oben  $m = k + 1$  mit einem  $k \in \mathbb{N}_0$  und

$$0 + 1 = 1 = m + n = (k + 1) + n = (k + n) + 1.$$

Mit der Kürzungsregel folgt  $k + n = 0$  und nach Teil a) gilt  $k = n = 0$ . Deshalb ist also  $m = 1$  und  $n = 0$ . Beginnt man mit der Annahme  $n \neq 0$ , dann erhält man analog  $m = 0$  und  $n = 1$ .  $\square$

Wir kommen jetzt zur Definition der *Multiplikation*. Dazu definieren wir zunächst für festes  $m \in \mathbb{N}_0$  rekursiv eine Folge  $n \mapsto m \cdot n$  durch

$$(2.11) \quad m \cdot 0 := 0, \quad m \cdot (n + 1) := (m \cdot n) + m \quad (n \in \mathbb{N}_0).$$

Die Definition der Multiplikation als innere Verknüpfung auf  $\mathbb{N}_0$  folgt nun in

**Definition 2.15.** Die Abbildung  $\cdot: \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \mathbb{N}_0$ ,  $(m, n) \mapsto m \cdot n$ , wobei  $m \cdot n$  durch (2.11) gegeben ist, heißt Multiplikation auf  $\mathbb{N}_0$ . Dabei heißen  $m$  und  $n$  Faktoren, und  $m \cdot n$  heißt das Produkt von  $m$  und  $n$ .

**Satz 2.16.**  $\mathbb{N}_0$  ist bezüglich der Multiplikation eine abelsche Halbgruppe mit 1 als neutralem Element, in der die Kürzungsregel in der Form

$$k \cdot m = k \cdot n \implies m = n \quad (k, m, n \in \mathbb{N}_0, k \neq 0)$$

gilt. Darüber hinaus gilt das Distributivgesetz

$$(k + m) \cdot n = (k \cdot n) + (m \cdot n) \quad (k, m, n \in \mathbb{N}_0).$$

*Beweis.* Offensichtlich ist die Multiplikation eine innere Verknüpfung auf  $\mathbb{N}_0$ .

a) *Distributivgesetz:* Für alle  $k, m, n \in \mathbb{N}_0$  gilt:  $(k + m) \cdot n = (k \cdot n) + (m \cdot n)$ .

Im Fall  $n = 0$  hat man

$$(k + m) \cdot 0 \stackrel{(2.11)}{=} 0 = 0 + 0 \stackrel{(2.11)}{=} (k \cdot 0) + (m \cdot 0).$$

Beim Induktionsschritt  $n \rightarrow n + 1$  erhält man mit dem Kommutativgesetz und dem Assoziativgesetz der Addition

$$\begin{aligned} (k+m) \cdot (n+1) &\stackrel{(2.11)}{=} ((k+m) \cdot n) + (k+m) \stackrel{\text{I.V.}}{=} ((k \cdot n) + (m \cdot n)) + (k+m) \\ &= ((k \cdot n) + k) + ((m \cdot n) + m) \stackrel{(2.11)}{=} ((k \cdot (n+1)) + (m \cdot (n+1))). \end{aligned}$$

b) *Neutrales Element:* Für alle  $m \in \mathbb{N}_0$  gilt:  $m \cdot 1 = m = 1 \cdot m$ .

Der Fall  $m = 0$  folgt aus (2.11) und der Induktionsschluss  $m \rightarrow m + 1$  ist gegeben durch

$$(m+1) \cdot 1 \stackrel{(2.11)}{=} m+1 \quad \text{und} \quad 1 \cdot (m+1) \stackrel{(2.11)}{=} (1 \cdot m) + 1 \stackrel{\text{I.V.}}{=} m+1.$$

c) *Kommutativgesetz:* Für alle  $m, n \in \mathbb{N}_0$  gilt:  $m \cdot n = n \cdot m$ .

Der Fall  $n = 0$ , also  $m \cdot 0 = 0 \cdot m = 0$ , folgt wieder unmittelbar aus (2.11). Beim Induktionsschritt  $n \rightarrow n + 1$  folgert man

$$m \cdot (n+1) \stackrel{(2.11)}{=} (m \cdot n) + m \stackrel{\text{I.V.}}{=} (n \cdot m) + m \stackrel{\text{b)}}{=} (n \cdot m) + (1 \cdot m) \stackrel{\text{a)}}{=} (n+1) \cdot m.$$

d) *Assoziativgesetz:* Für alle  $k, m, n \in \mathbb{N}_0$  gilt:  $(k \cdot m) \cdot n = k \cdot (m \cdot n)$ .

Der Fall  $n = 0$ , also  $(k \cdot m) \cdot 0 = k \cdot (m \cdot 0)$ , folgt aus (2.11) und dem Kommutativgesetz. Beim Induktionsschritt  $n \rightarrow n + 1$  ergibt sich

$$\begin{aligned} (k \cdot m) \cdot (n+1) &\stackrel{(2.11)}{=} [(k \cdot m) \cdot n] + (k \cdot m) \stackrel{\text{I.V.}}{=} [k \cdot (m \cdot n)] + (k \cdot m) \\ &\stackrel{\text{c)}}{=} [(m \cdot n) \cdot k] + (m \cdot k) \stackrel{\text{a)}}{=} [(m \cdot n) + m] \cdot k \stackrel{(2.11)}{=} [m \cdot (n+1)] \cdot k \stackrel{\text{c)}}{=} k \cdot [m \cdot (n+1)]. \end{aligned}$$

e) *Kürzungsregel:* Für  $k, m, n \in \mathbb{N}_0$ ,  $k \neq 0$  folgt aus  $k \cdot m = k \cdot n$  stets  $m = n$ .

Wir verwenden eine Induktion nach  $m$ . Sei  $m = 0$ , also  $0 = k \cdot 0 = k \cdot n$ . Zeige  $n = 0$ . Wegen  $k \neq 0$  existiert ein  $k' \in \mathbb{N}_0$  mit  $k = k' + 1$ . Es gilt also

$$0 = (k' + 1) \cdot n \stackrel{\text{a)}}{=} k' \cdot n + 1 \cdot n \stackrel{\text{b)}}{=} k' \cdot n + n.$$

Mit Lemma 2.14a) folgt  $n = 0$ .

Nun gelte die Aussage für ein  $m \in \mathbb{N}_0$  und wir nehmen  $k \cdot (m+1) = k \cdot n$  an. Zeige  $m+1 = n$ . Die Annahme  $n = 0$  führt analog zum Induktionsanfang auf einen Widerspruch. Also gilt  $n = n' + 1$  für ein  $n' \in \mathbb{N}_0$ . Damit ist

$$(k \cdot m) + k \stackrel{\text{a), c)}}{=} k \cdot (m+1) = k \cdot n = k \cdot (n' + 1) \stackrel{\text{a), c)}}{=} (k \cdot n') + k.$$

Die Kürzungsregel der Addition (Satz 2.13) impliziert  $k \cdot m = k \cdot n'$  und die Induktionsvoraussetzung  $m = n'$ , d. h.  $m+1 = n'+1 = n$ .  $\square$

Zur Vereinfachung der Darstellung vereinbaren wir wie üblich die Regel „Punkt-rechnung vor Strichrechnung“, d. h. für  $k, m, n \in \mathbb{N}_0$  gilt z. B.

$$k + m \cdot n := k + (m \cdot n).$$

Außerdem lässt man das Multiplikationszeichen  $\cdot$  meistens weg also  $mn := m \cdot n$ .

Wir definieren nun noch die Potenzen  $m^n \in \mathbb{N}_0$ . Dazu wählen wir für festes  $m \in \mathbb{N}_0$  im Rekursionstheorem (Satz 2.7)  $X = \mathbb{N}_0$ ,  $a = 1$  und  $f: \mathbb{N}_0 \rightarrow \mathbb{N}_0$ ,  $n \mapsto mn$ .

**Definition 2.17.** Für  $m, n \in \mathbb{N}_0$  ist die Potenz  $m^n \in \mathbb{N}_0$  definiert durch

$$m^0 := 1, \quad m^{n+1} := m^n \cdot m.$$

Als unmittelbare Folgerung aus dieser Definition und den Rechenregeln der Multiplikation (Satz 2.16) erhält man mittels vollständiger Induktion

**Folgerung 2.18.** Für alle  $k, m, n \in \mathbb{N}_0$  gilt:

- (i)  $m^n m^k = m^{n+k}$ ,
- (ii)  $m^n k^n = (mk)^n$ .
- (iii)  $(m^n)^k = m^{nk}$ .

### 2.2.2 Anordnung

Nachdem die Rechenoperationen eingeführt sind, definieren wir noch eine Ordnungsrelation auf  $\mathbb{N}_0$ .

**Definition 2.19.** a) Für  $m, n \in \mathbb{N}_0$  nennt man  $m$  *kleiner oder gleich*  $n$  (Schreibweise  $m \leq n$ ), wenn es ein  $x \in \mathbb{N}_0$  mit  $m + x = n$  gibt. Man nennt  $m$  (*echt*) *kleiner als*  $n$  und schreibt  $m < n$ , wenn  $m \leq n$  und  $m \neq n$  ist.

b) Die *Größer-oder-gleich-Relation* ( $m \geq n$ ) und die *Größer-Relation* ( $m > n$ ) sind definiert durch

$$m \geq n : \iff n \leq m, \quad m > n \iff n < m.$$

Wir werden im Folgenden zeigen, dass die Relation  $\leq$  eine totale Ordnung auf  $\mathbb{N}_0$  ist (vgl. Definitionen 1.54, 1.61 und dass die Relation  $<$  die zu  $\leq$  gehörende strenge Ordnung im Sinne von Definition 1.58 ist).

**Bemerkungen 2.20.** a) Nach der Kürzungsregel gilt  $m + x = m$  genau dann, wenn  $x = 0$  ist, d. h. es gilt  $m < n$  genau dann, wenn es ein  $x \in \mathbb{N}$  mit  $m + x = n$  gibt. Außerdem gilt

$$(2.12) \quad m \leq n \iff m < n \text{ oder } m = n.$$

b) Sind  $m, n \in \mathbb{N}_0$  mit  $m \leq n$ , also  $m + x = n$  für ein  $x \in \mathbb{N}_0$ , dann ist  $x$  eindeutig bestimmt, denn aus  $m + x = m + y$  folgt nach der Kürzungsregel  $x = y$ . Für  $m \leq n$  kann man deshalb die Subtraktion  $n - m$  definieren durch  $n - m := x$ , wobei  $x$  durch  $m + x = n$  eindeutig bestimmt ist. Die Subtraktion ist aber *keine* innere Verknüpfung auf  $\mathbb{N}_0$ , da sie nicht für alle  $m, n \in \mathbb{N}_0$  definiert ist.

Einige elementare Eigenschaften der oben eingeführten Relationen sind im folgenden Lemma zusammengestellt.

**Lemma 2.21.** Für  $k, l, m \in \mathbb{N}_0$  gilt:

- (i)  $0 \leq k$ ,
- (ii)  $k \leq k$  (Reflexivität),
- (iii)  $k < k + 1$ , insbesondere ist  $0 < 1$ ,
- (iv)  $k \leq k + l$ ,
- (v)  $0 = k$  oder  $1 \leq k$ ,
- (vi)  $k \leq l + 1 \iff k \leq l$  oder  $k = l + 1$ ,
- (vii)  $k \leq m \iff k < m + 1$ ,  $k + 1 \leq m \iff k < m$ ,
- (viii)  $\{j \in \mathbb{N}_0; m < j \wedge j < m + 1\} = \emptyset$ ,
- (ix)  $\{j \in \mathbb{N}_0; m \leq j \wedge j < m + 1\} = \{m\}$ ,
- (x)  $\{j \in \mathbb{N}_0; m < j \wedge j \leq m + 1\} = \{m + 1\}$ ,
- (xi)  $\{j \in \mathbb{N}_0; m \leq j \wedge j \leq m + 1\} = \{m, m + 1\}$ ,
- (xii)  $\{j \in \mathbb{N}_0; j \leq m + 1\} = \{j \in \mathbb{N}_0; j \leq m\} \cup \{m + 1\}$ ,
- (xiii)  $\{j \in \mathbb{N}_0; j < m + 1\} = \{j \in \mathbb{N}_0; j < m\} \cup \{m\}$ .

*Beweis.* Die Aussagen (i)–(iv) folgen direkt aus den Definitionen von  $\leq$  und  $<$ .

(v): Ist  $k = 0$ , sind wir fertig. Anderenfalls existiert ein  $x \in \mathbb{N}_0$  mit  $k = S^+(x) = x + 1$  und nach Definition von  $\leq$  folgt  $1 \leq k$ .

(vi)  $\implies$ : Wegen  $k \leq l + 1$  existiert ein  $y \in \mathbb{N}_0$  mit  $k + y = l + 1$ . Ist  $y = 0$ , dann gilt  $k = l + 1$ . Ist  $y \neq 0$ , dann gilt  $y = y' + 1$  mit einem  $y' \in \mathbb{N}_0$ , d. h.  $k + (y' + 1) = l + 1$ . Mit der Kürzungsregel folgt  $k + y' = l$  also  $k \leq l$ .

$\impliedby$ : Ist  $k = l + 1$ , dann ist nach (ii) auch  $k \leq l + 1$ . Ist dagegen  $k \leq l$ , d. h.  $k + y = l$  für ein  $y \in \mathbb{N}_0$ , dann ist  $k + (y + 1) = (k + y) + 1 = l + 1$  und wegen  $y + 1 \in \mathbb{N}_0$  ist  $k \leq l + 1$ .

(vii) Wir beweisen nur die erste Äquivalenz, die zweite erhält man ganz analog.

$\implies$ : Aus  $k \leq m$  folgt  $k + x = m$  mit  $x \in \mathbb{N}_0$ . Damit ist  $k + (x + 1) = m + 1$  und wegen  $x + 1 \in \mathbb{N}$  gilt  $k < m + 1$  (vgl. Bemerkung 2.20).

$\impliedby$ : Wir haben  $k + y = m + 1$  mit  $y \in \mathbb{N}$ . Da  $y \neq 0$  ist, gilt  $y = y' + 1$  mit  $y' \in \mathbb{N}_0$ , also  $(k + y') + 1 = m + 1$ . Mit der Kürzungsregel folgt  $k + y' = m$ , d. h.  $k \leq m$ .

(viii): Sei  $j \in \mathbb{N}_0$  mit  $m < j$  und  $j < m + 1$ , dann existieren  $x, y \in \mathbb{N}$  mit  $m + x = j$  und  $j + y = m + 1$ . Insgesamt gilt damit

$$m + (x + y) = (m + x) + y = j + y = m + 1$$

und mit der Kürzungsregel folgt  $x + y = 1$ . Nach Lemma 2.14b ist demnach  $x = 0$  oder  $y = 0$  im Widerspruch zu  $x, y \in \mathbb{N}$ . Es gibt also kein  $j \in \mathbb{N}_0$ , dass die Ungleichungen

$m < j$  und  $j < m + 1$  erfüllt, d. h.  $\{j \in \mathbb{N}_0; m < j < m + 1\} = \emptyset$ .

(ix): Sei  $M := \{j \in \mathbb{N}_0; m \leq j < m + 1\}$ , dann ist wegen (ii) und (iii) offensichtlich  $\{m\} \subset M$ . Ist umgekehrt  $j \in M$ , d. h.  $m + x = j$  und  $j + y = m + 1$  für geeignete  $x \in \mathbb{N}_0$ ,  $y \in \mathbb{N}$ , dann erhält man wie im Beweis von (viii) zunächst  $x + y = 1$  und mit Lemma 2.14b folgt unter Beachtung von  $y \neq 0$ , dass  $x = 0$  und damit  $m = j$  sein muss. Damit ist auch die Inklusion  $M \subset \{m\}$  gezeigt.

(x): analog zu (ix).

(xi): Mit  $M := \{j \in \mathbb{N}_0; m \leq j \wedge j \leq m + 1\}$  gilt für  $j \in \mathbb{N}_0$

$$\begin{aligned} j \in M &\iff m \leq j \wedge j \leq m + 1 \stackrel{(iv), (vi)}{\iff} (m \leq j \wedge j < m) \vee j = m + 1 \\ &\stackrel{(ix)}{\iff} j \in \{m\} \vee j \in \{m + 1\} \iff j \in \{m\} \cup \{m + 1\} \iff j \in \{m, m + 1\}. \end{aligned}$$

(xii): Dies folgt aus

$$\begin{aligned} \{j \in \mathbb{N}_0; j \leq m + 1\} &\stackrel{(vi)}{=} \{j \in \mathbb{N}_0; j \leq m \vee j = m + 1\} \\ &= \{j \in \mathbb{N}_0; j \leq m\} \cup \{j \in \mathbb{N}_0; j = m + 1\} = \{j \in \mathbb{N}_0; j \leq m\} \cup \{m + 1\}. \end{aligned}$$

(xiii): Wegen  $j \leq m \iff j < m \vee j = m$  gilt

$$\begin{aligned} \{j \in \mathbb{N}_0; j < m\} \cup \{m\} &= \{j \in \mathbb{N}_0; j < m\} \cup \{j \in \mathbb{N}_0; j = m\} \\ &= \{j \in \mathbb{N}_0; j < m \vee j = m\} = \{j \in \mathbb{N}_0; j \leq m\} \stackrel{(vii)}{=} \{j \in \mathbb{N}_0; j < m + 1\}. \quad \square \end{aligned}$$

Wir zeigen als nächstes, dass  $\leq$  eine totale Ordnung in Sinne von Definition 1.61 ist und dass die arithmetischen Operationen mit dieser Ordnung verträglich sind.

**Satz 2.22.** Für  $k, l, m, n \in \mathbb{N}_0$  gilt:

- (i)  $k \leq l \wedge l \leq m \implies k \leq m$  (Transitivität),
- (ii)  $k \leq l \wedge l \leq k \implies k = l$  (Antisymmetrie),
- (iii)  $k \leq l \vee l \leq k$  (Konnexität),
- (iv)  $k \leq l \iff k + m \leq l + m$  (Monotonie der Addition),
- (v)  $k \leq l \wedge m \leq n \implies k + m \leq l + n$ ,
- (vi)  $k \leq l \implies km \leq lm$  (Monotonie der Multiplikation),
- (vii)  $km \leq lm \wedge m \neq 0 \implies k \leq l$ ,
- (viii)  $k \leq l \wedge m \leq n \implies km \leq ln$ .

*Beweis.* (i): Aus  $k + x = l$  und  $l + y = m$  folgt  $k + (x + y) = l + y = m$ . Also ist  $k \leq m$

(ii): Wegen  $k + x = l$  und  $l + y = k$  ist  $k + (x + y) = l + y = k$ , und mit der Kürzungsregel folgt  $x + y = 0$ . Mit Lemma 2.14a) erhalten wir daraus  $x = 0$  und somit  $k = l$ .

(iii): Sei  $M := \{k \in \mathbb{N}_0; k \leq l \vee l \leq k\}$ . Wir zeigen mit vollständiger Induktion  $M = \mathbb{N}_0$ . Dabei ist der Induktionsanfang durch Lemma 2.21(i) gegeben. Ist nun  $k \in M$ , dann ist  $k + y = l$  oder  $l + y = k$  für ein  $y \in \mathbb{N}_0$ .

1. Fall  $l + y = k$ : Wegen  $l + (y + 1) = k + 1$  ist auch  $l \leq k + 1$  und somit  $k + 1 \in M$ .  
 2. Fall  $k + y = l$ : Ist  $y = 0$ , dann ist  $k = l$  und  $k + 1 = l + 1$ , d. h.  $l \leq k + 1$  und  $k + 1 \in M$ . Ist  $y \neq 0$ , dann ist  $y = y' + 1$  für ein  $y' \in \mathbb{N}_0$  und  $l = k + (y' + 1) = (k + 1) + y'$ . Damit ist auch in diesem Fall  $k + 1 \leq l$  und  $k + 1 \in M$ . Mit (P5) folgt jetzt  $M = \mathbb{N}_0$ .

(iv): Diese Aussage gilt wegen

$$\begin{aligned} k \leq l &\iff k + x = l \iff (k + x) + m = l + m \\ &\iff (k + m) + x = l + m \iff k + m \leq l + m, \end{aligned}$$

wobei wir das Kommutativgesetz, das Assoziativgesetz und die Kürzungsregel der Addition benutzt haben.

(v): Zweimalige Anwendung von (iv) liefert

$$k \leq l \wedge m \leq n \implies k + m \leq l + m \wedge l + m \leq l + n$$

und die Behauptung folgt daraus mit der Transitivität von  $\leq$ .

(vi): Dies erhält man mit dem Distributivgesetz, denn

$$k \leq l \implies k + x = l \implies (k + x)m = lm \implies km + xm = lm \implies km \leq lm.$$

(vii): Wir zeigen dies durch vollständige Induktion über  $k$ , wobei die Aussage für  $k = 0$  wegen  $0 \leq l$  (vgl. Lemma 2.21(i)) offensichtlich richtig ist. Für den Induktionsschluss nehmen wir an, dass  $km \leq lm \implies k \leq l$  gilt. Es folgt dann für ein  $x \in \mathbb{N}_0$

$$\begin{aligned} (k + 1)m \leq lm &\implies km + m \leq lm \implies km + (m + x) = lm \\ &\stackrel{x \neq 0}{\implies} km \leq lm \wedge km \neq lm \stackrel{\text{I.V.}}{\implies} k \leq m \wedge k \neq m \stackrel{\text{La. 2.21(vii)}}{\implies} k + 1 \leq m. \end{aligned}$$

(viii): Dies beweist man ähnlich wie (v) durch zweimalige Anwendung von (vi) unter Ausnutzung der Transitivität.  $\square$

**Folgerung 2.23.** Die  $\leq$ -Relation ist eine totale Ordnung auf  $\mathbb{N}_0$  im Sinne von Definitionen 1.54 und 1.61.

*Beweis.* Die  $\leq$ -Relation ist reflexiv, transitiv und antisymmetrisch (vgl. Lemma 2.21(ii) und Satz 2.22(i),(ii)). Wegen Satz 2.22(iii) ist  $\leq$  sogar eine totale Ordnung.  $\square$

Da  $\leq$  insbesondere eine Halbordnung auf  $\mathbb{N}_0$  definiert, ist  $<$  die zugehörige strenge Halbordnung im Sinne von Definition 1.58. Für  $<$  beweist man zunächst ganz analog zu Satz 2.22

**Satz 2.24.** Für  $k, l, m, n \in \mathbb{N}_0$  gilt:

- (i)  $k < l \wedge l < m \implies k < m$  (Transitivität),
- (ii)  $k < l \iff k + m < l + m$  (Monotonie der Addition),

- (iii)  $k < l \wedge m \leq n \implies k + m < l + n$ ,
- (iv) Ist  $m \neq 0$ , dann gilt  $k < l \iff km < lm$  (Monotonie der Multiplikation),
- (v)  $k < l \wedge m < n \implies km < ln$ .

Außerdem gilt das Trichotomiegesetz (siehe Lemma 1.62(iii)).

**Satz 2.25.** Für alle  $k, l \in \mathbb{N}_0$  gilt genau eine der Beziehungen

$$k < l, \quad k = l, \quad l < k.$$

Aufgrund der Transitivität von  $\leq$  und  $<$  lassen sich Bedingungen vom Typ  $l \leq n \wedge n \leq m$  zu  $l \leq n \leq m$  verkürzen. Die Menge  $\{j \in \mathbb{N}_0; m < j \wedge j \leq m + 1\}$  aus Lemma 2.21(x) kann man damit auch in der Form  $\{j \in \mathbb{N}_0; m < j \leq m + 1\}$  schreiben.

Wir untersuchen jetzt  $\mathbb{N}_0$  auf erste und letzte Elemente (siehe Definition 1.56a).

**Satz 2.26.** a) 0 ist erstes Element von  $\mathbb{N}_0$  bezüglich  $\leq$ , d. h.  $0 \leq k$  für alle  $k \in \mathbb{N}_0$ .

b)  $\mathbb{N}_0$  besitzt kein letztes Element, d. h. es existiert kein  $n \in \mathbb{N}_0$  mit  $k \leq n$  für alle  $k \in \mathbb{N}_0$ .

c) Jede nicht leere Teilmenge  $M$  von  $\mathbb{N}_0$  besitzt ein erstes Element, d. h. es existiert ein  $n \in M$  mit  $n \leq m$  für alle  $m \in M$ .

*Beweis.* a) ist die Aussage von Lemma 2.21(i).

b) Die Annahme, dass  $n$  letztes Element ist, führt wegen  $n < n + 1$  (Lemma 2.21(iii)) sofort zum Widerspruch.

c) Sei  $\emptyset \neq M \subset \mathbb{N}_0$ . Wir müssen zeigen, dass  $M$  ein erstes Element besitzt. Dazu betrachten wir die Menge

$$K := \{k \in \mathbb{N}_0; k \leq m \text{ für alle } m \in M\}.$$

Nach a) gilt zunächst  $0 \in K$ . Sei nun  $m \in M$ , dann ist  $m < m + 1$  (Lemma 2.21(iii)), d. h.  $m + 1 \notin K$ . Damit kann  $K$  aber auch nicht die Bedingung  $(k \in K \implies k + 1 \in K)$  erfüllen, denn aus dieser Bedingung folgte wegen  $0 \in K$  mit (P5) sofort  $K = \mathbb{N}_0$  also ein Widerspruch zu  $m + 1 \notin K$ . Deshalb muss ein  $n \in K$  existieren mit  $n + 1 \notin K$ . Für dieses  $n$  gilt nach Definition von  $K$  insbesondere  $n \leq m$  für alle  $m \in M$  und es existiert ein  $m' \in M$  mit  $\neg(n + 1 \leq m')$ . Nach Satz 2.25 gilt deshalb  $m' < n + 1$ , also insgesamt

$$n \leq m' < n + 1.$$

Mit Lemma 2.21(ix) folgt  $n = m'$ , d. h.  $n \in M$ , und damit ist  $n$  das gesuchte erste Element von  $M$ .  $\square$

**Folgerung 2.27.** Die  $\leq$ -Relation ist eine Wohlordnung auf  $\mathbb{N}_0$  im Sinne von Definition 1.66.

In Satz 2.9 haben wir gezeigt, dass alle Peano-Systeme mengentheoretisch gleichberechtigt sind. Wir wollen dies jetzt auf die algebraischen Eigenschaften ausdehnen.

**Satz 2.28.** Seien  $(D, S, d)$ ,  $(D', S', d')$  zwei Peano-Systeme mit Additionen  $+$  bzw.  $\oplus$ , Multiplikationen  $\cdot$  bzw.  $\odot$  und Kleiner-oder-gleich-Relationen  $\leq$  bzw.  $\otimes$  gemäß Definitionen 2.11, 2.15 und 2.19. Die eindeutig bestimmte Abbildung  $\varphi: D \rightarrow D'$  definiert durch

$$\varphi(d) = d', \quad \varphi(S(n)) = S'(\varphi(n)) \quad (n \in D)$$

aus Satz 2.9 erfüllt für alle  $m, n \in D$

(i)  $\varphi(m + n) = \varphi(m) \oplus \varphi(n)$ ,

(ii)  $\varphi(m \cdot n) = \varphi(m) \odot \varphi(n)$ ,

(iii)  $m \leq n \iff \varphi(m) \otimes \varphi(n)$ .

Wir haben bisher aus den Peano-Axiomen die wesentlichen Eigenschaften von  $\mathbb{N}_0$  hergeleitet. Es stellt sich die Frage, ob es nicht möglich ist auf das ein oder andere dieser Axiome zu verzichten. Die folgenden Beispiele zeigen, dass das Weglassen irgendeines dieser Axiome zu Mengen führt, die man nicht mehr als *natürliche Zahlen* bezeichnen würde.

a) Das System  $(\emptyset, \emptyset, \emptyset)$  erfüllt (P2)–(P5), aber nicht (P1), da  $\emptyset \notin \emptyset$ .

b) Das System  $(\{\emptyset\}, S, \emptyset)$  mit  $S(\emptyset) := \{\emptyset\}$  erfüllt (P1), (P3), (P4) und (P5), aber nicht (P2), da  $S$  keine Abbildung von  $\{\emptyset\}$  in sich ist, sondern  $S: \{\emptyset\} \rightarrow \{\{\emptyset\}\}$ .

c) Das System  $(\{\emptyset\}, S, \emptyset)$  mit  $S(\emptyset) := \emptyset$  erfüllt (P1), (P2), (P4) und (P5), aber nicht (P3).

d) Das System  $(\{\emptyset, \{\emptyset\}\}, S, \emptyset)$  mit  $S(\emptyset) = S(\{\emptyset\}) := \{\emptyset\}$  erfüllt (P1), (P2), (P3) und (P5), aber nicht (P4), da  $S$  nicht injektiv ist.

e) Sei  $(D, S, d)$  ein beliebiges Peano-System und  $x \notin D$ . (Ein solches  $x$  muss es geben, denn sonst wäre  $D$  die Allmenge.) Setze  $D^* := D \cup \{x\}$  und definiere

$$S^*: D^* \rightarrow D^*, \quad n \mapsto \begin{cases} S(n), & n \in D \\ x, & n = x. \end{cases}$$

Das System  $(D^*, S^*, d)$  erfüllt (P1)–(P4), aber nicht (P5). Für  $D$  gilt nämlich  $D \subset D^*$  sowie

$$d \in D \text{ und } (n \in D \implies S^*(n) = S(n) \in D),$$

aber es gilt  $D \neq D^*$ .

Es ist klar, dass die Systeme aus a), b), c) und d) nicht als Modelle der natürlichen Zahlen in Frage kommen. Würde man ein System wie  $(D^*, S^*, d)$  aus e) als Modell der natürlichen Zahlen wählen, dann erhielte man durch wiederholtes Nachfolger-Bilden *nicht* die ganze Menge  $D^*$ , was ebenfalls der Vorstellung von den natürlichen Zahlen widerspricht. Dies zeigt, dass alle fünf Peano-Axiome zur Beschreibung eines vernünftigen Modells der natürlichen Zahlen notwendig sind.

**Bemerkung.** Bisher haben wir das Beweisprinzip der vollständigen Induktion dazu benutzt, um die Gültigkeit einer Aussage  $A(n)$  für alle  $n \in \mathbb{N}_0$  zu zeigen. Man kann dieses Prinzip aber auch dazu benutzen, die Gültigkeit einer Aussage  $A(n)$  für alle  $n \geq n_0$  für beliebiges  $n_0 \in \mathbb{N}_0$  zu beweisen. Dazu zeigt man

- (i)  $A_{n_0}$  ist richtig (Induktionsanfang).  
(ii) Für alle  $n \geq n_0$  gilt: Wenn  $A(n)$  richtig ist, dann auch  $A(n+1)$ .

Um einzusehen, dass damit tatsächlich  $A(n)$  für alle  $n \geq n_0$  bewiesen ist, betrachtet man die Menge

$$M := \{j \in \mathbb{N}_0; A(n_0 + j)\}.$$

Aus (i) und (ii) erhält man dann

- (i)\*  $0 \in M$ ,  
(ii)\*  $j \in M \implies j+1 \in M$

und mit (P5) folgt  $M = \mathbb{N}_0$  (siehe auch Satz 1.43). Damit ist aber  $A(n_0 + j)$  für alle  $j \in \mathbb{N}_0$  wahr bzw.  $A(n)$  für alle  $n \geq n_0$ .

## 2.3 Endliche und unendliche Mengen

Für  $n \in \mathbb{N}_0$  heißt

$$A_n := \{k \in \mathbb{N}_0; k < n\}$$

das  $n$ -te Anfangsstück von  $\mathbb{N}_0$ .

**Bemerkung 2.29.** Nach Lemma 2.21(i),(xiii) gilt  $A_0 = \emptyset = 0$  und  $A_{n+1} = A_n \cup \{n\}$ , d. h.  $A_1 = \{0\}$ ,  $A_2 = \{0, 1\}$ ,  $A_3 = \{0, 1, 2\}$ , usw. Benutzt man das Standardmodell der natürlichen Zahlen aus Abschnitt 1.3, dann gilt sogar  $A_n = n$  (Beweis durch Induktion).

**Lemma 2.30.** Für  $m, n \in \mathbb{N}_0$  gilt

- (i)  $m \leq n \iff A_m \subset A_n$ ,  
(ii)  $m = n \iff A_m = A_n$ ,  
(iii)  $A_m \subset A_n \vee A_n \subset A_m$ .

*Beweis.* (i) Ist  $m \leq n$ , dann folgt  $A_m \subset A_n$  aus der Transitivität von  $<$ . Sei jetzt umgekehrt  $A_m \subset A_n$ . Für  $m = 0$  ist wegen Lemma 2.21(i) nichts mehr zu zeigen. Anderenfalls existiert ein  $m' \in \mathbb{N}_0$  mit  $m' + 1 = m$ , d. h.  $m' < m$  und  $m' \in A_m$ . Wegen  $A_m \subset A_n$  ist auch  $m' \in A_n$ , d. h.  $m' < n$ . Nach Lemma 2.21(vii) ist dies äquivalent zu  $m' + 1 \leq n$ , also  $m \leq n$ .

(ii) Die Richtung  $\implies$  ist klar. Für die Umkehrung erhält man aus  $A_m = A_n$  mit (i) die Ungleichungen  $m \leq n$  und  $m \geq n$ . Die Behauptung folgt jetzt aus Satz 2.22(ii).

(iii) folgt aus (i) und Satz 2.22(iii). □

Die Anfangsstücke werden uns als Vergleichsmengen zur Bestimmung der Anzahl der Elemente einer endlichen Menge dienen. Bevor wir aber *endlich* und *Anzahl der Elemente einer Menge* überhaupt definieren können, benötigen wir noch einige weitere Eigenschaften der Anfangsstücke.

**Lemma 2.31.** Sei  $n \in \mathbb{N}_0$  und  $\varphi: A_n \rightarrow A_n$  injektiv, dann ist  $\varphi$  auch surjektiv.

*Beweis.* Wir machen eine Induktion nach  $n$ . Für den Induktionsanfang  $n = 0$  hat man dabei nur zu beachten, dass  $A_0 = \emptyset$  ist, und dass  $\varphi = \emptyset$  die einzige Abbildung von  $\emptyset \rightarrow \emptyset$  ist.  $\emptyset$  ist aber als Abbildung sowohl injektiv als auch surjektiv.

$n \rightarrow n + 1$ : Sei  $\varphi: A_{n+1} \rightarrow A_{n+1}$  injektiv. Wir unterscheiden zwei Fälle:

1. *Fall  $\varphi(A_n) \subset A_n$ :* Die Funktion  $\varphi|_{A_n}: A_n \rightarrow A_n$  ist als Restriktion einer injektiven Abbildung ebenfalls injektiv und nach Induktionsvoraussetzung auch surjektiv. Da  $\varphi$  injektiv ist, muss  $\varphi(n) = n$  sein. Also gilt nach Lemma 1.31(iv)  $\varphi(A_{n+1}) = \varphi(A_n) \cup \varphi(\{n\}) = \varphi|_{A_n}(A_n) \cup \varphi(\{n\}) = A_n \cup \{n\} = A_{n+1}$ , d. h.  $\varphi$  ist surjektiv.

2. *Fall  $\varphi(m) = n$  für ein  $m \in A_n$ :* Weil  $\varphi$  injektiv ist, folgt  $\varphi(k) \neq n$  und somit  $\varphi(k) \in A_n$  für alle  $k \in A_{n+1}$ ,  $k \neq m$ . Setzt man nun

$$\psi: A_n \rightarrow A_n, k \mapsto \begin{cases} \varphi(k), & k \neq m \\ \varphi(n), & k = m, \end{cases}$$

dann ist  $\psi$  injektiv und nach Induktionsvoraussetzung surjektiv. Nach Definition von  $\psi$  ist deshalb  $A_n = \psi(A_n) \subset \varphi(A_{n+1})$  und wegen  $\varphi(m) = n$  gilt sogar  $A_{n+1} \subset \varphi(A_{n+1})$ . Dies bedeutet aber, dass  $\varphi$  surjektiv ist.  $\square$

*Zur Erinnerung (vgl. Definition 1.69):* Zwei Mengen  $X$  und  $Y$  heißen gleich mächtig (Schreibweise  $X \sim Y$  oder  $X \simeq Y$ ), wenn eine bijektive Abbildung von  $X$  auf  $Y$  existiert. Ein Menge  $Y$  heißt mindestens so mächtig wie eine Menge  $X$  (Schreibweise  $X \preceq Y$  oder  $Y \succeq X$ ), wenn eine bijektive Abbildung von  $X$  auf eine Teilmenge von  $Y$  existiert, d. h. wenn eine injektive Abbildung von  $X$  nach  $Y$  existiert. Man sagt auch „ $Y$  ist mächtiger als  $X$ “ oder „ $X$  ist weniger mächtig als  $Y$ “.

**Bemerkung 2.32.** Ist  $X \subset Y$ , dann gilt offensichtlich auch  $X \preceq Y$ , denn die Inklusionsabbildung  $\text{Id}_X: X \rightarrow Y$  ist eine geeignete injektive Abbildung von  $X$  nach  $Y$ . Ebenso folgt aus  $X = Y$  die Gleich-Mächtigkeit von  $X$  und  $Y$ , also  $X \sim Y$ , wobei man die Identität auf  $X$  als Bijektion wählen kann. Die Umkehrungen dieser Aussagen gelten allerdings nicht, wie man sich an einfachen Beispielen klar machen kann.

Die wesentlichen Eigenschaften der Anfangsstücke  $A_n$  sind im folgenden Satz zusammengefasst.

**Satz 2.33.** Für  $m, n \in \mathbb{N}_0$  gilt

$$(i) \quad m \leq n \iff A_m \subset A_n \iff A_m \preceq A_n,$$

$$(ii) \quad m = n \iff A_m = A_n \iff A_m \sim A_n.$$

*Beweis.* (i) Es ist nur noch  $A_m \subset A_n \iff A_m \preceq A_n$  zu zeigen, der Rest folgt aus Lemma 2.30 und Bemerkung 2.32. Sei deshalb  $A_m \preceq A_n$  und  $\varphi: A_m \rightarrow A_n$  injektiv. Nehmen wir jetzt  $A_m \not\subset A_n$  an, dann folgt aus Lemma 2.30(iii)  $A_n \not\subseteq A_m$  und mit der Inklusionsabbildung  $I_{A_n}: A_n \rightarrow A_m$ ,  $k \mapsto k$ , erhalten wir eine injektive Abbildung  $(I_{A_n} \circ \varphi): A_m \rightarrow A_m$ , die nach Lemma 2.31 auch surjektiv ist. Dies ist aber ein Widerspruch wegen

$$A_m = (I_{A_n} \circ \varphi)(A_m) = \varphi(A_m) \subset A_n \subsetneq A_m.$$

(ii) Auch hier ist nur noch  $A_m = A_n \iff A_m \sim A_n$  zu zeigen. Das folgt aber aus (i), da  $A_m \sim A_n$  sowohl  $A_m \preceq A_n$  als auch  $A_n \preceq A_m$  impliziert.  $\square$

**Folgerung 2.34.** *Ist  $M \sim A_m$  und  $M \sim A_n$  für  $m, n \in \mathbb{N}_0$ , dann ist  $m = n$ .*

*Beweis.* Sind  $\varphi: M \rightarrow A_m$  und  $\psi: M \rightarrow A_n$  beide bijektiv, dann ist  $\psi \circ \varphi^{-1}: A_m \rightarrow A_n$  ebenfalls bijektiv und nach Satz 2.33(ii) ist  $m = n$ .  $\square$

**Definition 2.35.** a) Eine Menge  $M$  heißt endlich, wenn es ein  $n \in \mathbb{N}_0$  gibt mit  $M \sim A_n$ . Man nennt die eindeutig bestimmte Zahl  $n$  die Anzahl der Elemente von  $M$  oder die Mächtigkeit (Kardinalität) von  $M$  und schreibt  $|M| = n$ ,  $\sharp M = n$  oder  $\text{card } M = n$ .

b) Eine Menge  $X$ , die nicht endlich ist, heißt unendlich ( $|X| = \infty$ ,  $\sharp X = \infty$  oder  $\text{card } M = \infty$ ).

In der Literatur sind verschiedene Definitionen von endlich und unendlich gebräuchlich. Wir wollen im Folgenden zeigen, dass die wichtigsten dieser Definitionen zu unseren äquivalent sind.

**Folgerung 2.36.** a) *Die Anfangsstücke  $A_n$  sind für jedes  $n \in \mathbb{N}_0$  endlich mit  $\sharp A_n = n$ . Insbesondere ist die leere Menge  $\emptyset = A_0$  endlich mit  $\sharp \emptyset = 0$ .*

b) *Ist  $M$  eine endliche Menge mit  $\sharp M = n$  und ist  $x \notin M$ , dann ist  $M \cup \{x\}$  ebenfalls endlich mit  $\sharp(M \cup \{x\}) = n + 1$ .*

*Beweis.* Teil a) ist unmittelbar klar. In Teil b) existiert nach Voraussetzung eine bijektive Abbildung  $\varphi: M \rightarrow A_n$ . Setzt man jetzt  $M^* := M \cup \{x\}$  und definiert

$$\varphi^*: M^* \rightarrow A_{n+1}, \quad \varphi^*(k) := \begin{cases} \varphi(k), & k \in M \\ n, & k = x, \end{cases}$$

dann ist  $\varphi^*$  bijektiv und damit ist die Aussage ist bewiesen.  $\square$

**Lemma 2.37.** a) *Ist  $M$  endlich, dann ist jede injektive Abbildung  $\psi: M \rightarrow M$  auch surjektiv.*

b) *Existiert zu einer Menge  $X$  eine Abbildung  $\psi: X \rightarrow X$ , die injektiv aber nicht surjektiv ist, dann ist  $X$  unendlich.*

*Beweis.* a) Da  $M$  endlich ist, gibt es ein  $n \in \mathbb{N}_0$  und eine bijektive Abbildung  $\varphi: M \rightarrow A_n$ . Ist nun  $\psi: M \rightarrow M$  eine beliebige injektive Abbildung, dann ist  $\varphi \circ \psi \circ \varphi^{-1}: A_n \rightarrow A_n$  injektiv und nach Lemma 2.31 auch surjektiv. Folglich ist auch  $\psi = \varphi^{-1} \circ (\varphi \circ \psi \circ \varphi^{-1}) \circ \varphi$  surjektiv.

b) Diese Aussage ist logisch äquivalent zu der von Teil a. Beachte  $A \implies B$  ist genau dann wahr, wenn  $\neg B \implies \neg A$  wahr ist.  $\square$

Wir werden jetzt die unendlichen Mengen etwas genauer untersuchen. Aus Lemma 2.37b folgt unmittelbar, dass  $\mathbb{N}_0$  eine unendliche Menge ist, denn die Nachfolgerfunktion  $S^+$  ist eine injektive, aber nicht surjektive Funktion von  $\mathbb{N}_0$  in sich. Das folgende Lemma ist das Kernstück des gesamten Abschnitts. Es sagt aus, dass  $\mathbb{N}_0$  in einem gewissen Sinn die „kleinste“ unendliche Menge ist.

**Lemma 2.38.** *Ist  $X$  eine unendliche Menge, dann gilt  $\mathbb{N}_0 \preceq X$ .*

*Beweis.* Wir müssen eine injektive Abbildung von  $\mathbb{N}_0$  nach  $X$ , also eine injektive Folge  $(x_n)_{n \in \mathbb{N}_0}$  in  $X$  finden.

*Beweisidee.* Wähle  $x_0 \in X$  beliebig. Sind nun  $x_0, x_1, \dots, x_{n-1}$  schon paarweise verschieden gewählt, dann setze  $U_n := \{x_0, x_1, \dots, x_{n-1}\}$  und wähle  $x_n \in X \setminus U_n$  beliebig. Dieses Verfahren kann man unendlich oft durchführen, da  $X$  eine unendliche Menge ist und deshalb die „Restmenge“  $X \setminus U_n \neq \emptyset$  ist. Die so erhaltene Folge  $(x_n)_{n \in \mathbb{N}_0}$  ist die gesuchte injektive Abbildung von  $\mathbb{N}_0 \in X$ .

Diese Beweisidee muss in zweierlei Hinsicht noch präzisiert werden. Zum einen wird hier die intuitive Vorstellung einer unendlichen Menge benutzt, dass nach dem Wegnehmen endlich vieler Elemente in der Restmenge immer noch Elemente übrig bleiben. Zum anderen ist die Vorschrift „ $n \mapsto$  beliebiges Element aus  $X \setminus U_n$ “ keine exakte Definition einer Abbildung.

*Exakter Beweis.* Sei

$$\mathfrak{C} := \{E \subset X; E \text{ endlich}\}.$$

Speziell gilt  $\emptyset \in \mathfrak{C}$  und  $X \notin \mathfrak{C}$ . Wegen  $X \setminus E = \emptyset \iff X = E$  ist deshalb  $X \setminus E \neq \emptyset$  für alle  $E \in \mathfrak{C}$ . (Dieses Argument ist rein mengentheoretisch und benutzt nicht die intuitive Vorstellung von endlich und unendlich.)

Sei jetzt  $\psi: \mathfrak{P}(X) \setminus \{\emptyset\} \rightarrow X$  eine Auswahlfunktion für  $X$ , d. h. es gilt  $\psi(M) \in M$  für alle  $M \subset X$ ,  $M \neq \emptyset$  (vgl. Abschnitt 1.4, „Äquivalente Formulierungen des Auswahlaxioms d“) und Bemerkung 1.49). Wir definieren eine Funktion

$$g: \mathfrak{C} \rightarrow \mathfrak{C}, \quad E \mapsto E \cup \{\psi(X \setminus E)\},$$

die jeder Menge  $E \in \mathfrak{C}$  ein noch nicht zu  $E$  gehörendes Element hinzufügt. Man beachte, dass  $E \cup \{\psi(X \setminus E)\}$  nach Folgerung 2.36b wieder eine endliche Teilmenge von  $X$ , also ein Element von  $\mathfrak{C}$  ist. Als nächstes konstruieren wir mit Hilfe des Rekursionstheorems eine Folge  $(U_n)_{n \in \mathbb{N}_0}$  in  $\mathfrak{C}$  durch

$$(2.13) \quad U_0 := \emptyset, \quad U_{n+1} := g(U_n) = U_n \cup \{\psi(X \setminus U_n)\} \quad (n \in \mathbb{N}_0).$$

Die Folge  $(U_n)_{n \in \mathbb{N}_0}$  ist monoton wachsend, d. h.

$$(2.14) \quad m \leq n \implies U_m \subset U_n \quad (m, n \in \mathbb{N}_0).$$

Die gesuchte Folge  $(x_n)_{n \in \mathbb{N}_0}$  in  $X$  ist nun gegeben durch

$$(2.15) \quad x_n := \psi(X \setminus U_n) \quad (n \in \mathbb{N}_0).$$

Vergleicht man (2.13) mit (2.15), dann sieht man, dass  $x_n$  genau das Element von  $X$  ist, das beim Übergang von  $U_n$  zu  $U_{n+1}$  hinzugefügt wird. Wir müssen noch zeigen, dass die Folge  $(x_n)_{n \in \mathbb{N}_0}$  injektiv ist. Seien dazu  $m, n \in \mathbb{N}_0$  mit  $m \neq n$ , o. B. d. A.  $m < n$ , also  $m + 1 \leq n$ . Nun ist einmal  $x_n = \psi(X \setminus U_n) \in X \setminus U_n$ , also  $x_n \notin U_n$ . Andererseits gilt nach Definition der Folge  $(U_n)_{n \in \mathbb{N}_0}$  und (2.14)

$$x_m = \psi(X \setminus U_m) \in U_m \cup \{\psi(X \setminus U_m)\} = U_{m+1} \subset U_n.$$

Damit muss  $x_m \neq x_n$  sein, d. h.  $(x_n)_{n \in \mathbb{N}_0}$  ist eine injektive Folge. □

Die angestrebten äquivalenten Charakterisierungen von unendlich ist im folgenden Satz enthalten.

**Satz 2.39.** *Für eine Menge  $X$  sind äquivalent:*

- (i)  $X$  ist unendlich, d. h. es gilt  $X \not\sim A_n$  für alle  $n \in \mathbb{N}_0$ .
- (ii)  $\mathbb{N}_0 \preceq X$ .
- (iii) Es existiert eine surjektive Abbildung  $\chi: X \rightarrow \mathbb{N}_0$ .
- (iv) Es existiert eine injektive Abbildung  $\varphi: X \rightarrow X$ , die nicht surjektiv ist.

*Beweis.* (ii)  $\iff$  (iii) ist die Aussage von Lemma 1.71. Die übrigen Äquivalenzen beweisen wir durch einen Ringschluss. (i)  $\implies$  (ii) gilt nach Lemma 2.38. Ist nun (ii) erfüllt, dann existieren eine Menge  $X_0 \subset X$  und eine bijektive Abbildung  $\psi: \mathbb{N}_0 \rightarrow X_0$ . Mit der Nachfolgerfunktion  $S^+: \mathbb{N}_0 \rightarrow \mathbb{N}_0$  definieren wir nun eine Abbildung

$$\psi^* := \psi \circ S^+ \circ \psi^{-1}: X_0 \rightarrow X_0,$$

die als Zusammensetzung injektiver Abbildungen ebenfalls injektiv ist.  $\psi^*$  ist aber nicht surjektiv, denn natürlich ist  $\psi(0) \in X_0$ , aber wegen der Injektivität von  $\psi$  und (P3) ist  $\psi(0) \notin \psi^*(X_0)$ . Wir setzen jetzt noch  $\psi^*$  zu einer Abbildung  $\varphi$  von  $X$  in sich fort durch

$$\varphi: X \rightarrow X, \quad \varphi(x) := \begin{cases} \psi^*(x), & x \in X_0 \\ x, & x \in X \setminus X_0. \end{cases}$$

Man sieht leicht, dass  $\varphi$  ebenfalls injektiv, aber nicht surjektiv ist, womit auch die Implikation (ii)  $\implies$  (iv) bewiesen ist. Der letzte Schritt (iv)  $\implies$  (i) folgt schließlich noch aus Lemma 2.37.  $\square$

Durch logische Negation erhält man hieraus entsprechende Charakterisierungen endlicher Mengen.

**Satz 2.40.** *Für eine Menge  $M$  sind äquivalent:*

- (i)  $M$  ist endlich, d. h. es existiert ein  $n \in \mathbb{N}_0$  mit  $M \sim A_n$ .
- (ii) Es existiert keine injektive Abbildung  $\varphi: \mathbb{N}_0 \rightarrow M$ .
- (iii) Es existiert keine surjektive Abbildung  $\chi: M \rightarrow \mathbb{N}_0$ .
- (iv) Jede injektive Abbildung  $\psi: M \rightarrow M$  ist auch surjektiv.

Jede der vier Aussagen von Satz 2.39 kann man als Definition von unendlich benutzen und ebenso kann man die Aussagen von Satz 2.40 als Definition von endlich benutzen. Der Beweis, dass diese Aussagen äquivalent sind, hängt ganz entscheidend vom Auswahlaxiom ab, das wir im Beweis von Lemma 2.38 benutzt haben. Man kann in der Tat zeigen, dass ohne das Auswahlaxiom diese Aussagen nicht mehr äquivalent sind.

Die folgenden Eigenschaften, die der anschaulichen Vorstellung endlicher bzw. unendlicher Mengen entsprechen, lassen sich jetzt sehr leicht beweisen.

**Folgerung 2.41.** a) Sei  $X$  eine unendliche Menge,  $Y$  eine beliebige Menge.

- (i) Ist  $Y \supset X$ , dann ist  $Y$  unendlich.
- (ii) Existiert eine injektive Abbildung  $\varphi: X \rightarrow Y$ , dann ist  $Y$  unendlich.
- (iii) Existiert eine surjektive Abbildung  $\psi: Y \rightarrow X$ , dann ist  $Y$  unendlich.

b) Ist  $M$  eine endliche Menge und  $N \subset M$ , dann ist auch  $N$  endlich mit  $\#N \leq \#M$ .

c) Sind  $M, N$  endliche Mengen, dann ist auch  $M \cup N$  endlich und es gilt  $\#(M \cup N) = \#M + \#N - \#(M \cap N)$ .

d) Ist  $M$  endlich,  $N$  beliebig, dann ist  $M \setminus N$  endlich und  $\#(M \setminus N) = \#M - \#(M \cap N)$ .

*Beweis.* a) (i) Da  $X$  unendlich ist, existiert eine injektive Abbildung  $\chi: \mathbb{N}_0 \rightarrow X$ . Definiert man  $\psi: \mathbb{N}_0 \rightarrow Y$  durch  $\psi(n) := \chi(n)$ ,  $n \in \mathbb{N}_0$ , dann ist  $\psi$  ebenfalls injektiv und  $Y$  ist unendlich.

a) (ii) Mit der Funktion  $\chi$  aus dem Beweis von (i) setze  $\chi_1 := \varphi \circ \chi$ . Dann ist  $\chi_1: \mathbb{N}_0 \rightarrow Y$  injektiv und  $Y$  ist unendlich.

a) (iii) Setze  $\chi_1 := \chi \circ \psi$ , wobei  $\chi: X \rightarrow \mathbb{N}_0$  die surjektive Funktion aus Satz 2.39 (iii) ist, dann ist  $\chi_1: Y \rightarrow \mathbb{N}_0$  surjektiv und  $Y$  ist nach Satz 2.39 unendlich.

b) Wäre  $N$  unendlich, dann müsste nach Teil a auch  $M$  unendlich sein. Ist nun  $\#M = m$  und  $\#N = n$ , dann existieren bijektive Abbildungen  $\chi_1: M \rightarrow A_m$  und  $\chi_2: N \rightarrow A_n$ . Mit der Inklusionsabbildung  $\text{Id}_N: N \rightarrow M$  erhält man mittels  $\chi_1 \circ \text{Id}_N \circ \chi_2^{-1}$  eine injektive Abbildung von  $A_n$  nach  $A_m$ , d. h.  $A_n \preceq A_m$ , und mit Satz 2.33(i) folgt  $n \leq m$ .

Rest Übung. □

In Lemma 2.38 oder Satz 2.39 haben wir gesehen, dass jede unendliche Menge mindestens so mächtig wie  $\mathbb{N}_0$  ist. Wir wollen jetzt noch die Mengen untersuchen, die genau so mächtig oder weniger mächtig wie  $\mathbb{N}_0$  sind.

**Definition 2.42.** Eine Menge  $A$  mit  $A \preceq \mathbb{N}_0$  heißt abzählbar.

**Folgerung 2.43.** Jede endliche Menge ist abzählbar.

*Beweis.* Ist  $A$  endlich, dann existiert ein eindeutiges  $n \in \mathbb{N}_0$  und eine bijektive Abbildung  $\varphi: A \rightarrow A_n$ . Damit ist aber  $\varphi$  eine bijektive Abbildung von  $A$  auf eine Teilmenge von  $\mathbb{N}_0$ , d. h.  $A \preceq \mathbb{N}_0$ . □

Abzählbare Mengen können endlich oder unendlich sein. Eine abzählbare Menge, die unendlich ist, nennt man auch abzählbar unendlich.

**Folgerung 2.44.** Eine Menge  $A$  ist genau dann abzählbar unendlich, wenn  $A \sim \mathbb{N}_0$ .

*Beweis.* Ist  $A$  abzählbar unendlich, dann gilt  $A \preceq \mathbb{N}_0$ , weil  $A$  abzählbar ist, und es gilt  $A \succeq \mathbb{N}_0$ , weil  $A$  unendlich ist (Satz 2.39). Nach dem Satz von Schröder-Bernstein (Satz 1.73) ist deshalb  $A \sim \mathbb{N}_0$ . Umgekehrt folgt aus  $A \sim \mathbb{N}_0$  sowohl  $A \preceq \mathbb{N}_0$ , d. h.  $A$  ist abzählbar, als auch  $A \succeq \mathbb{N}_0$ , d. h.  $A$  ist unendlich. □

**Folgerung 2.45.** Die Menge  $\mathbb{N}_0$  ist abzählbar unendlich.

**Satz 2.46.** a) Die Vereinigung zweier abzählbarer Mengen ist abzählbar.

b)  $\mathbb{N}_0 \times \mathbb{N}_0$  ist abzählbar, und allgemeiner ist das kartesische Produkt zweier abzählbarer Mengen abzählbar.

c) Ist  $(M_n)_{n \in \mathbb{N}_0}$  eine Folge abzählbarer Mengen, dann ist  $\bigcup_{n=0}^{\infty} M_n$  abzählbar.

Man sollte aber nicht auf die Idee kommen, dass alle Mengen abzählbar sind, z. B. gilt nach dem Satz von Cantor (Satz 1.75)

**Lemma 2.47.**  $\mathfrak{P}(\mathbb{N}_0)$  ist überabzählbar, d. h.  $\mathbb{N}_0 \prec \mathfrak{P}(\mathbb{N}_0)$ .

