KAPITEL II

Natürliche Zahlen

1. Die natürlichen Zahlen und die vollständige Induktion

Wie am Anfang der Mengenlehre eine axiomatische Einführung stand, so sollen jetzt die natürlichen Zahlen axiomatisch eingeführt werden. Dabei steht der Prozeß des gewöhnlichen Zählens zunächst im Vordergrund. Die heute übliche Begründung der natürlichen Zahlen basiert auf Axiomen, die von Peano 1889 veröffentlicht wurden, die aber auch Dedekind 1888 schon bekannt waren.

Wir werden einige einfache Eigenschaften der natürlichen Zahlen in der folgenden Definition festlegen. Dabei werden wir nebeneinander eine mathematisch präzise Formulierung, die wir in der Sprache der Mengenlehre geben können, und die umgangssprachliche Formulierung der gewünschten Eigenschaften für natürliche Zahlen angeben. Diese Eigenschaften nennt man auch die Peano-Axiome.

Die Existenz einzelner natürlicher Zahlen (z.B. zwei oder drei) ist in den logischen Grundlagen, die wir hier verwenden, enthalten, weil man einzelne Objekte nebeneinander stellen kann und sie damit abzählen kann. Die Existenz der *Menge aller natürlichen Zahlen* ist dadurch jedoch nicht gegeben. Das ist nämlich eine Menge mit unendlich vielen Elementen. Wir wissen bisher nicht einmal, ob es überhaupt irgendeine Menge mit unendlich vielen Elementen gibt. Daher müssen wir die Existenz der Menge aller natürlichen Zahlen zusätzlich durch ein mengentheoretisches Axiom fordern.

Das Rechnen mit natürlichen Zahlen ist ein wesentlich komplexerer Vorgang. Bevor wir überhaupt die Addition von natürlichen Zahlen einführen können, was erst im Abschnitt 3 geschehen wird, müssen wir starke Hilfsmittel über Rekursion und Induktion bereitstellen.

Definition 1.1. Ein Tripel $(\mathbb{N}, 1, \mu)$ bestehend aus einer Menge $\mathbb{N}$, einem Element $1 \in \mathbb{N}$ und einer Abbildung $\mu : \mathbb{N} \longrightarrow \mathbb{N}$, genannt *Nachfolgerfunktion*, heißt (eine) *Menge der natürlichen Zahlen*, wenn die folgenden Axiome erfüllt sind:

(P1) $1 \in \mathbb{N}$, („1 ist eine natürliche Zahl"),

(P2) $\mu : \mathbb{N} \longrightarrow \mathbb{N}$ ist eine Abbildung, („jede natürliche Zahl besitzt einen eindeutig bestimmten Nachfolger"),

(P3) $\forall n \in \mathbb{N}[\mu(n) \neq 1]$, („1 ist kein Nachfolger einer natürlichen Zahl"),

(P4) μ ist injektiv, („natürliche Zahlen mit gleichen Nachfolgern sind gleich"),

(P5) (Prinzip der vollständigen Induktion)

$$\forall E \subset \mathbb{N}[(1 \in E \wedge \forall n \in E[\mu(n) \in E]) \Longrightarrow E = \mathbb{N}],$$

(„eine Eigenschaft, die der 1 zukommt und mit einer beliebigen natürlichen Zahl auch ihrem Nachfolger, kommt allen natürlichen Zahlen zu").

Wir schreiben mit der Nachfolgerfunktion μ und $n \in \mathbb{N}$ häufig $n + 1 := \mu(n)$.

Axiom 6. (Existenz der Menge der natürlichen Zahlen)
Es existiert eine Menge der natürlichen Zahlen $(\mathbb{N}, 1, \mu)$.

Wie wichtig die Forderung nach der Existenz einer Menge der natürlichen Zahlen ist, ersieht man aus dem folgenden Satz. Nur wenn es eine Menge der natürlichen Zahlen gibt, kann es überhaupt auch andere unendliche Mengen geben. Die Menge der natürlichen Zahlen kann man als den kleinsten Prototyp einer unendlichen Menge auffassen. Weiter kann man in jeder unendlichen Menge ein Modell für eine Menge von natürlichen Zahlen finden. Wir erinnern noch einmal an unsere Definition einer unendlichen Menge M (Kap.I. 2.29 und Kap.I.2.31). Es muß zu ihr eine (Selbst-)Abbildung $\lambda : M \longrightarrow M$ geben, die injektiv aber nicht surjektiv ist.

Zum Beweis des folgenden Satzes benötigen wir zunächst ein Lemma.

Lemma 1.2. *Seien M eine Menge, $\lambda : M \longrightarrow M$ eine Abbildung und $m \in M$ ein Element. Dann gibt es in M eine kleinste Teilmenge N mit $\lambda(N) \subset N$ und $m \in N$.*

Beweis. Wir betrachten die Menge $\mathfrak{M}$ aller Teilmengen $A \subset M$, für die gilt $\lambda(A) \subset A$ und $m \in A$. Diese Menge enthält sicherlich M als Element. Nun bilden wir den Durchschnitt über alle so gefundenen Teilmengen

$$N := \bigcap\{A \subset M | \lambda(A) \subset A, m \in A\}.$$

Offenbar ist dann $m \in N$. Für $n \in N$ ist n in allen genannten Teilmengen A enthalten, also auch $\lambda(n)$. Damit ist auch $\lambda(n) \in N$. N ist daher die kleinste Teilmenge von M mit $m \in N$ und $\lambda(N) \subset N$.
Insbesondere ist diese kleinste Teilmenge N in M mit $\lambda(N) \subset N$ und $m \in N$ eindeutig bestimmt. $\square$

Man kann sich diese kleinste Teilmenge N in M vorstellen als die Menge der Elemente, die man aus m durch beliebig häufige Anwendung von λ erhält, also die Menge $\{m, \lambda(m), \lambda(\lambda(m)), \dots\}$. Leider ist es recht schwierig, diese Menge formal richtig anzugeben, dashalb haben wir den unanschaulichen, aber mathematisch bequemen Weg der Durchschnittsbildung eingeschlagen. Wir werden diese Mothode bei den algebraischen Strukturen in Kapitel 4 häufig verwenden.

Satz 1.3. *Die folgenden Aussagen sind äquivalent:*

(1) *Es existiert eine Menge der natürlichen Zahlen.*
(2) *Es existiert eine unendliche Menge.*

Beweis. Wenn es eine Menge der natürlichen Zahlen $(\mathbb{N}, 1, \mu)$ gibt, so ist μ nach (P4) injektiv und nach (P3) nicht surjektiv. Also ist $\mathbb{N}$ eine unendliche Menge.
Sei umgekehrt M eine unendliche Menge und λ eine injektive und nicht surjektive Abbildung von M in M. Dann gibt es ein Element $m \in M$, das nicht im Bild von λ liegt. Wir betrachten jetzt die kleinste Teilmenge $N \subset M$ mit $\lambda(N) \subset N$ und $m \in N$. Sei $\nu : N \longrightarrow N$ die Einschränkung von λ auf die Teilmenge N. Wir zeigen, daß für (N, m, ν) die Peano-Axiome erfüllt sind. Offenbar ist ν als Einschränkung von λ wieder injektiv, und es gilt $\forall n \in N[\nu(n) \neq m]$, da m nicht im Bild von λ liegt. Es bleibt nur die Gültigkeit des Prinzips der vollständigen Induktion für (N, m, ν) zu zeigen. Ist $E \subset N$ mit $m \in E$ und $\forall n \in E[\nu(n) \in E]$, dann gilt für E auch die Bedingung $\nu(E) \subset E$ bzw. $\lambda(E) \subset E$. Weil N die kleinste solche Menge ist und $E \subset N$ gilt, folgt $E = N$. Damit ist die Gültigkeit des Prinzips der vollständigen Induktion (P5) bewiesen. $\square$

Die Konstruktion einer Menge der natürlichen Zahlen in einer beliebigen unendlichen Menge kann zu recht überraschenden Beispielen führen. Die Abbildung $f : \mathbb{R}^+ \ni x \mapsto x^2 + 1 \in \mathbb{R}^+$ von den positiven rellen Zahlen in sich ist bekanntlich injektiv und es gilt $1 \notin f(\mathbb{R}^+)$. Eine Menge der natürlichen Zahlen in $\mathbb{R}^+$ ist dann $N = \{1, 2, 5, 26, \dots\}$.

Aus den vielen wichtigen Eigenschaften, die eine Menge von natürlichen Zahlen besitzt, ist das Zahlenrechnen in $\mathbb{N}$ hervorzuheben. Bevor wir aber die einfachsten Rechenoperationen einführen können, müssen wir eines der wichtigsten Beweisprinzipien studieren, den Beweis durch vollständige Induktion. Es gibt dazu viele Varianten. Wir wollen lediglich zwei davon angeben. Sie alle bauen auf dem Peano-Axion (P5) auf. Weiter benötigen wir ein vor allem in der Informatik und mathematischen Logik wichtiges Hilfsmittel, die Definition von Abbildungen durch primitive Rekursion, bevor wir die einfachsten Rechenoperationen in der Menge der natürlichen Zahlen einführen können. Dieses Hilfmittel werden wir im nächsten Paragraphen beprechen.

Satz 1.4. *(über den Beweis durch vollständige Induktion):*
Für jede natürliche Zahl $n \in \mathbb{N}$ sei eine Aussage $\mathfrak{A}(n)$ formuliert. Dafür gelte

Induktionsanfang:	$\mathfrak{A}(1)$ *ist richtig (wahr) und*
Induktionsannahme:	*aus der Richtigkeit von* $\mathfrak{A}(n)$
Induktionsschluß:	*folgt die Richtigkeit von* $\mathfrak{A}(n+1)$.

Dann ist $\mathfrak{A}(n)$ für alle $n \in \mathbb{N}$ richtig.
(Formal: $(\mathfrak{A}(1) \wedge \forall n \in \mathbb{N}[\mathfrak{A}(n) \Longrightarrow \mathfrak{A}(n+1)]) \Longrightarrow \forall n \in \mathbb{N}[\mathfrak{A}(n)])$

Beweis. Sei $E := \{n \in \mathbb{N} | \mathfrak{A}(n)\}$. Es gilt $1 \in E$ und $\forall n \in E[n+1 \in E]$ wegen der Induktionsvoraussetzungen. Nach (P5) ist $E = \mathbb{N}$, also $\forall n \in \mathbb{N}[\mathfrak{A}(n)]$. $\square$

Varianten dieses Satzes sind vor allem Induktionsaussagen, die erst von einer vorgegebenen Zahl $n_0 \in \mathbb{N}$ an gelten:

$$\mathfrak{A}(n_0) \wedge \forall n \in \mathbb{N}[n \geq n_0 \wedge \mathfrak{A}(n) \Longrightarrow \mathfrak{A}(n+1)])$$
$$\Longrightarrow \forall n \in \mathbb{N}[n \geq n_0 \Longrightarrow \mathfrak{A}(n)].$$

Diese Aussage werden wir an dieser Stelle nicht beweisen, zumal wir die Ordnung $m \leq n$ auf den natürlichen Zahlen noch gar nicht kennen. Die Aussage ergibt sich später aber ganz leicht aus dem Beispiel einer Menge von natürlichen Zahlen, die eine Teilmenge T von $\mathbb{N}$ ist mit derselben Nachfolgerabbildung, dem Anfangselement n_0, und deren Elemente gerade diejenigen $n \in \mathbb{N}$ sind, für die $n_0 \leq n$ gilt, also $(\{n \in \mathbb{N} | n_0 \leq n\}, n_0, \mu)$. (vgl. Beispiel 3.8 (2)).

Für den nächsten Satz setzen wir voraus, daß die Ordnung von $\mathbb{N}$ schon bekannt ist. Diese Ordnung wird zwar erst in 3.3 eingeführt werden. Der Satz gehört jedoch systematisch in diesen Abschnitt über vollständige Induktion. Er wird zur Herleitung des Ordnungsbegriffes in $\mathbb{N}$ auch nicht verwendet.

Satz 1.5. *(über die starke vollständige Induktion)*
Für jede natürliche Zahl $n \in \mathbb{N}$ sei eine Aussage $\mathfrak{A}(n)$ formuliert. Dafür gelte

Induktionsanfang:	$\mathfrak{A}(1)$,
Induktionsannahme:	*aus* $\forall i \leq n[\mathfrak{A}(i)]$, *d.h. aus* $\mathfrak{A}(1), \ldots, \mathfrak{A}(i), \ldots, \mathfrak{A}(n)$,
Induktionsschluß:	*folgt* $\mathfrak{A}(n+1)$.

Dann gilt $\mathfrak{A}(n)$ für alle $n \in \mathbb{N}$.

Beweis. Wir definieren $\mathfrak{B}(n) :\Longleftrightarrow \forall i \in \mathbb{N}[i \leq n \Longrightarrow \mathfrak{A}(i)]$. Dann gelten $\mathfrak{B}(1)$ und $\forall n \in \mathbb{N}[\mathfrak{B}(n) \Longrightarrow \mathfrak{B}(n+1)]$. Also ist $\forall n \in \mathbb{N}[\mathfrak{B}(n)]$ und damit auch $\forall n \in \mathbb{N}[\mathfrak{A}(n)]$. $\square$

2. Primitive Rekursion

Wir wollen eine Abbildung $\varphi : X \longrightarrow X$ iterieren, also $\varphi^2 := \varphi\varphi$, $\varphi^{n+1} := \varphi\varphi^n$ bilden. Diese zunächst ganz einfach erscheinende Bildung bringt eine grundlegende Schwierigkeit mit sich. Wir wissen nicht, ob φ^n für *alle* $n \in \mathbb{N}$ mit den gewünschten Eigenschaften definiert ist. Dabei hilft zunächst auch noch nicht das Prinzip der vollständigen Induktion. Deswegen beschränken wir uns zunächst darauf, für ein Element $c \in X$ die Elemente $\varphi^n(c) \in X$ zu definieren, genau eine Abbildung

$$\alpha : \mathbb{N} \ni n \mapsto \varphi^n(c) \in X$$

zu definieren. Das geschieht in dem folgenden Satz.

Satz 2.1. *(über die einfache Rekursion): Sei X eine Menge, $c \in X$ ein Element und $\varphi : X \longrightarrow X$ eine Abbildung. Dann gibt es genau eine Abbildung $\alpha : \mathbb{N} \longrightarrow X$ mit*

(1) $\alpha(1) = c$,
(2) $\forall n \in \mathbb{N}[\alpha(n+1) = \varphi(\alpha(n))]$,

d.h. so daß das Diagramm

$$\begin{tikzcd}
 & \mathbb{N} \arrow[r, "\mu"] \arrow[dd, "\alpha"] & \mathbb{N} \arrow[dd, "\alpha"] \\
\{1\} \arrow[ur, "\iota"] \arrow[dr, "\gamma"'] & & \\
 & X \arrow[r, "\varphi"'] & X
\end{tikzcd}$$

kommutiert, wobei $\gamma(1) = c$, $\iota(1) = 1$.

Beweis. Quelle und Ziel für die gesuchte Abbildung α stehen fest. Wir suchen den Graphen von α. Dazu betrachten wir die Abbildung $(\mu \times \varphi) : \mathbb{N} \times X \ni (n, x) \mapsto (\mu(n), \varphi(x)) \in \mathbb{N} \times X$ und das Element $(1, c) \in \mathbb{N} \times X$. Nach Lemma 1.2 sei G die kleinste Teilmenge von $\mathbb{N} \times X$ mit $(\mu \times \varphi)(G) \subset G$ und $(1, c) \in G$.
1) Es ist $(m, y) \in G \Longleftrightarrow ((m, y) = (1, c) \vee \exists (n, x) \in G[(m, y) = (n+1, \varphi(x))]$. Hierbei gilt „$\Longleftarrow$“ wegen der Definition von G. Die Richtung „$\Longrightarrow$“ erhält man aus der folgenden Argumentation: Angenommen, die Folgerung gilt nicht. Dann gibt es ein $(m, y) \in G$ mit $(m, y) \neq (1, c)$ und $\forall (n, x) \in G[(m, y) \neq (n+1, \varphi(x))]$. Dann gilt $(\mu \times \varphi)(G \setminus \{(m, y)\}) \subset G \setminus \{(m, y)\}$ und $(1, c) \in G \setminus \{(m, y)\}$. Das kann aber nicht sein, weil G die kleinste Menge mit diesen Eigenschaften ist.
2) G ist Graph einer Abbildung von $\mathbb{N}$ nach X. Wir zeigen durch vollständige Induktion $\forall n \in \mathbb{N} \exists x \in X[(n, x) \in G]$. Sei also $\mathfrak{A}(n)$ die Induktionsaussage $\exists x \in X[(n, x) \in G]$.
Induktionsanfang: $\mathfrak{A}(1)$ gilt wegen $(1, c) \in G$.

Induktionsannahme: Gelte $\mathfrak{A}(n)$, d.h. $\exists x \in X[(n,x) \in G]$.
Induktionsschluß: Wegen $(n+1, \varphi(x)) \in G$ gilt $\mathfrak{A}(n+1)$.
Damit folgt die Behauptung.
Weiter zeigen wir durch vollständige Induktion: $\forall n \in \mathbb{N}\ \forall x, y \in X[(n,x) \in G \wedge (n,y) \in G \Longrightarrow x = y]$. Sei $\mathfrak{A}(n)$ die Induktionsaussage $\forall x, y \in X[(n,x) \in G \wedge (n,y) \in G \Longrightarrow x = y]$.
Induktionsanfang: Sei $(1,x) \in G$ und $(1,c) \in G$. Angenommen $x \neq c$. Wegen 1) gibt es $(n,z) \in G[(1,x) = (n+1, \varphi(z))]$, also $1 = n+1$ im Widerspruch zu (P3). Also ist $x = c$. Daraus folgt $\mathfrak{A}(1)$.
Induktionsannahme: Gelte $\mathfrak{A}(n)$, d.h. $\forall x, y \in X[(n,x) \in G \wedge (n,y) \in G \Longrightarrow x = y]$.
Induktionsschluß: Seien $x, y \in X$ gegeben mit $(n+1, x) \in G$ und $(n+1, y) \in G$. Da n durch $n+1$ eindeutig festgelegt ist (μ ist injektiv), gibt es (nach 1)) $u, v \in G$ mit $(n,u) \in G, (n,v) \in G$ und $\varphi(u) = x$ und $\varphi(v) = y$, wegen $(n+1, \varphi(u)) = (n+1, x)$ und $(n+1, \varphi(v)) = (n+1, y)$. Nach Induktionsannahme ist $u = v$, also $x = \varphi(u) = \varphi(v) = y$.
Also ist $\alpha := (\mathbb{N}, X, G)$ eine Abbildung.
3) α erfüllt die Bedingungen $\alpha(1) = c$ und $\forall n \in \mathbb{N}[\alpha(n+1) = \varphi(\alpha(n))]$, denn $(n,x) \in G$ und $(n+1, \varphi(x)) \in G$ implizieren $\alpha(n) = x$ und $\alpha(n+1) = \varphi(x) = \varphi\alpha(n)$.
4) Es bleibt zu zeigen, daß α eindeutig bestimmt ist. Sei also $\beta : \mathbb{N} \longrightarrow X$ mit $\beta(1) = c$ und $\forall n \in \mathbb{N}[\beta(n+1) = \varphi\beta(n)]$ gegeben. Wir zeigen durch vollständige Induktion $\forall n \in \mathbb{N}[\alpha(n) = \beta(n)]$. Sei $\mathfrak{A}(n)$ die Induktionsaussage $\alpha(n) = \beta(n)$.
Induktionsanfang: Es ist $\alpha(1) = c = \beta(1)$, also gilt $\mathfrak{A}(1)$.
Induktionsannahme: Sei $\alpha(n) = \beta(n)$.
Induktionsschluß: Dann ist $\alpha(n+1) = \varphi(\alpha(n)) = \varphi(\beta(n)) = \beta(n+1)$.
Damit gilt $\alpha = \beta$. $\square$

In diesem Satz ist das Hilfsmittel der vollständigen Induktion gleich mehrfach angewendet worden. Damit haben wir jetzt aber auch die Möglichkeit, die Funktion φ^n für alle $n \in$ zu definieren. Wir schreiben einfach $\varphi^1(c) = c$ und $\varphi^{n+1}(c) = \varphi(\varphi^n(c))$. Für festgewähltes $c \in X$ gibt es damit eine Abbildung $\varphi()(c) : \mathbb{N} \longrightarrow X$ gegeben, wobei $\varphi(n)(c) = \varphi^n(c)$ gelte. Da damit der Wert für jedes $c \in X$ eindeutig festgelegt ist, haben wir auch die Abbildungen $\varphi^n : X \longrightarrow X$ für alle $n \in \mathbb{N}$ definiert. Häufig braucht man zur rekursiven Definition von Abbildungen etwas kompliziertere Bedingungen an die Rekursion. Der einfachste Fall ist der

Satz 2.2. *(über die primitive Rekursion): Sei X eine Menge, $c \in X$ ein Element und $\varphi : \mathbb{N} \times X \longrightarrow X$ eine Abbildung. Dann gibt es genau eine Abbildung $\alpha : \mathbb{N} \longrightarrow X$ mit*

(1) $\alpha(1) = c$,
(2) $\forall n \in \mathbb{N}[\alpha(n+1) = \varphi(n, \alpha(n))]$,

d.h. so daß das Diagramm

$$\begin{tikzcd} & \mathbb{N} \arrow[r, "\mu"] \arrow[d, "(\mathrm{id}\ , \alpha)"] & \mathbb{N} \arrow[d, "\alpha"] \\ \{1\} \arrow[ur, "\iota"] \arrow[dr, "\gamma"'] & & \\ & \mathbb{N} \times X \arrow[r, "\varphi"'] & X \end{tikzcd}$$

kommutiert, wobei $\gamma(1) = (1, c)$, $\iota(1) = 1$ und $(\mathrm{id}\ , \alpha)(n) := (n, \alpha(n))$.

Beweis. Wir wenden 2.1 an auf $\mathbb{N} \times X$, $(1, c) \in \mathbb{N} \times X$ und $\psi : \mathbb{N} \times X \longrightarrow \mathbb{N} \times X$, $\psi(n, x) := (n + 1, \varphi(n, x))$. Dann gibt es genau eine Abbildung $\beta : \mathbb{N} \longrightarrow \mathbb{N} \times X$ mit $\beta(1) = (1, c)$ und $\beta(n + 1) = \psi(\beta(n))$ für alle $n \in N$:

$$\begin{tikzcd} & \mathbb{N} \arrow[r, "\mu"] \arrow[d, "\beta"] & \mathbb{N} \arrow[d, "\beta"] \\ \{1\} \arrow[ur, "\iota"] \arrow[dr, "\gamma"'] & & \\ & \mathbb{N} \times X \arrow[r, "\psi"'] & \mathbb{N} \times X. \end{tikzcd}$$

Durch β werden eindeutig Abbildungen $\rho : \mathbb{N} \longrightarrow \mathbb{N}$ und $\alpha : \mathbb{N} \longrightarrow X$ definiert mit $\beta(n) = (\rho(n), \alpha(n))$. Für diese Abbildungen gilt $\rho(1) = 1$, $\alpha(1) = c$ und $(\rho(n+1), \alpha(n+1)) = \beta(n+1) =$

$\psi(\beta(n)) = \psi(\rho(n), \alpha(n)) = (\rho(n) + 1, \varphi(\rho(n), \alpha(n)))$, also ist $\rho(n+1) = \rho(n) + 1$ und $\alpha(n+1) = \varphi(\rho(n), \alpha(n))$. Da die Abbildung ρ aber $\rho(1) = 1$ und $\rho(n+1) = \rho(n) + 1 = \mu\rho(n)$ erfüllt und ebenso $\mathrm{id}\ (1) = 1$ und $\mathrm{id}\ (n+1) = \mu\,\mathrm{id}\ (n)$ gilt, ist $\rho = \mathrm{id}$ nach 2.1, also ist $\alpha(n+1) = \varphi(n, \alpha(n))$.
Ist $\alpha' : \mathbb{N} \longrightarrow X$ gegeben mit $\alpha'(1) = c$ und $\alpha'(n+1) = \varphi(n, \alpha'(n))$ für alle $n \in \mathbb{N}$, so erfüllt $\beta' : \mathbb{N} \longrightarrow \mathbb{N} \times X$ mit $\beta'(n) := (n, \alpha'(n))$ die Bedingungen $\beta'(1) = (1, \alpha'(1)) = (1, c)$ und $\beta'(n+1) = (n+1, \alpha'(n+1)) = (n+1, \varphi(n, \alpha'(n))) = \psi(n, \alpha'(n)) = \psi(\beta'(n))$, also ist $\beta = \beta'$ und damit $\alpha = \alpha'$. $\square$

Wir kommen jetzt zu den Grundlagen der natürlichen Zahlen zurück. Wir hatten schon gefordert, daß eine Menge der natürlichen Zahlen existieren soll. Es ist aber zunächst nicht klar, ob es hier verschiedene Wahlmöglichkeiten für diese Menge gibt. Wir werden in Beispiel 3.8 tatsächlich verschiedene Mengen angeben, die die Peano- Axiome erfüllen und damit als Mengen der natürlichen Zahlen in Frage kommen. Damit wäre es möglich, daß späteres Rechnen mit natürlichen Zahlen von der Wahl der Menge abhängt, was natürlich recht unsinnig wäre. Deswegen ist der folgende Satz wichtig.

Satz 2.3. *(von der Eindeutigkeit der Menge der natürlichen Zahlen): Seien* $(\mathbb{N}, 1, \mu)$ *und* (A, a, ν) *Mengen der natürlichen Zahlen. Dann gibt es genau eine Abbildung* $\alpha : \mathbb{N} \longrightarrow A$ *mit* $\alpha(1) = a$ *und* $\alpha\mu = \nu\alpha$*, und diese Abbildung ist bijektiv.*

Beweis. : Nach 2.1 folgt Existenz und Eindeutigkeit von $\alpha : \mathbb{N} \longrightarrow A$ mit $\alpha(1) = a$, $\alpha(n+1) = \nu(\alpha(n))$. Ebenso gibt es genau ein $\beta : A \longrightarrow \mathbb{N}$, so daß das Diagramm

$$\begin{tikzcd} & A \arrow[r, "\nu"] \arrow[d, "\beta"] & A \arrow[d, "\beta"] \\ \{a\} \arrow[ur] \arrow[dr] & & \\ & \mathbb{N} \arrow[r, "\mu"'] & \mathbb{N}. \end{tikzcd}$$

kommutiert. Insgesamt haben wir $\beta\alpha(1) = \beta(a) = 1 = \mathrm{id}\ (1)$ und $\forall n \in \mathbb{N}[\beta\alpha(n+1) = \beta\nu\alpha(n) = \mu\beta\alpha(n)]$ und $\forall n \in \mathbb{N}[\mathrm{id}\ (n+1) = \mu\,\mathrm{id}\ (n)]$. Wegen der Eindeutigkeit in 2.1 folgt $\beta\alpha = \mathrm{id}$. Analog sieht man $\alpha\beta = \mathrm{id}_A$. $\square$

Bemerkung 2.4. Wir bemerken, daß α die gesamte bisher bekannte „Struktur" von $\mathbb{N}$ erhält wegen $\alpha(1) = a$ und $\alpha\mu = \nu\alpha$ (es ist gleichgültig, ob man erst den Nachfolger in $\mathbb{N}$ bildet und dann nach A geht, oder gleich nach A geht und dann dort den Nachfolger bildet). Man kennt den „Nachfolger" in A wegen $\nu = \alpha\mu\alpha^{-1}$. Ebenso kennt man die „Eins" in $A : \alpha(1) = a$. Wir wählen daher eine Menge der natürlichen Zahlen $(\mathbb{N}, 1, \mu)$ fest aus und bezeichnen sie fortan als *die Menge der natürlichen Zahlen.* Nach der vorhergehenden Bemerkung ist das keine Einschränkung. In jeder anderen Menge der natürlichen Zahlen könnte die Theorie genauso aufgebaut werden und ergäbe über die bijektive Abbildung α dieselben Resultate (dieselben Primzahlen, dieselbe Primzahlzerlegung etc.).

3. Die Strukturen auf den natürlichen Zahlen

Wir wollen in diesem Abschnitt die üblichen Regeln des Rechnens mit den natürlichen Zahlen entwickeln. Dabei werden wir uns auf die einfache Rekursion stützen und mit ihr zunächst Addition und Multiplikation von natürlichen Zahlen definieren. Mit Hilfe der primitiven Rekursion kann man dann auch das Potenzieren von natürlichen Zahlen einführen.

Definition und Lemma 3.1. (1) Sei $m \in \mathbb{N}$. Wir definieren die Abbildung $\alpha_m : \mathbb{N} \longrightarrow \mathbb{N}$ durch die Bedingungen

$$\alpha_m(1) = m + 1,$$
$$\forall n \in \mathbb{N}[\alpha_m(n+1) = \alpha_m(n) + 1]$$

(bezüglich $m + 1 = \mu(m) \in \mathbb{N}$, $\rho : \mathbb{N} \longrightarrow \mathbb{N}$, $\rho(n) = \mu(n)$). Wir kürzen $\alpha_m(n) =: m + n$ ab. Die Abbildung $\mathbb{N} \times \mathbb{N} \ni (m, n) \mapsto m + n \in \mathbb{N}$ heißt *Addition.*

(2) Sei $m \in \mathbb{N}$. Wir definieren die Abbildung $\mu_m : \mathbb{N} \longrightarrow \mathbb{N}$ durch die Bedingungen

$$\mu_m(1) = m,$$
$$\forall n \in \mathbb{N}[\mu_m(n+1) \ = \mu_m(n) + m]$$

(bezüglich $m \in \mathbb{N}$, $\rho : \mathbb{N} \longrightarrow \mathbb{N}$, $\rho(n) = n+m$). Wir kürzen $\mu_m(n) =: m \cdot n$ ab. Die Abbildung $\mathbb{N} \times \mathbb{N} \ni (m,n) \mapsto m \cdot n \in \mathbb{N}$ heißt *Multiplikation.*

(3) Sei $m \in \mathbb{N}$. Wir definieren die Abbildung $\rho_m : \mathbb{N} \longrightarrow \mathbb{N}$ durch die Bedingungen

$$\rho_m(1) = m,$$
$$\forall n \in \mathbb{N}[\rho_m(n+1) = \rho_m(n) \cdot m]$$

(bezüglich $m \in \mathbb{N}$, $\rho(n) = n \cdot m$). Wir kürzen $\rho_m(n) =: m^n$ ab. Die Abbildung $\mathbb{N} \times \mathbb{N} \ni (m,n) \mapsto m^n \in \mathbb{N}$ heißt *Potenzieren.*

Beweis. In allen drei Fällen existieren die Abbildungen und sind eindeutig bestimmt wegen 2.1 $\alpha_1(n) = n+1$ und $\mu(n) = n+1$ können tatsächlich indentifiziert werden wegen $\alpha_1(1) = \mu(1)$ und $\forall n \in \mathbb{N}[\alpha_1(\mu(n)) = \mu(\alpha_1(n))]$ und $\forall n \in \mathbb{N}[\mu\ \mu(n) = \mu\ \mu(n)]$, also wegen $\alpha_1 = \mu$. $\square$

Man muß sich die Bedeutung der Rekursionsformeln klar machen, um zu verstehen, daß mit diesen Konstruktionen etwas ganz Alltägliches gemeint ist. Die Rekursionsformel für die Addition ist gegeben durch $m + (n+1) = (m+n)+1$, also einfach durch einen Spezialfall des Assoziativgesetzes für die Addition. Bei der Multiplikation ist die Bedingung $m \cdot (n+1) = (m \cdot n) + m$, also ein einfacher Fall des Distributivgesetzes. Schließlich fordern wir für das Potenzieren $m^{n+1} = m^n \cdot m$. Daher sind einige einfache Fälle der Rechenregeln für natürliche Zahlen schon in der Definition angelegt. Die anderen Rechenregeln muß man allerdings beweisen.

Satz 3.2. *(Rechengesetz für natürliche Zahlen):*
Für alle $m, n, t \in \mathbb{N}$ gilt:

(1) $m + n = n + m;$ $m \cdot n = n \cdot m;$
(2) $(m + n) + t = m + (n + t);$ $(m \cdot n) \cdot t = m \cdot (n \cdot t);$
(3) $t + m = t + n \Longrightarrow m = n;$ $t \cdot m = t \cdot n \Longrightarrow m = n;$
(Kürzungsgesetz)
(4) $m \cdot (n + t) = m \cdot n + m \cdot t;$
(5) $1 \cdot n = n.$

Beweis. Zunächst weisen wir die Rechnengesetze für die Addition nach.
(1) i) Wir wissen schon $m + (n + 1) = (m + n) + 1$. Durch Induktion nach m beweisen wir zunächst $1 + m = m + 1$. Es ist $1 + 1 = 1 + 1$. Ist $1 + m = m + 1$, so ist auch $1 + (m + 1) = (1+m)+1 = (m+1)+1$. Also folgt die Behauptung. Jetzt zeigen wir $m + (n + 1) = (m + n) + 1 = (m + 1) + n$ durch Induktion nach n. Wir brauchen nur die letzte Gleichung zu zeigen. Es ist $(m + 1) + 1 = (m + 1) + 1$. Ist $(m + n) + 1 = (m + 1) + n$, so ist $(m + (n + 1)) + 1 = ((m + n) + 1) + 1 = ((m + 1) + n) + 1 = (m + 1) + (n + 1)$, also folgt die Behauptung. Jetzt kommen wir endlich zum Kommutativgesetz der Addition, das wir wieder durch Induktion nach n zeigen. Es ist $m + 1 = 1 + m$, wie oben gezeigt. Ist $m + n = n + m$, so folgt $m + (n + 1) = (m + n) + 1 = (n + m) + 1 = (n + 1) + m$ nach dem vorher Gezeigten, und wir sind fertig.
(2) i) Das Assoziativgesetz weisen wir durch Induktion nach t nach. Es ist $(m + n) + 1 = m + (n + 1)$ nach Definition. Gilt $(m+n)+t = m+(n+t)$, so folgt $(m+n)+(t+1) = ((m+n)+t)+1 = (m+(n+t))+1 = m+((n+t)+1) = m+(n+(t+1))$.
(3) i) Induktion nach t: Ist $1+m = 1+n$, so ist nach (P4) $m = n$. Folgt aus $t+m = t+n$ für jede Wahl von m und n immer $m = n$, so folgt $(t+1)+m = (t+1)+n \Longrightarrow 1+(t+m) = 1+(t+n) \Longrightarrow t + m = t + n \Longrightarrow m = n$.
Wir kommen nun zu den Rechengesetzen der Multiplikation. Nach Definition gilt $m \cdot 1 = m$ und $m \cdot (n + 1) = (m \cdot n) + m$.
(5) Aus der Definition folgt $1 \cdot 1 = 1$. Wenn $1 \cdot n = n$ gilt, so folgt $1 \cdot (n + 1) = (1 \cdot n) + 1 = n + 1$.

(1) ii) Wir zeigen zunächst $(n+1) \cdot m = n \cdot m + m$ durch Induktion nach m. Es ist $(n+1) \cdot 1 = n+1 = n \cdot 1 + 1$. Wenn $(n+1) \cdot m = n \cdot m + m$ gilt, so ist $(n+1) \cdot (m+1) = (n+1) \cdot m + (n+1) = n \cdot m + m + n + 1 = n \cdot m + n + m + 1 = n \cdot (m+1) + (m+1)$. Weiter ist nach (5) $1 \cdot m = m = m \cdot 1$. Wenn $n \cdot m = m \cdot n$ gilt, so ist $(n+1) \cdot m = n \cdot m + m = m \cdot n + m = m \cdot (n+1)$.
(4) Es ist $m \cdot (n+1) = m \cdot n + m = m \cdot n + m \cdot 1$. Wenn $m \cdot (n+t) = m \cdot n + m \cdot t$ gilt, so folgt $m \cdot (n + (t+1)) = m \cdot ((n+t)+1) = m \cdot (n+t) + m = m \cdot n + m \cdot t + m = m \cdot n + m \cdot (t+1)$.
(2) ii) Es ist $(m \cdot n) \cdot 1 = m \cdot n = m \cdot (n \cdot 1)$. Ist $(m \cdot n) \cdot t = m \cdot (n \cdot t)$, so folgt $(m \cdot n) \cdot (t+1) = (m \cdot n) \cdot t + m \cdot n = m \cdot (n \cdot t) + m \cdot n = m \cdot ((n \cdot t) + n) = m \cdot (n \cdot (t+1))$.
(3) ii) Diesen Beweis stellen wir bis zum Beweis des Satzes 3.5 zurück. $\square$

Die natürlichen Zahlen tragen noch eine weitere interessante Struktur. Sie bilden eine total geordnete Menge. Die Eigenschaften dieser Ordnung untersuchen wir im folgenden. Insbesondere wird sich herausstellen, daß diese Ordnung zusätzliche wichtige Eigenschaften hat, sie ist eine Wohlordnung. Zunächst definieren wir diese Ordnung auf $\mathbb{N}$.

Definition und Satz 3.3. Auf $\mathbb{N}$ ist eine totale Ordnung gegeben durch $m \leq n :\Longleftrightarrow (m = n \vee \exists p \in \mathbb{N}[p + m = n])$.

Beweis. Die Reflexivität ist unmittelbar klar. Für den Beweis der Transitivität sei $a \leq b$ und $b \leq c$. Wenn in einem der beiden Fälle Gleichheit gilt, so folgt unmittelbar $a \leq c$. Sei also $a+s = b$ und $b + t = c$. Dann folgt $a + s + t = c$, also $a \leq c$. Sei $a \leq b$, $b \leq a$ und $a \neq b$. Dann gilt $a + s = b$ und $b + t = a$, also $a + s + t + 1 = a + 1$, nach 3.2 (3) i) also $s + t + 1 = 1$ im Widerspruch zu (P3). Damit gilt auch die Antisymmetrie. Die Eigenschaft der totalen Ordnung folgt aus der Wohlordnung der natürlichen Zahlen, die wir sogleich zeigen werden. $\square$

Definition 3.4. Eine Ordnung auf einer Menge A heißt *Wohlordnung*, wenn jede nichtleere Teilmenge von A ein kleinstes Element besitzt.

Satz 3.5. (1) $\forall m, n, p \in \mathbb{N}[m \leq n \Longleftrightarrow p + m \leq p + n]$,
(2) $\forall m, n, p \in \mathbb{N}[m \leq n \Longrightarrow p \cdot m \leq p \cdot n]$,
(3) $\forall n \in \mathbb{N}[1 \leq n]$,
(4) $\forall n \in \mathbb{N}[n \neq n + 1]$,
(5) $\{m \in \mathbb{N} | n \leq m \wedge m \leq n + 1\} = \{n, n + 1\}$,
(6) $\mathbb{N}$ *mit* $\leq$ *ist wohlgeordnet.*

Beweis. (1) Gelte $m \leq n$. Wenn $m = n$ gilt, dann ist nichts zu zeigen. Sei $m + t = n$. Dann folgt $p + m + t = p + n$, also $p + m \leq p + n$. Sei umgekehrt $p + m \leq p + n$. Wenn $m \leq n$ ist, ist nichts zu zeigen. Wenn jedoch $m \geq n$ gilt, dann ist nach dem ersten Teil der Aussage $p + m \geq p + n$, zusammen mit der anderen Ungleichung erhält man $p + m = p + n$. Nach dem Kürzungsgesetzt ergibt sich $m = n$.
(2) Gelte $m \leq n$. Dann folgt $p \cdot n = p \cdot (m + t) = p \cdot m + p \cdot t$, also $p \cdot m \leq p \cdot n$.
(3) Es ist $1 \leq 1$. Weiter folgt aus $1 \leq n$ und $1 + t = n$ sofort $1 + t + 1 = n + 1$, also $1 \leq n + 1$. Ist jedoch $1 \leq n$ und $1 = n$, so folgt $1 + 1 = n + 1$, also wieder $1 \leq n + 1$.
(4) Sei $E = \{n \in \mathbb{N} | n \neq n + 1\}$. $1 \in E$ wegen (P3). Sei $n \in E \Longrightarrow n \neq n+1 \Longrightarrow \mu(n) \neq \mu(n+1) \Longrightarrow n+1 \in E \Longrightarrow E = \mathbb{N}$.
(5) Offenbar erfüllen $m = n$ und $m = n + 1$ die Bedingungen $n \leq m$ und $m \leq n+1$. Sei jetzt $m \neq n$ und $n \leq m$ und $m \leq n+1$. Dann ist $m = n + t$ für ein $t \in \mathbb{N}$, also $n + t \leq n + 1$. Wegen $1 \leq t$ gilt auch $n + 1 \leq n + t$ und damit $m = n + t = n + 1$. Also sind die beiden angegebenen Mengen gleich.
(6) Sei $I \subset \mathbb{N}$, $I \neq \emptyset$. Sei $A := \{n \in \mathbb{N} | \forall i \in I[n \leq i]\}$. Wir wollen zeigen, daß $A \cap I \neq \emptyset$. Wenn nämlich dann $r \in A \cap I$, dann gilt $\forall i \in I[r \leq i]$, d.h. $r \in I$ ist das kleinste Element von I. Wir nehmen jetzt an, daß $A \cap I = \emptyset$. Nach (3) ist $1 \in A$. Sei $n \in A$ und sei $i \in I$. Wegen $A \cap I = \emptyset$ ist $n \notin I$, also

$n \neq i$. Weiter ist $n \leq i$, also existiert ein $t \in \mathbb{N}$ mit $n + t = i$. Wegen $1 \leq t$ ist $n + 1 \leq n + t = i$, also ist auch $n + 1 \in A$. Nach Induktionsprinzip ist daher $A = \mathbb{N}$ und $I \subset \mathbb{N} = A$, ein Widerspruch zu $A \cap I = \emptyset$. □

Beweis. von 3.2 (3) ii) Aus $1 \cdot m = 1 \cdot n$ folgt $m = n$. Wenn aus $t \cdot m = t \cdot n$ die Gleichung $m = n$ folgt, so schließen wir wie folgt. Sei $(t + 1) \cdot m = (t + 1) \cdot n$. Wenn $m = n$, dann sind wir schon fertig. Sonst gilt $n \leq m$ oder $m \leq n$. Bis auf Umbenennung können wir $n \leq m$ mit $n + s = m$ annehmen. Dann ist $t \cdot n + n + 1 = (t + 1) \cdot n + 1 = (t + 1) \cdot m + 1 = (t + 1) \cdot (n + s) + 1 = t \cdot n + n + t \cdot s + 1$, nach 3.2 (3) i) also $1 = t \cdot s + 1$ im Widerspruch zu (P3). Also kann $n + s = m$ nicht eintreten. Es gilt daher $n = m$. □

Bemerkung 3.6. Die letzte Aussage des Satzes ist ein wichtiges mathematisches Beweismittel, das man auch die „Jagd nach dem kleinsten Verbrecher“ nennt. Wenn man eine Aussage $\mathfrak{A}(n)$ für alle $n \in \mathbb{N}$ beweisen will und eine vollständige Induktion kompliziert wird, so hilft häufig die folgende Argumentation. Man nimmt an, daß es Elemente $r \in \mathbb{N}$ gibt, für die die Aussage $\mathfrak{A}(n)$ falsch ist. Dann gibt es nach Teil (4) des Satzes auch ein kleinstes solches $n_0 \in \mathbb{N}$, für das $\mathfrak{A}(n_0)$ falsch ist. Das Element n_0 nennt man oft auch den kleinsten „Verbrecher“. Man zeigt dann, daß diese Bedingung zu einem Widerspruch führt. Es gibt also keine Elemente $n \in \mathbb{N}$, für die die Aussage falsch ist. Sie ist daher für alle $n \in \mathbb{N}$ richtig.

Der Begriff der Wohlordnung hat eine weitere ungemein wichtige Bedeutung in der Mengenlehre. Es gibt nämlich ein weiteres Axiom der Mengenlehre über die Wohlordnung. Für viele Anwendungen sind die dazu äquivalenten (und damit auch als Axiome der Mengenlehre verwendbaren) Aussagen ebenso wichtig. Wir können sie hier nur für spätere Anwendungen formulieren, aber ihre Äquivalenz nicht beweisen.

Axiom 7. Jede Menge kann wohlgeordnet werden, d.h. auf jeder Menge gibt es eine Wohlordnung.

Satz 3.7. *Unter den übrigen Axiomen der Mengenlehre sind äquivalent:*

(1) *(Wohlordnungsaxiom) Jede Menge kann wohlgeordnet werden.*
(2) *(Zornsches Lemma) Besitzt in einer geordneten Menge A jede total geordnete Teilmenge eine obere Schranke, so besitzt A ein maximales Element.*
(3) *(Auswahlaxiom) Zu jeder Menge $M \neq \emptyset$ gibt es eine Abbildung $f : \mathcal{P}(M) \longrightarrow M$ mit der Eigenschaft*

$$\forall U \in \mathcal{P}(M) \setminus \{\emptyset\}[f(U) \in U].$$

„Es gibt eine Abbildung f, die aus jeder nichtleeren Teilmenge U von M eines ihrer Elemente, nämlich $f(U)$, auswählt."

Bevor wir weitere Eigenschaften der natürlichen Zahlen studieren, wollen wir einige Beispiele für Mengen der natürlichen Zahlen anführen und erinnern dazu nochmals an den Satz 2.3.

Beispiele 3.8. (1) Ein durch Axiom 6 gegebenes Tripel $(\mathbb{N}, 1, \mu)$ ist eine Menge der natürlichen Zahlen.
(2) Sei $n_0 \in \mathbb{N}$ eine natürliche Zahl. Dann ist die Menge $N := \{n \in \mathbb{N} | n_0 \leq n\}$ zusammen mit n_0 und der Einschränkung $\mu|_N$ von μ als $\mu|_N : N \longrightarrow N$ eine Menge der natürlichen Zahlen.
(3) $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ zusammen mit 0 und μ' mit

$$\mu'(n) = \begin{cases} \mu(n), & \text{für } n \in \mathbb{N}, \\ 1, & \text{für } n = 0, \end{cases}$$

ist eine Menge der natürlichen Zahlen.

(4) $\mathbb{N}_0 \times \mathbb{N}_0$ zusammen mit $(0,0)$ und $\nu : \mathbb{N}_0 \times \mathbb{N}_0 \longrightarrow \mathbb{N}_0 \times \mathbb{N}_0$ mit

$$\nu(m,n) := \begin{cases} (m+1, n-1), & \text{falls } n > 0, \\ (0, m+1), & \text{falls } n = 0, \end{cases}$$

ist eine Menge der natürlichen Zahlen.

Das letzte Beispiel ist etwas komplizierter und zeigt, daß es häufig nicht sofort ersichtlich ist, ob man ein Modell für eine Menge der natürlichen Zahlen vor sich hat. Dabei gibt es einen einfachen Trick, neue Modelle zu konstruieren. Dazu gehen wir noch einmal auf 2.3 zurück. Wenn man zwei Mengen der natürlichen Zahlen $(\mathbb{N}, 1, \mu)$ und (A, a, ν) hat, dann gibt es eine bijektive Abbildung $\alpha : \mathbb{N} \longrightarrow A$, die die gegebenen Strukturen erhält. Hat man nun nur eine Menge A und eine bijektive Abbildung $\alpha : \mathbb{N} \longrightarrow A$, so kann man auf A eine Struktur einer Menge von natürlichen Zahlen immer einführen. Man definiert die „Eins" in A durch $\alpha(1)$ und die Nachfolgerabbildung $\nu : A \longrightarrow A$ durch $\nu := \alpha\mu\alpha^{-1}$. Dann kann man leicht nachprüfen, daß (A, a, ν) eine Menge der natürlichen Zahlen ist. So ist auch unser Beispiel (4) entstanden. Der Leser mag versuchen, die bijektive Abbildung $\alpha : \mathbb{N} \longrightarrow \mathbb{N}_0 \times \mathbb{N}_0$ zu finden.

Man nennt eine Menge A *abzählbar unendlich*, wenn es eine bijektive Abbildung $\alpha : \mathbb{N} \longrightarrow A$ gibt. Die Abbildung wird dann auch eine *Abzählung* von A genannt. Offenbar kann man jede abzählbar unendliche Menge mit der Struktur einer Menge der natürlichen Zahlen versehen. Abzählbar unendliche Mengen sind $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$, $\mathbb{Q}^n$ und viele andere mehr. Die jeweils induzierte Struktur einer Menge der natürlichen Zahlen auf den genannten Mengen hängt selbstverständlich von der gewählten Abzählung ab. Selbst auf $\mathbb{N}$ mit $1 \in \mathbb{N}$ kann man verschiedene Nachfolgerfunktionen $\mu_i : \mathbb{N} \longrightarrow \mathbb{N}$ angeben, mit denen $(\mathbb{N}, 1, \mu_i)$ eine Menge der natürlichen Zahlen wird. Man kann also sehr exotische Beispiele für Mengen der natürlichen Zahlen finden. Beispiele für unendliche Mengen, die nicht abzählbar sind, sind $\mathbb{R}$, $\mathbb{C}$ und $\mathrm{Abb}(\mathbb{R},\mathbb{R}) = \mathbb{R}$, die Menge der reellen Funktionen. Diese Überlegungen führen jetzt aber schon in das Gebiet der Kardinalzahlen, die wir nicht weiter betrachten wollen.

Eine der wichtigen Rechenregeln in den natürlichen Zahlen ist die Division mit Rest, die in der Zahlentheorie eine grundlegende Bedeutung hat. Wir beweisen sie hier vor allem, um in der Folgerung eine Aussage über die Darstellung des größten gemeinsamen Teilers zweier Zahlen zu erhalten. Der dort angegebene Algorithmus ist Grundlage vieler zahlentheoretischer Programmpakete auf Computern.

Wir geben die Division mit Rest gleich für die Menge der ganzen Zahlen an, weil sie in dieser Menge ihre volle Nützlichkeit entwickelt. Man kann auch leicht die Division mit Rest für natürliche Zahlen formulieren und beweisen. Wie man formal die Menge der ganzen Zahlen $\mathbb{Z}$ einführt, werden wir erst im 5. Abschnitt dieses Kapitels diskutieren.

Satz 3.9. *(Division mit Rest) Es gilt*

$$\forall x \in \mathbb{Z}, n \in \mathbb{N} \exists q \in \mathbb{Z}, r \in \mathbb{N}_0 [x = qn + r \wedge r \leq n - 1],$$

und in dieser Darstellung sind q und r durch x und n eindeutig bestimmt.

Beweis. Sei $M := \{x - pn | p \in \mathbb{Z} \wedge 0 \leq x - pn\}$. Dann gilt $M \subset \mathbb{N}_0$ und $M \neq \emptyset$. Denn für $x \geq 0$ ist $x \in M$ und für $x < 0$ ist $x - xn = x(1 - n) = (-x)(n - 1) \geq 0$, also $x - xn \in M$. Da $\mathbb{N}$ und damit auch $\mathbb{N}_0$ wohlgeordnet sind, existiert ein kleinstes Element $r \in M$ mit $x - qn = r$ oder $x = qn + r$. Wenn $r \geq n$, dann ist $r - n \geq 0$ und $x - qn - n = x - (q + 1)n = r - n$, also $r - n \in M$ im Widerspruch dazu, daß r minimal in M gewählt ist. Damit ist $r \leq n - 1$. Um nun die Eindeutigkeit von q und r zu zeigen, gelte auch $x = qn + r = q'n + r'$ mit $r' \leq n - 1, r' \in \mathbb{N}_0$

und $q' \in \mathbb{Z}$. Ohne Einschränkung der Allgemeinheit kann $r \leq r'$ angenommen werden. Dann ist $0 \leq r' - r = qn - q'n = (q - q')n$. Damit ist auch $q - q' \geq 0$. Wäre nun $q - q' \geq 1$, so wäre $(q - q')n \geq n$ im Widerspruch zu $(q - q')n = r' - r \leq n - 1$. Daher muß $q = q'$ und dann auch $r = x - qn = x - q'n = r'$ gelten. □

Folgerung 3.10. *Seien $m, n \in \mathbb{Z}$ nicht beide 0, und sei $t \in \mathbb{N}$ größter gemeinsamer Teiler von m und n. Dann gibt es $a, b \in \mathbb{Z}$ mit $am + bn = t$.*

Beweis. Sei t kleinstes Element in der Menge $M := \{am + bn | a, b \in \mathbb{Z} \wedge am + bn > 0\}$. Da die Menge offenbar nicht leer ist und in $\mathbb{N}$ liegt, existiert t, und es ist $t = a_0 m + b_0 n$. Die Division mit Rest ergibt $m = qt + r$ mit $0 \leq r < t$. Wegen $r = m - qt = m - qa_0 m - qb_0 n = (1 - qa_0)m - qb_0 n$ ist $r \in M$ oder $r = 0$. Weil t in M minimal ist und $r < t$ gilt, muß $r = 0$ gelten. Also ist $m = qt$. Ebenso erhält man $n = pt$. Also ist t ein gemeinsamer Teiler von m und n. Ist $d \in \mathbb{N}$ ein weiterer gemeinsamer Teiler von m und n, so gilt $xd = m$ und $yd = n$, also $t = a_0 xd + b_0 yd = (a_0 x + b_0 y)d$. Damit ist d ein Teiler von t und t größter gemeinsamer Teiler von m und n. □

Bemerkung 3.11. Einen Algorithmus zur Bestimmung von t, a_0 und b_0 aus m und $n \neq 0$ erhält man so:
1. Schritt: man führe eine Division mit Rest aus: $m = q \cdot n + r$ und $0 \leq r < n$. Das kann man z.B. mit den in Computersprachen vorhandenen Operationen $q = \operatorname{div}(m, n)$ und $r = \operatorname{mod}(m, n)$ durchführen.
2. Schritt: man iteriere den 1. Schritt, indem man m durch n, n durch r ersetzt, bis $r = 0$ eintritt.

$$\begin{array}{llll}
m_0 := m, & n_0 := n, & m_0 = q_0 n_0 + r_0, & 0 \leq r_0 < n_0, \\
m_1 := n_0, & n_1 := r_0, & m_1 = q_1 n_1 + r_1, & 0 \leq r_1 < r_0, \\
\vdots & \vdots & \vdots & \vdots \\
m_k := n_{k-1}, & n_k := r_{k-1}, & m_k = q_k n_k. &
\end{array}$$

Dann ist n_k der größte gemeinsame Teiler von m und n, denn $n_k = r_{k-1}$ teilt $m_k = n_{k-1}$ und wegen $m_{k-1} = q_{k-1}n_{k-1} + r_{k-1}$ auch m_{k-1}. Nach endlich vielen Schritten ist dann n_k ein Teiler von m und n. Weiter ist $r_0 = m - q_0 n$ und $r_1 = m_1 - q_1 n_1 = n - q_1(m - q_0 n) = -q_1 m + (1 + q_0)n$. Ist $r_i = a_i m + b_i n$ und $r_{i+1} = a_{i+1}m + b_{i+1}n$, so ist $r_{i+2} = m_{i+2} - q_{i+2}n_{i+2} = r_i - q_{i+2}r_{i+1} = a_i m + b_i n - q_{i+2}(a_{i+1}m + b_{i+1}n) = (a_i - q_{i+2}a_{i+1})m + (b_i - q_{i+2}b_{i+1})n$. Also sind alle Reste, insbesondere aber r_{k-1} von der Form $r_{k-1} = am + bn$. Also ist jeder gemeinsame Teiler von m und n auch Teiler von r_{k-1}, d.h. r_{k-1} ist größter gemeinsamer Teiler. Die obige Berechnung der Faktoren a und b durch den Übergang

$$\begin{pmatrix} a_i & a_{i+1} \\ b_i & b_{i+1} \end{pmatrix} \mapsto \begin{pmatrix} a_{i+1} & a_i - q_{i+2}a_{i+1} \\ b_{i+1} & b_i - q_{i+2}b_{i+1} \end{pmatrix}$$

in jedem Schritt des Algorithmus ergibt mit dem Anfangswert $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ die gewünschte Darstellung $\mathrm{ggT}(m, n) = am + bn$. Der Anfangswert ist dadurch zu erklären, daß man den gegebenen Algorithmus eventuell durch Umbenennung mit $m > n$ durchführt (der Fall $m = n$ ist trivial) und ihn noch um eine Zeile nach oben hin erweitert, nämlich

$$m_{-1} := n, \quad n_{-1} := m, \quad m_{-1} = 0 \cdot n_{-1} + r_{-1}, \quad 0 \leq r_{-1} < n_{-1}.$$

Damit hat man $r_{-2} := n_{-1} = m = 1 \cdot m + 0 \cdot n$ und $r_{-1} = n = 0 \cdot m + 1 \cdot n$. Dann kann man die iterative Anwendung der Division mit Rest in jedem Schritt begleiten von der angegebenen Umschreibung der Paare (a_i, b_i) und (a_{i+1}, b_{i+1}). Wenn der Algorithmus dann abbricht, hat man insbesondere die Koeffizienten der Darstellung $r_{k-1} = am + bn$ erhalten.

4. Anzahlaussagen

Nachdem in Kapitel I in Definition 2.29 eine abstrakte Definition von endlichen Mengen ohne Rückgriff auf natürliche Zahlen gegeben wurde und jetzt die natürlichen Zahlen mit vielen ihrer Eigenschaften auch zur Verfügung stehen, können wir auch die viel anschaulichere Beschreibung endlicher Mengen geben, nämlich mit Hilfe der endlichen durch eine natürliche Zahl festgelegten Anzahl der Elemente in einer Menge. Wir werden danach in diesem Abschnitt für eine Reihe von Mengen die Anzahl ihrer Elemente genau bestimmen.

Satz 4.1. *Die Menge* $\{1,\dots,n\} := \{i \in \mathbb{N} | 1 \le i \le n\}$ *ist endlich.*

Beweis. Sei $\alpha : \{1,\dots,n\} \longrightarrow \{1,\dots,n\}$ injektiv. Es ist nach Kapitel I 2.30 zu zeigen, daß α surjektiv ist. Wir beweisen das durch vollständige Induktion nach n. Die Behauptung ist klar für $n = 1$. Sei $\alpha : \{1,\dots,n+1\} \longrightarrow \{1,\dots,n+1\}$ eine injektive Abbildung und $\alpha' : \{1,\dots,n\} \longrightarrow \{1,\dots,n+1\}$ die Einschränkung von α.
1. Fall: $\mathrm{Bi}(\alpha') \subseteq \{1,\dots,n\}$. Dann ist α' injektiv und nach Induktionsannahme damit auch surjektiv, also bijektiv. Da α injektiv ist, ist $\alpha(n+1) \notin \{1,\dots,n\}$, also $\alpha(n+1) = n+1$. Damit ist α surjektiv.
2. Fall: Wenn $\mathrm{Bi}(\alpha') \not\subseteq \{1,\dots,n\}$, dann gibt es genau ein i mit $\alpha'(i) = n+1 = \alpha(i)$. Da α injektiv ist, gibt es auch ein $j \in \{1,\dots,n\}$ mit $\alpha(n+1) = j$. Sei nun $\beta : \{1,\dots,n\} \longrightarrow \{1,\dots,n\}$ definiert durch

$$\beta(m) = \begin{cases} \alpha(m), & m \neq i, \\ j, & m = i. \end{cases}$$

α injektiv $\Longrightarrow$ β surjektiv $\Longrightarrow$ alle Zahlen $\{1,\dots,n+1\} \setminus \{j, n+1\}$ kommen in $\mathrm{Bi}(\alpha)$ vor, aber auch $n+1$ und j, also ist α surjektiv. □

Satz 4.2. *Seien* m, n *natürliche Zahlen.*

(1) *Es gibt dann und nur dann eine injektive Abbildung* $\alpha : \{1,\dots,m\} \longrightarrow \{1,\dots,n\}$, *wenn* $m \le n$ *gilt.*

(2) *Es gibt dann und nur dann eine surjektive Abbildung* $\alpha : \{1, \ldots, m\} \longrightarrow \{1, \ldots, n\}$, *wenn* $m \geq n$ *gilt.*
(3) *Es gibt dann und nur dann eine bijektive Abbildung* $\alpha : \{1, \ldots, m\} \longrightarrow \{1, \ldots, n\}$, *wenn* $m = n$ *gilt.*

Beweis. (1) Wenn $m \leq n$, dann ist die Inklusionsabbildung eine injektive Abbildung. Wenn $m > n$ ist, dann ist die Komposition $\{1, \ldots, m\} \xrightarrow{\alpha} \{1, \ldots, n\} \hookrightarrow \{1, \ldots, m\}$ ebenfalls injektiv, also nach 4.1 surjektiv, aber m ist nicht nur im Bild dieser Abbildung wegen $m > n$. Widerspruch. Damit ist $m \leq n$.
(2) Sei $m \geq n$. Dann ist

$$\alpha(i) = \begin{cases} i & 1 \leq i \leq n \\ 1 & n < i \leq m \end{cases}$$

eine surjektive Abbildung $\alpha : \{1, \ldots, m\} \longrightarrow \{1, \ldots, n\}$.
Sei α surjektiv. Sei $\beta : \{1, \ldots, n\} \longrightarrow \{1, \ldots, m\}, g(i) =$ kleinstes $j : \alpha(j) = i$.
Damit ist β eine Abbildung und injektiv. $\Longrightarrow$ (nach Teil (1)) $n \leq m$.
(3) Wenn $n = m$ ist, dann ist die identische Abbildung eine bijektive Abbildung. Wenn $\alpha : \{1, \ldots, m\} \longrightarrow \{1, \ldots, n\}$ bijektiv ist, dann ist $m \leq n$ nach Teil 1 und $m \geq n$ nach Teil 2, also $m = n$. $\square$

Jetzt haben wir die Hilfsmittel zur Verfügung, um zu zeigen, daß die Endlichkeit einer Menge damit zusammenfällt, daß sie mit den natürlichen Zahlen bis zu einer bestimmten Zahl n abgezählt werden kann. Der Beweis des folgenden Satzes wird auch ergeben, daß die Anzahl der Elemente einer endlichen Menge von der Wahl der Abzählung, d.h. von der Reihenfolge, wie die Elemente abgezählt werden, unabhängig ist. Die zunächst so selbstverständlich erscheinende Tatsache, daß jede Abzählung einer endlichen Menge zu derselben Anzahl von Elementen führt, hat einen recht komplizierten Beweis, den wir auch als Beweis (mit einem Stern) markiert haben, der in der Vorlesung ausgelassen werden kann.

Satz 4.3. *Eine Menge $A \neq \emptyset$ ist genau dann endlich, wenn es ein $m \in \mathbb{N}$ und eine bijektive Abbildung $\beta : \{1, \dots , m\} \longrightarrow A$ gibt. m ist durch A eindeutig bestimmt und wird* Anzahl *der Elemente von A genannt.*

Beweis*. Die eine Richtung des Beweises ist recht einfach. Sei $\beta : \{1, \dots , m\} \longrightarrow A$ eine bijektive Abbildung. Sei $\gamma : A \longrightarrow A$ injektiv. Dann ist auch $\beta^{-1}\gamma\beta : \{1, \dots , m\} \longrightarrow \{1, \dots , m\}$ injektiv, also auch surjektiv. Damit wird dann auch $\gamma = \beta\beta^{-1}\gamma\beta\beta^{-1}$ surjektiv, also ist A endlich.

Die andere Richtung des Beweises ist die eigentlich wichtige Aussage des Satzes. Wir erläutern zunächst die Idee dieses längeren Beweises. Wir wollen die vorgegebene Menge so abzählen wie wir es uns naiv vorstellen. Dazu benötigen wir eine Abzählabbildung von $\mathbb{N}$ in A. Wir hoffen, daß wir nicht alle natürlichen Zahlen benötigen, aber ob das geht, werden wir erst später feststellen können. Eine Abbildung $\mathbb{N} \longrightarrow A$ kann mit einfacher Rekursion definiert werden. Der Anfang ist leicht: wir wählen irgendein Element von A, das wir als erstes abzählen. Die Fortsetzung der Abzählung ist komplizierter. Wenn wir schon n Elemente aus A abgezählt haben, dann müssen wir das nächste abzuzählende Element angeben. Es darf nicht unter den schon abgezählten Elementen vorkommen. Deshalb genügt es für die einfache Rekursion nicht, lediglich das letzte abgezählte Element zu kennen, man muß die Teilmenge U aller bisher abgezählten Elemente kennen. Dann kann man daraus das nächste abzuzählende Element festlegen, indem man ein Element aus dem Komplement von U in A wählt. Es kommt also eine Variante des Auswahlaxioms mit ins Spiel, weil wir zu jeder Teilmenge U ein Element außerhalb wählen müssen. Diese formulieren wir zunächst.

Sei also $A \neq \emptyset$ endlich. Wir benutzen eine Auswahlabbildung $f : \mathcal{P}(A) \setminus \{\emptyset\} \longrightarrow A$ (vgl. 3.7) mit $f(U) \in U$ für alle Teilmengen

$U \neq \emptyset$ von A. Weiter sei $g : \mathcal{P}(A) \setminus \{A\} \longrightarrow A$ die Abbildung $g(U) := f(A \setminus U)$. Dann gilt $g(U) \notin U$ für alle Teilmengen $U \neq A$ von A.

Sei $X := \{(a, U) | a \in U, U \in \mathcal{P}(A)\} \subset A \times \mathcal{P}(A)$. Wir definieren eine Abbildung $\varphi : X \longrightarrow X$ durch

$$\varphi(a, U) := \begin{cases} (g(U), U \cup \{g(U)\}) & \text{für } U \neq A, \\ (a, A) & \text{für } U = A. \end{cases}$$

Weiter legen wir ein Element $a_1 \in A$ und damit ein Element $(a_1, U_1) \in X$ mit $U_1 := \{a_1\}$ fest.

Nach Satz 2.1 gibt es genau eine Abbildung, d.h. eine Folge, $\alpha : \mathbb{N} \longrightarrow X$ mit $\alpha(1) = (a_1, U_1)$ und $\alpha(r+1) = \varphi(\alpha(r))$. Wir schreiben $(a_r, U_r) := \alpha(r)$ und erhalten so $(a_{r+1}, U_{r+1}) = \varphi(a_r, U_r)$, also

$$a_{r+1} = \begin{cases} g(U_r), & \text{wenn } U_r \neq A, \\ a_r, & \text{wenn } U_r = A, \end{cases}$$
$$U_{r+1} = \begin{cases} U_r \cup \{a_{r+1}\}, & \text{wenn } U_r \neq A, \\ A, & \text{wenn } U_r = A. \end{cases}$$

Wir können uns U_r als die Menge $\{a_1, \ldots, a_r\} = \{a_i | 1 \leq i \leq r\}$ vorstellen, jedoch ist nicht klar, daß U_r tatsächlich diese Form hat.

Im Falle $U_r \neq A$ ist nun $a_{r+1} = g(U_r) \notin U_r$, also $U_r \subsetneqq U_{r+1}$. Im Falle $U_r = A$ ist $U_r \subset U_{r+1}$. Sei $r < s$ und $U_r \neq A$. Dann ist $U_r \subsetneqq U_{r+1}$. Ist $U_r \subsetneqq U_{r+t}$, so ist dann $U_{r+t} \subset U_{r+t+1}$, also auch $U_r \subsetneqq U_{r+t+1}$. Damit ist mit vollständiger Induktion $U_r \subsetneqq U_{r+t}$ für alle $t \in \mathbb{N}$, insbesondere also $U_r \subsetneqq U_s$.

Sei $r < s$ und $U_r \neq A$. Wir zeigen jetzt, daß dann $a_r \neq a_s$ gilt. Für $s = r+1$ haben wir $a_s = a_{r+1} \notin U_r$ und wegen $a_r \in U_r$ gilt $a_s \neq a_r$. Ist $s = r+t$ und $a_{r+t} \neq a_r$, so gibt es zwei Fälle. Ist $U_s = A$, so ist $a_{r+t+1} = a_{s+1} = a_s \neq a_r$. Ist $U_s \neq A$, so ist

$a_{r+t+1} = a_{s+1} \notin U_s$, also auch $a_{r+t+1} \notin U_r$ und damit $a_{r+t+1} \neq a_r$. Die Behauptung $a_r \neq a_{r+t}$ gilt also für alle $t \in \mathbb{N}$.

Wir betrachten die Menge $B := \{a_i | i \in \mathbb{N}\} \subset A$. Wenn für alle $r \neq s$ gilt $a_r \neq a_s$, dann ist die Abbildung $\mathbb{N} \ni i \mapsto a_i \in B$ bijektiv. Wir können damit die Abbildung $B \ni a_i \mapsto a_{i+1} \in B$ konstruieren, die injektiv ist, aber nicht surjektiv. B ist als Teilmenge von A aber ebenfalls endlich, ein Widerspruch.

Daher gibt es $r < s$ mit $a_r = a_s$. Nach der vorhergehenden Überlegung ist dann $U_r = A$. Sei $m \in \mathbb{N}$ die kleinste solche Zahl, d.h. die kleinste Zahl in $\{s \in \mathbb{N} | U_s = A\}$. Wir zeigen jetzt, daß die Abbildung $\beta : \{1, \ldots, m\} \longrightarrow A$ mit $\beta(i) = a_i$ bijektiv ist. Für alle $r < m$ ist $U_i \neq A$ und daher sind alle a_r für $r \in \{1, \ldots, m\}$ paarweise verschieden, d.h. β ist injektiv. Sei nun $a \in A$ und $a \notin \mathrm{Bi}(\beta)$. Dann ist $a \neq a_1$ und daher $a \notin U_1$. Ist $a \notin U_r$, so ist $a \notin U_r \cup \{\beta(r+1)\} = U_r \cup \{a_{r+1}\} = U_{r+1}$, also ist $a \notin U_n$ für alle $n \in \mathbb{N}$. Das ist ein Widerspruch wegen $U_m = A$. Daher ist β auch surjektiv.

Die Eindeutigkeit von m folgt nun unmittelbar aus Satz 4.2. $\square$

Folgerung 4.4. (1) *(Dirichletsches Schubfächerprinzip): Wenn man n Objekte auf m Schubfächer verteilt und $n > m$ ist, dann gibt es mindestens ein Schubfach, das mehrere Objekte enthält.*

(2) *Wenn man n Objekte auf m Schubfächer verteilt und $n < m$ ist, dann gibt es mindestens ein leeres Schubfach.*

Beweis. (1) $\alpha : \{1, \ldots, n\} \longrightarrow \{1, \ldots, m\}$ und $n > m$ impliziert, daß α nicht injektiv ist. Also existiert ein Schubfach j und Objekte i_1, i_2 mit $\alpha(i_1) = \alpha(i_2) = j$.
(2) $\alpha : \{1, \ldots, n\} \longrightarrow \{1, \ldots, m\}$ und $n < m$ impliziert, daß α nicht surjektiv ist. Also existiert ein Schubfach j mit $\alpha^{-1}(j) = \emptyset$. $\square$

Definition 4.5. Wir bezeichnen mit $\mathbb{N}_0 \ni n \mapsto n! \in \mathbb{N}$ die eindeutig bestimmte Abbildung mit $0! := 1, 1! = 1$ und $(n+1)! = n! \cdot (n+1)$. (2.2)

Satz 4.6. *Es gibt $n!$ verschiedene bijektive Abbildungen*

$$\alpha : \{1, \dots, n\} \longrightarrow \{1, \dots, n\}.$$

Diese Abbildungen heißen Permutationen.

Beweis. (durch vollständige Induktion) Wir beweisen allgemeiner: Sind A, B Mengen mit je n Elementen, dann gibt es genau $n!$ Bijektionen von A nach B. Ist $n = 1$, so ist das klar. Sei die Behauptung für Mengen mit n Elementen richtig. Seien $A = \{a_1 \dots, a_{n+1}\}$ und $B = \{b_1, \dots, b_{n+1}$ Mengen mit $n+1$ Elementen. Wir definieren $A_i := A \setminus \{a_i\}, B_i := B \setminus \{b_i\}$. Sei $\alpha : A \longrightarrow B$ eine Bijektion mit $\alpha(a_{n+1}) = b_i$. Dann ist $\alpha' : A_n \longrightarrow B_i$ wieder bijektiv mit $\alpha'(a_j) = \alpha(a_j)$. Umgekehrt kann jede Bijektion $\alpha' : A_n \longrightarrow B_i$ zu einer Bijektion $\alpha : A \longrightarrow B$ fortgesetzt werden durch $\alpha(a_j) = \begin{cases} \alpha'(a_j) & j \leq n \\ b_i & j = n+1 \end{cases}$. Nach Induktionsannahme gibt es $n!$ bijektive $\alpha' : A_n \longrightarrow B_i$, also auch $n!$ bijektive Abbildungen $\alpha : A \longrightarrow B$ mit $\alpha(a_n) = b_i$. Es gibt $n+1$ Möglichkeiten für die Wahl von b_i, also insgesamt $n! \cdot (n+1) = (n+1)!$ bijektive Abbildungen $\alpha \cdot A \longrightarrow B$. □

Satz 4.7. *Seien $A = \{a_1, \dots, a_m\}$ und $B = \{b_1, \dots, b_n\}$ endliche Mengen mit m bzw. n Elementen. Dann gibt es n^m Abbildungen von A nach B.*

Beweis. Durch Induktion nach m: Für $m = 1$ gibt es offenbar $n = n^1$ Abbildungen $\alpha(a_1) = b_i$. Sei die Behauptung für m und alle $n \in \mathbb{N}$ wahr und sei $A = \{a_1, \dots, a_{m+1}\}$. Dann läßt sich jede Abbildung $\alpha' : \{a_1, \dots, a_m\} \longrightarrow \{b_1, \dots, b_n\}$ fortsetzen zu einer Abbildung $\alpha : A \longrightarrow B$ durch die Festsetzung $\alpha(a_(m+1) := b_i$ (und $\alpha(a_j) = \alpha'(a_j)$ für $1 \leq J \leq m$) und jede Abbildung $\alpha : A \longrightarrow B$ kommt auf diese Weise vor. Also gibt es $n^m \cdot n = n^{m+1}$ Abbildungen von A nach B. □

Definition und Lemma 4.8. Sei $B \subset A$ eine Teilmenge. Die *charakteristische Funktion* χ_B von B ist die Abbildung χ_B :

$A \longrightarrow \{0,1\}$ mit

$$\chi_B(a) = \begin{cases} 0 & a \notin B \\ 1 & a \in B. \end{cases}$$

Dann ist $\mathcal{P}(A) \ni B \mapsto \chi_B \in \mathrm{Abb}(A, \{0,1\}) = \{0,1\}^A$ eine bijektive Abbildung.

Beweis. Die Umkehrabbildung ist $\alpha \mapsto B := \{a \in A | \alpha(a) = 1\} = \alpha^{-1}(1)$. $\square$

Folgerung 4.9. *Sei A eine endliche Menge mit n Elementen. Dann besitzt A genau 2^n Teilmengen, d.h. die Potenzmenge $\mathcal{P}(A)$ besitzt genau 2^n Elemente.*

Beweis. $\mathcal{P}(A)$ und $\{1,2\}^A$ haben gleich viele, also 2^n Elemente. $\square$

Definition 4.10. Der *Binomialkoeffizient* $\begin{pmatrix} n \\ r \end{pmatrix}$ ist die Anzahl der r-elementigen Teilmengen einer Menge A mit n Elementen für $0 \leq r \leq n$. Wir definieren für $r > 0$: $\begin{pmatrix} n \\ -r \end{pmatrix} := 0$, und für $m > n$: $\begin{pmatrix} n \\ m \end{pmatrix} := 0$.

Beachte: $\begin{pmatrix} n \\ 0 \end{pmatrix} = \begin{pmatrix} n \\ n \end{pmatrix} = 1$.

Folgerung 4.11. $\sum_{r=0}^{n} \begin{pmatrix} n \\ r \end{pmatrix} = 2^n$.

Beweis. Durch Abzählen der r-elementigen Teilmengen für alle r. $\square$

Satz 4.12. *Für alle $n \in \mathbb{N}_0$ und $0 \leq r \leq n$ gilt*

$$\begin{pmatrix} n \\ r-1 \end{pmatrix} + \begin{pmatrix} n \\ r \end{pmatrix} = \begin{pmatrix} n+1 \\ r \end{pmatrix}.$$

BEWEIS. Bezeichne $|B|$ die Anzahl der Elemente von B. Sei A eine Menge mit $n+1$ Elementen und sei $a \in A$, $A' := A \setminus \{a\}$. Dann ist

$$
\begin{aligned}
\binom{n+1}{r} &= \left|\left\{U \subset A \,\middle|\, |U| = r\right\}\right| \\
&= \left|\left\{U \subset A \,\middle|\, a \in U \wedge |U| = r\right\} \dot\cup \left\{U \subset A \,\middle|\, a \notin U \wedge |U| = r\right\}\right| \\
&= \Big|\left\{U \subset A \,\middle|\, \exists V \subset A'[U = V \dot\cup \{a\} \wedge |V| = r-1]\right\} \dot\cup \\
&\qquad\qquad \left\{U \subset A' \,\middle|\, |U| = r\right\}\Big| \\
&= \left|\left\{V \subset A' \,\middle|\, |V| = r-1\right\} \dot\cup \left\{U \subset A' \,\middle|\, |U| = r\right\}\right| \\
&= \binom{n}{r-1} + \binom{n}{r}.
\end{aligned}
$$

□

Folgerung 4.13. *(Pascalsches Dreieck für Binomialkoeffizienten): Man erhält das Pascalsche Dreieck, indem man die beiden Seiten des Dreiecks mit Einsen besetzt und das Innere dadurch ausfüllt, daß man je zwei nebeneinander stehende Zahlen addiert und darunter zwischen ihnen notiert:*

$$
\begin{array}{lccccccccc}
\binom{0}{0} & & & & & 1 & & & & \\
\binom{1}{r} & & & & 1 & & 1 & & & \\
\binom{2}{r} & & & 1 & & 2 & & 1 & & \\
\binom{3}{r} & & 1 & & 3 & & 3 & & 1 & \\
\binom{4}{r} & 1 & & 4 & & 6 & & 4 & & 1
\end{array}
\qquad
\begin{array}{ccc}
\binom{n}{r-1} & + & \binom{n}{r} \\
& \binom{n+1}{r} &
\end{array}
$$

Jeder Eintrag dieses Dreiecks in der n-ten Zeile an der r-ten Stelle enthält dann den Wert $\binom{n}{r}$.

Satz 4.14. *Für* $0 \leq r \leq n$ *gilt* $\binom{n}{r} = \dfrac{n!}{r!(n-r)!}$

Beweis. Durch vollständige Induktion nach n beweisen wir

$$\mathfrak{A}(n) :\Longleftrightarrow \forall r \in \mathbb{N}\Big[0 \leq r \leq n \Longrightarrow \binom{n}{r} = \frac{n!}{r!(n-r)!}\Big].$$

Induktionsanfang: Es ist $\binom{1}{0} = 1 = \dfrac{1!}{0! \cdot 1!}$ und $\binom{1}{1} = 1 = \dfrac{1!}{1! \cdot 0!}$.
Induktionsannahme: Sei $\mathfrak{A}(n)$ wahr.
Induktionsschluß:

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r} = \frac{n!}{(r-1)!(n-r+1)!} + \frac{n!}{r!(n-r)!}$$
$$= \frac{n! \cdot r + n!(n+1-r)}{r!(n+1-r)!} = \frac{(n+1)!}{r!((n+1)-r)!}$$

für $1 \leq r \leq n$.
Für $r = 0$ ist $\binom{n+1}{0} = 1 = \dfrac{(n+1)!}{0!(n+1)!}$ und für $r = n+1$ ist $\binom{n+1}{n+1} = 1 = \dfrac{(n+1)!}{(n+1)!0!}$. □

Satz 4.15. *(Die binomische Formel) Für alle* $a, b \in \mathbb{R}$ *und* $n \in \mathbb{N}$ *gilt*

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}.$$

Beweis. Beim Ausmultiplizieren kommt a^r so oft vor, wie man r Faktoren aus n Faktoren auswählen kann, also $\binom{n}{r}$ mal. Die restlichen $n - r$ Faktoren ergeben b^{n-r}. □

5. Ein kurzer Aufbau des Zahlensystems

In diesem kurzen Abschnitt wollen wir andeuten, wie man nun mit den für die natürlichen Zahlen gewonnenen Eigenschaften das weitere Zahlsystem entwickelt werden kann. Wir geben lediglich die Konstruktionen der Mengen der ganzen Zahlen, der rationalen Zahlen, der reellen Zahlen und der komplexen Zahlen an, ohne jeweils die Rechengesetze herzuleiten. Lediglich für die komplexen Zahlen definieren wir die Addition und die Multiplikation.

Definition 5.1. Die Menge der *ganzen Zahlen* $\mathbb{Z}$ wird wie folgt definiert. Auf $\mathbb{N} \times \mathbb{N}$ bildet man eine Äquivalenzrelation $\sim$ durch

$$(a, b) \sim (c, d) :\Longleftrightarrow a + d = b + c.$$

Die Menge der Äquivalenzklassen $\mathbb{N} \times \mathbb{N}/\sim$ ist dann $\mathbb{Z}$.
Man fasse die Klasse $\overline{(a, b)}$ als $a - b$ auf.

Definition 5.2. Die Menge der *rationalen Zahlen* $\mathbb{Q}$ wird wie folgt definiert. Auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ bildet man eine Äquivalenzrelation $\sim$ durch

$$(a, b) \sim (c, d) :\Longleftrightarrow ad = cb.$$

Dann definiert man $\mathbb{Q} := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/\sim$ und kürzt $\overline{(a, b)}$ durch $\frac{a}{b}$ ab.

Definition 5.3. Die Menge der *reellen Zahlen* $\mathbb{R}$ wird wie folgt definiert. Eine Teilmenge $a \subset \mathbb{Q}$ heißt *Dedekindscher Schnitt*, wenn

(1) $a \neq \emptyset \wedge a \neq \mathbb{Q}$,
(2) $\forall x \in a \forall y \in \mathbb{Q}[x \leq y \Longrightarrow y \in a]$,
(3) a enthält kein kleinstes Element (bzgl. der Ordnung von $\mathbb{Q}$).

Die Menge $\mathbb{R}$ der reellen Zahlen ist die Menge der Dedekindschen Schnitte. Eine reelle Zahl ist also ein Dedekindscher Schnitt.

Nach Einführung der Ordnung in der Mange der reellen Zahlen und der Identifizierung der rationalen Zahlen mit speziellen reellen Zahlen stellt sich dann heraus, daß der zugehörige Dedekindsche Schnitt für eine reelle Zahl r aus allen rationalen Zahlen x mit $r < x$ besteht.

Definition 5.4. Die Menge der *komplexen Zahlen* $\mathbb{C}$ ist $\mathbb{R} \times \mathbb{R}$ mit den Rechenoperationen $(a, b) + (c, d) = (a + c, b + d)$ und $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$. Es ist $i := (0, 1)$.