Aufbau des Zahlensystems und Funktionenlehre

Dr. Theo Overhagen
Mathematik
Universität Siegen

Vorbemerkung

Ziel der folgenden Vorlesung ist der Aufbau des Zahlensystems von den natürlichen zu den reellen Zahlen sowie eine Einführung der elementaren Funktionen. Dabei soll nicht eine strenge Systematik oder Axiomatik im Vordergrund stehen, sondern wir wollen das vorhandene Wissen über die verschiedenen Zahlenmengen ordnen, überlegen, wozu man diese Zahlenmengen verwendet und wie man mit ihnen umgeht, und uns die Zusammenhänge klarmachen.

Vorausgesetzt wird ein Wissen über die verschiedenen Zahlenmengen, wie es in der Schule vermittelt wird, z.B. die Kenntnis der natürlichen Zahlen $1, 2, 3, \cdots$, der Null sowie der negativen ganzen Zahlen $-1, -2, -3, \cdots$, der rationalen Zahlen (Brüche) $\frac{1}{3}, \frac{2}{3}, -\frac{195}{14}$ sowie gewisser reeller nichtrationaler (irrationaler) Zahlen wie $\sqrt{5}$, π oder e.

Weiter wird vorausgesetzt, daß grundlegende Begriffe der naiven Mengenlehre bekannt sind wie z.B. „Element“ und „Elementbeziehung“ $x \in M$, „Teilmenge“ und „Teilmengenbeziehung“ $M \subset N$, „Durchschnitt“ $M \cap N$, „Vereinigung“ $M \cup N$ oder „Mengendifferenz“ $M \setminus N$. Wie üblich, wird die „leere Menge“ mit $\emptyset$ bezeichnet.

Weiter wird der Funktionsbegriff vorausgesetzt zusammen mit den grundlegenden möglichen Zusatzeigenschaften von Funktionen wie „injektiv“, „surjektiv“ und „bijektiv“.

In der Mathematik ist man nicht damit zufrieden, Eigenschaften bestimmter Objekte bzw. bestimmte Zusammenhänge zu erkennen, sondern man will die Allgemeingültigkeit beweisen. Auf die verschiedenen gängigen Beweisverfahren wie „direkter Beweis“, „indirekter Beweis“, „Widerspruchsbeweis“ und „Induktionsbeweis“gehen wir bei Gelegenheit ein.

Literatur

Appell, K., Appell, J.: Mengen - Zahlen - Zahlbereiche. Berlin 2005.
Ebbinghaus et al.: Zahlen, Springer 1988.
Kirsch, A.: Mathematik wirklich verstehen. Aulis Köln 1987
Kirsch, A.:Elementare Zahlen- und Größenbereiche. Vandenhoeck & Ruprecht 1970.
Kramer: Zahlen für Einsteiger. Vieweg 2008.
Krömer,R.: Aufbau des Zahlensystems und Funktionenlehre, Vorlesung 2013, Siegen.
Messerle: Zahlbereichserweiterungen. Teubner 1975.
Müller: Arithmetik als Prozess. 2004.
Padberg, F.,Danckwerts, R., Stein, M.: Zahlbereiche. Spektrum, Berlin 2001.
Reiss, Chr., Schmieder: Basiswissen Zahlentheorie. Springer 2005/07.
Scheid,H., Schwarz,W.: Elemente der Arithmetik und Algebra. Springer 2016.
Strehl, R.: Zahlbereiche. Herder 1972.

1 Grundlagen

1.1 Der Mengenbegriff, Schreibweisen, Spezielle Mengen

Der Begriff **Menge** geht auf Bolzano (1781-1848) und G.Cantor (1845-1918) zurück.

Nach Cantor ist eine Menge die Zusammenfassung bestimmter, wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens zu einem Ganzen. Die Objekte der Menge heißen **Elemente** der Menge.

Weder der Begriff „Menge“ noch der Begriff „Element“ werden im mathematischen Sinn definiert; sie werden auch nicht durch Axiome definiert. (Ein spezieller Zweig der Mathematik befasst sich mit der axiomatischen Mengenlehre, die auf den Zermelo-Fraenkel-Axiomen, Neumann-Bernays-Gödel-Axiomen oder anderen Axiomensystemen aufbaut.)

Wir haben ein natürliches, intuitiv richtiges Verständnis für Mengen; allerdings führen Konstruktionen wie „die Menge aller Mengen, die sich nicht selbst als Element enthalten“ zu einem Widerspruch, der Russell' schen Antinomie. Gleiches gilt für „die Menge aller Mengen“. Mit Hilfe der Cantorschen „naiven Mengenlehre“ oder - besser gesagt - der mengentheoretischen Sprechweise lassen sich mathematische Zusammenhänge klar und relativ kurz beschreiben.

Endliche Mengen können (insbesondere wenn sie relativ wenig Elemente haben) durch Aufzählen ihrer Elemente angegeben werden:

$$M = \{blau, gelb, rot\} \qquad \text{oder} \quad M = \{Max, Moritz, WitweBolte\}.$$

Dabei kommt es vereinbarungsgemäß nicht auf eine Reihenfolge an oder darauf, ob ein Element mehr als einmal genannt wird. Die Mengen

$$\{blau, rot, gelb\}, \qquad \{blau, gelb, rot\}, \qquad \{blau, blau, gelb, rot\}$$

werden als gleich angesehen.

Mengen mit sehr vielen oder sogar unendlich vielen Elementen beschreibt man durch die Eigenschaft, die die Elemente dieser Menge charakterisiert:

$$\{x; x \text{ ist Einwohner Chinas}\} \quad \text{oder} \quad \{x; x \text{ ist Vielfaches von 3 und kleiner als 1000}\}.$$

Für Mengen wie der aus dem letzten Beispiel benutzt man auch die aufzählende Schreibweise mit Auslassungspunkten

$$\{3, 6, 9, 12, \ldots, 996, 999\},$$

aber nur, wenn das Bildungsgesetz aus den angeführten Beispielen oder aus dem Zusammenhang klar ersichtlich ist.

Will man ausdrücken, dass ein Objekt x Element einer Menge M ist, dann schreibt man $x \in M$. Ist x nicht Element von M, dann schreibt man $x \notin M$.

„Die“ Menge, die gar keine Elemente hat, heißt **leere Menge**. Schreibweise: $\emptyset$.

Zwei Mengen M, N heißen **gleich** (in Zeichen $M = N$), wenn sie dieselben Elemente haben. In mengentheoretischer Sprechweise drückt man das so aus:

Die Mengen M und N sind gleich genau dann, wenn gilt: Für alle x gilt: $(x \in M) \quad \Leftrightarrow \quad (x \in N)$.

Ist jedes Element x einer Menge M auch Element der Menge N, dann heißt M **Teilmenge** von N und umgekehrt heißt N **Obermenge** von M. Schreibweise:

$$M \subseteqq N \quad \Longleftrightarrow \quad \text{Für alle } x \in M \text{ gilt } x \in N.$$

Insbesondere ist also auch jede Menge M Teilmenge von sich selbst und die leere Menge ist Teilmenge jeder Menge:

$$\emptyset \subseteqq M \subseteqq M$$

M heißt **echte Teilmenge** von N (bzw. N **echte Obermenge** von M), wenn M Teilmenge von N, aber von N verschieden ist. Jedes Element von M ist also auch Element von N, aber es gibt (mindestens) ein Element in N, das nicht in M enthalten ist. Schreibweise: $M \subsetneqq N$.

Sei M eine beliebige Menge. Die Menge, deren Elemente die Teilmengen von M sind, heißt **Potenzmenge** von M. Schreibweise: $\mathcal{P}(M)$.

Die Potenzmenge von M enthält immer die leere Menge und die Menge M.

Speziell ist $\mathcal{P}(\emptyset) = \{\emptyset\}$, also eine einelementige Menge. Die Potenzmenge einer einelementigen Menge $\{x\}$ ist $\mathcal{P}(\{x\}) = \{\emptyset, \{x\}\}$, enthält also zwei Elemente.

Allgemein gilt: Besitzt M genau n Elemente, so hat $\mathcal{P}(M)$ 2^n Elemente.

Neue Mengen kann man auch durch „Mengenoperationen“ bilden:

(a) Die **Vereinigung** der Mengen M und N ist die Menge

$$M \cup N := \{x;\ x \in M \text{ oder } x \in N\}.$$

(b) Der **Durchschnitt** der Mengen M und N ist die Menge

$$M \cap N := \{x;\ x \in M \text{ und } x \in N\}.$$

(c) Die **Differenz** der Mengen M und N ist die Menge

$$M \setminus N := \{x;\ x \in M \text{ und } x \notin N\}.$$

(d) Das **(kartesische) Produkt** der Mengen M und N ist die Menge

$$M \times N := \{(x, y);\ x \in M \text{ und } y \in N\}.$$

Hier ist speziell die Reihenfolge der Objekte in (x, y) zu beachten.

Bemerkungen:

(1) Mengen ohne gemeinsame Elemente heißen **elementfremd** oder **disjunkt**. Ihr Durchschnitt ist die leere Menge.

(2) Die Vereinigungs- und Durchschnittsbildung kann auch auf beliebig viele Mengen ausgedehnt werden.

(3) Ist $M \subseteqq N$, dann heißt die Differenz $N \setminus M$ auch **Komplement** von M in N.

Dieser Begriff wird vor allem dann verwendet, wenn N eine Grundmenge ist, die alle in einer bestimmten Untersuchung in Frage stehenden Mengen umfasst. $N \setminus M$ heißt dann einfach das Komplement von M. Schreibweise: $\overline{M}$.

(4) Das kartesische Produkt $M \times N$ hat eine andere Gestalt als die Grundmengen M und N. Es besteht aus geordneten Paaren.

Das kartesische Produkt lässt sich auch für endlich viele Mengen $M_1, M_2, \ldots, M_n$ definieren durch

$$M_1 \times M_2 \times \ldots \times M_n := \{(x_1, x_2, \ldots, x_n);\ x_i \in M_i,\ 1 \le i \le n\}.$$

Beispiele: Wir betrachten die Mengen $X = \{1, 2, 3\}$, $M = \{1, 2\}$ und $N = \{1, 3\}$. Dann gilt:

$$2 \in M, \qquad 2 \notin N, \qquad M \subsetneqq X, \qquad N \subsetneqq X, \qquad X \subseteqq X, \qquad M \nsubseteqq N,$$
$$M \cap N = \{1\}, \qquad M \cup N = X, \qquad M \cup X = X, \qquad M \cap X = M.$$
$$M \setminus N = \{2\}, \qquad N \setminus M = \{3\}, \qquad X \setminus M = \{3\}, \qquad M \setminus X = \emptyset.$$

Für die Komplemente bezüglich X gilt

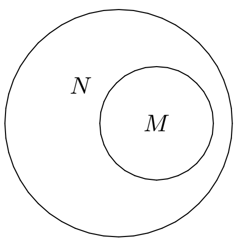
$$\overline{M} = \{3\}, \qquad \overline{N} = \{2\}, \qquad \overline{X} = \emptyset, \qquad \overline{\emptyset} = X.$$

Die Potenzmengen der drei Mengen sind

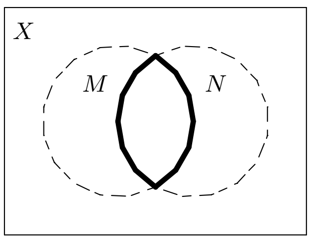
$\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$, $\mathcal{P}(N) = \{\emptyset, \{1\}, \{3\}, N\}$, $\mathcal{P}(X) = \{\emptyset, M \cap N, \overline{N}, N \setminus M, M, N, \{2, 3\}, M \cup N\}$.

$M \times N = \{(1, 1), (1, 3), (2, 1), (2, 3)\}$, $M \times \{1\} = \{(1, 1), (2, 1)\}$, $M \times M = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$.

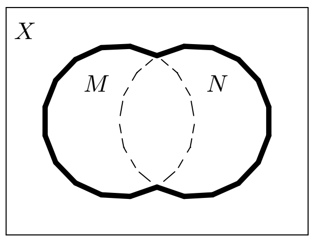
Eine Möglichkeit, Beziehungen zwischen Mengen grafisch darzustellen, sind Venn-Diagramme:



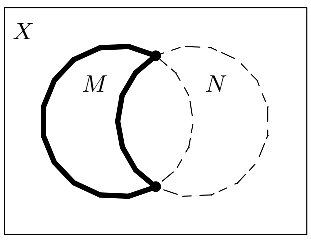
$M \subsetneqq N$



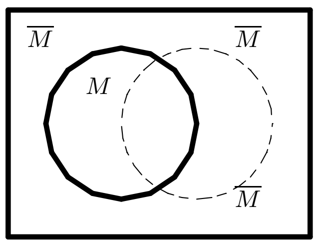
$M \cap N$



$M \cup N$



$M \setminus N$



$\overline{M}$

1.2 Entwicklung des Zahlbegriffs

In der Antike (speziell in der griechischen Mathematik) verstand man unter **Zahl** stets eine natürliche Zahl größer als 1, also eine der Zahlen $2, 3, 4, \ldots$, aufbauend auf der 1 als **Einheit**: Eine Zahl ist „die aus Einheiten zusammengesetzte Menge“ (Euklid).

„Wie eine Maßeinheit der Anfang und die Grundlage des Messens, aber selbst kein Maß ist, so ist die Eins die Grundlage des Zählens, der Ursprung der Zahl, aber selbst keine Zahl“ (Aristoteles).

Allgemein betrachtete man **Größen**: „Die Größe ist teils diskret, teils kontinuierlich und besteht teils aus Teilen, die eine Lage zueinander haben, teils aus Teilen, die keine Lage haben. Diskret ist die Zahl und die Rede, kontinuierlich die Linie, die Fläche, der Körper, außerdem noch die Zeit und der Ort“ (Aristoteles).

Brüche betrachteten die antiken griechischen Mathematiker nicht als Zahlen, sondern als Verhältnisse natürlicher Zahlen, z.B. in der Musiklehre. Irrationale Zahlen betrachteten sie als Verhältnisse von Größen z.B. in der Geometrie.

Die Null und die negativen Zahlen (seit dem 6. Jahrhundert in Indien im Gebrauch) und die komplexen Zahlen (um 1545 erstmals von Cardano zum Lösen quadratischer Gleichungen eingesetzt) waren noch lange nach ihrem Auftreten umstritten.

Erst im 17. Jahrhundert veränderte sich der Zahlbegriff allgemein: Man kam zu der Erkenntnis: „Zahl ist etwas, das sich zu Eins verhält wie eine beliebige Strecke zu einer gegebenen Strecke.“ Und im Laufe des 19. Jahrhunderts wurde der heute geläufige Aufbau entwickelt: Zahlen gelten fortan als Elemente von Mengen, auf denen bestimmte Operationen durchführbar sind.

Wegen der besonderen Bedeutung der verschiedenen Zahlmengen in der Mathematik haben sich spezielle Bezeichnungen durchgesetzt.

(1) Mit
$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$
bezeichnet man die Menge der natürlichen Zahlen, und mit
$$\mathbb{N}_0 = \{0, 1, 2, 3, 4, \ldots\}$$
die Menge der natürlichen Zahlen einschließlich Null.

(2) Mit
$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$
bezeichnet man die Menge der ganzen Zahlen.

(3) Mit
$$\mathbb{Q} = \{\frac{p}{q};\ p \in \mathbb{Z},\ q \in \mathbb{N}\}$$
bezeichnet man die Menge der rationalen Zahlen, und mit
$$\mathbb{Q}^+ = \{\frac{p}{q};\ p, q \in \mathbb{N}\}$$
die Menge der positiven rationalen Zahlen.

(4) Mit
$$\mathbb{R} = \{\text{alle Punkte der Zahlengeraden}\} = \{\text{alle Dezimalbrüche}\}$$
bezeichnet man die Menge der reellen Zahlen.

(5) Mit
$$\mathbb{C} = \{a + b\sqrt{-1};\ a, b \in \mathbb{R}\}$$
bezeichnet man die Menge der komplexen Zahlen.

1.3 Funktionen

Funktionen spielen in der Mathematik und auch der Schulmathematik eine wichtige Rolle. Z.B. werden Gleichungen häufig als Funktionsgleichungen und entsprechend Lösungsmengen als Graphen, Nullstellenmengen oder Schnittmengen mehrerer Graphen usw. interpretiert.

Definition 1.3.1 *Wir betrachten zwei Mengen M und N.*

(a) Eine Teilmenge f des kartesischen Produkts $M \times N$ heißt **Funktion** *von M nach N , wenn es zu jedem $x \in M$ genau ein $y \in N$ gibt mit $(x, y) \in f$. Schreibweise: $f : M \to N$.*

(b) Für $(x, y) \in f$ heißt y **Wert** *der Funktion für x und umgekehrt x* **Urbild** *von y. Schreibweise: $y = f(x)$.*

(c) M heißt **Definitionsmenge** *und N* **Wertebereich**.

Beispiele 1.3.2

(1) Beim freien Fall hängt der Weg s, den ein Körper (bei Vernachlässigung der Reibung) zurücklegt, von der Fallzeit t ab. Die Abhängigkeit wird beschrieben durch die Funktion $s = s(t) = \frac{1}{2}gt^2$ (mit Erdbeschleunigung g).

(2) Der Druck p eines Gases ist abhängig von seinem Volumen V und seiner Temperatur T: $p = p(V, T) = \frac{c \cdot T}{V}$ (mit Materialkonstanten c).

(3) Der Preis einer Theater- oder Konzertkarte hängt i.a. von der Sitzreihe ab. Diese Abhängigkeit wird durch z.B. eine Preistabelle beschrieben:

Reihe	1 bis 5	6 bis 10	11 bis 20	21 bis 30
Preis in Euro	35	28	20	13

(4) Das Porto eines Briefes innerhalb Deutschlands hängt vom Gewicht (und der Größe) des Briefes ab. Ist P das Porto in Euro, G das Gewicht in Gramm, dann gilt zur Zeit

$$P = P(G) = \begin{cases} 0,70 & \text{falls } 0 < G \leq 20 \\ 0,85 & \text{falls } 20 < G \leq 50 \\ 1,45 & \text{falls } 50 < G \leq 500 \\ 2,60 & \text{falls } 500 < G \leq 1000 \end{cases}$$

(5) Die Anzahl X der Permutationen (Vertauschungen) von n verschiedenen Objekten hängt von ihrer Zahl n ab: $X = X(n) = n!$

(6) Die Länge l eines Intervalls $[a, b]$ auf der reellen Zahlengeraden hängt von den Intervallenden ab: $l = l(a, b) = b - a$.

Gemeinsam ist allen diesen Beispielen, dass es eine gewisse Menge M gibt (die möglichen Fallzeiten, Paare aus Volumen und Temperatur, Reihen, Briefgewichte, Anzahlen bzw. Paaren von Intervallenden), und zu jedem $x \in M$ lässt sich in **eindeutiger Weise** ein Element y aus einer zweiten Menge N bestimmen.

In der Schulmathematik betrachtet man meist Funktionen mit einer reellen Variablen.
Die Lösungsmenge aller algebraischen Gleichungen, die man eindeutig nach einer der Unbekannten, z.B. y, auflösen kann, definiert eine Funktion. Zum Beispiel kann man die Gleichung

$$y - x^2 = 0$$

eindeutig nach y auflösen, und sie definiert die Funktion

$$y = y(x) = x^2$$

(der Graph ist die „Normalparabel").

Dagegen definiert die Gleichung

$$y^2 + x^2 = 1$$

keine Funktion, denn man kann sie nicht eindeutig nach y auflösen. Trotzdem kann man die Lösungsmenge graphisch darstellen, und zwar als Kurve (in diesem Fall ist das der Einheitskreis).

Als „Faustregel" gilt: Betrachtet man eine Gleichung mit zwei Unbekannten x und y und stellt die Menge der Lösungen $(x|y)$ in einem kartesischen Koordinatensystem grafisch dar, und schneidet mindestens eine Parallele zur y-Achse den „Graph" mehr als einmal, dann handelt es sich nicht um einen Funktionsgraphen.

Die Funktions-Definition erfüllt aber auch z.B. die **Dirichlet-Funktion**

$$y = \begin{cases} 0 & \text{für } x \in \mathbb{Q} \\ 1 & \text{für } x \in \mathbb{R} \setminus \mathbb{Q} \end{cases} .$$

Die Zuordnungsvorschrift liefert eine Funktion von $\mathbb{R}$ nach $\mathbb{R}$ (jedem x wird genau ein y zugeordnet), die aber grafisch nicht in gewohnter Weise darstellbar ist.

Die Definition der Funktion ist so allgemein, dass es sinnvoll ist, Funktionen mit besonderen Eigenschaften gesondert zu betrachten.

Definition 1.3.3 *Es seien M und N Mengen, $f : M \to N$ eine Funktion.*

(a) Sind zu je zwei verschiedenen $x_1, x_2 \in M$ die Funktionswerte auch verschieden, d.h. gilt

$$x_1 \neq x_2 \qquad \Rightarrow \qquad f(x_1) \neq f(x_2)$$

bzw.

$$f(x_1) = f(x_2) \qquad \Rightarrow \qquad x_1 = x_2,$$

dann heißt die Funktion f **injektiv**.

(b) Gibt es zu jedem $y \in N$ ein $x \in M$ mit $y = f(x)$, dann heißt die Funktion f **surjektiv**.

(c) Ist f sowohl injektiv als auch surjektiv, dann heißt f **bijektiv**.

Bemerkungen und Beispiele 1.3.4

(1) Eine Funktion $f : M \to N$ ist injektiv genau dann, wenn es zu jedem $y \in N$ höchstens ein $x \in M$ gibt mit $f(x) = y$.
Durch Verkleinern der Definitionsmenge (man wählt zu jedem Funktionswert y nur ein Urbild x aus und entfernt die anderen Urbilder von y aus M) erhält man zu jeder Funktion $f : M \to N$ eine injektive Funktion $f_1 : M_1 \to N$ mit gleicher Zuordnungsvorschrift.

(2) Die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^2$ ist nicht injektiv, die Funktion $f_1 : \mathbb{R}_0^+ \to \mathbb{R}$ mit derselben Zuordnungsvorschrift ist injektiv.

(3) Eine Funktion $f : M \to N$ ist surjektiv genau dann, wenn jedes $y \in N$ Funktionswert ist.
Durch Verkleinern der Wertemenge (man wählt nur die Funktionswerte aus) erhält man zu jeder Funktion $f : M \to N$ eine surjektive Funktion $f_2 : M \to N_2$ mit gleicher Zuordnungsvorschrift.

(4) Die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^2$ ist nicht surjektiv, die Funktion $f_2 : \mathbb{R} \to \mathbb{R}_0^+$ mit derselben Zuordnungsvorschrift ist surjektiv.

(5) Ist $f : M \to N$ bijektiv, dann gibt es eine Funktion $g : N \to M$, die jedem $y \in N$ das zugehörige Urbild $x \in M$ mit $y = f(x)$ zuordnet, d.h. für die gilt

$$g\big(f(x)\big) = x.$$

g heißt **Umkehrfunktion** von f.
Beispiel: $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = 2x$ hat die Umkehrfunktion $g : \mathbb{R} \to \mathbb{R}$ mit $g(y) = \frac{1}{2}\,y$.

1.4 Relationen

Zwischen 2 Elementen einer Menge können Beziehungen bestehen, die man in der Mathematik durch „Relationen“ ausdrückt.

Zum Beispiel kann man aus der Menge der Besucher einer Disco an einem festen Tag Paare der Besucher bilden, die miteinander getanzt haben. Das kann auch die Situation einschließen, dass jemand allein, also mit sich getanzt hat. Wir betrachten also eine geeignete Teilmenge des kartesischen Produkts $M \times M$ einer festen Menge mit sich.

Definition 1.4.1 *Sei M eine nichtleere Menge. $R \subset M \times M$ heißt* **Relation auf** *M. Für $a, b \in M$ mit $(a, b) \in R$ schreibt man auch $a \sim b$.*

Bemerkung 1.4.2 *Funktionen f der Form $f : M \to M$ sind Relationen, allerdings mit der zusätzlichen Einschränkung, dass es keine 2 Paare der Form $(a, b_1), (a, b_2)$ mit $b_1 \neq b_2$ in der Relation geben darf.*

Die Elemente einer Menge werden oft sortiert (nach Größe, Gewicht, Bedeutung usw.). Ist das möglich, dann kann man die entsprechenden Beziehungen durch eine **Ordnungsrelation** beschreiben:

Definition 1.4.3 *Sei M eine nichtleere Menge, R eine Relation auf. Ist R transitiv, d.h. gilt für alle $a, b, c \in M$*

$$a \sim b \text{ und } b \sim c \qquad \Rightarrow \qquad a \sim c \qquad\qquad \textbf{(Transitivität)}\ ,$$

dann heißt R **Ordnungsrelation**.

Bemerkungen und Beispiele 1.4.4

(1) Sei

$$A := \{1, 2\}, \quad B := \{1, 2, 3\}, \quad C := \{2, 3\}, \quad D := \{2, 3, 4\},$$

dann gilt

$$\emptyset \subseteqq A \subseteqq A \subseteqq B \subseteqq \mathbb{N}, \qquad \emptyset \subseteqq C \subseteqq B \subseteqq \mathbb{N}, \qquad C \subseteqq D.$$

„$\subseteqq$“ ist eine Ordnungsrelation für die angegebenen Mengen. Es gilt aber z.B. $B \nsubseteqq D$ und $D \nsubseteqq B$.

(2) Eine Relation auf der nichtleeren Menge M heißt **reflexiv**, wenn für alle $a \in M$ gilt $a \sim a$.

„$\subseteqq$“ ist reflexiv, „$\subsetneqq$“ ist nicht reflexiv.

(3) Die Menge $\mathbb{N}$ der natürlichen Zahlen ist geordnet. Die Relation „$\leq$“ hat ähnliche Eigenschaften wie die Teilmengenbeziehung mit dem Unterschied, dass man zwei beliebige natürliche Zahlen der Größe nach miteinander vergleichen kann. Eine solche Ordnungsrelation nennt man **vollständig**.

Sowohl bei „$\subseteqq$“ als auch bei „$\leq$“ gilt:

$$\text{Aus} \quad a \sim b \qquad \text{und} \qquad b \sim a \qquad \text{folgt} \qquad a = b.$$

Diese Eigenschaft heißt **Antisymmetrie**.

Ist eine Relation transitiv, reflexiv, antisymmetrisch und vollständig, dann heißt sie **nichtstrenge Ordnung**. Die zugehörige Menge heißt **vollständig geordnet**.

Ist eine Relation transitiv, reflexiv und antisymmetrisch, dann heißt sie **nichtstrenge Halbordnung**.

(4) Die Relationen „$\subsetneqq$“ und „$<$ “ auf $\mathbb{N}$ sind transitiv, aber weder reflexiv noch antisymmetrisch. „$\subsetneqq$“ ist (auf der Potenzmenge von $\mathbb{N}$) nicht vollständig, „$<$ “ ist vollständig. Mit beiden Relationen kann man die Elemente der jeweiligen Menge wiederum ordnen.

An Stelle der Antisymmetrie tritt die **Trichotomie-Eigenschaft**: Für beliebige $a, b \in M$ gilt

$$\text{entweder} \qquad a \sim b \qquad \text{oder} \qquad a = b \qquad \text{oder} \qquad a \sim b.$$

Ist eine Relation transitiv, vollständig und hat die Trichotomie-Eigenschaft, dann heißt sie **strenge Ordnungsrelation**.

„$<$ “ ist also eine strenge Ordnungsrelation, „$\subsetneqq$“ und „$\leq$“ nicht.

(5) Nur auf vollständig geordneten Mengen sind Begriffe wie „kleinstes Element“, „größtes Element“, „untere Schranke“, „obere Schranke“ sinnvoll.

Wenn man bei einem Einkauf mit einer Ein-Euro-Münze bezahlt, ist es dem Kaufmann egal, mit welcher speziellen Münze man bezahlt. Er sieht alle Euro-Münzen als gleichwertig an. Das kann für einen

Münzsammler anders sein - z.B. ist eine finnische 1-Cent-Münze für den Sammler viel mehr wert als eine deutsche 1-Cent-Münze.

Gleichwertigkeit wird in der Mathematik durch den Begriff der Äquivalenzrelation beschrieben. Relationen dieser Art müssen natürlich reflexiv und transitiv sein. Außerdem müssen sie **symmetrisch** sein, d.h.

$$\text{für alle} \quad a, b \in M \quad \text{mit } a \sim b \quad \text{gilt} \qquad b \sim a.$$

Diese drei Eigenschaften charakterisieren die gewünschten Relationen:

Definition 1.4.5 *Sei M eine nichtleere Menge, R eine Relation auf M. Ist R transitiv, reflexiv und symmetrisch, dann heißt R* **Äquivalenzrelation**.

Beispiele 1.4.6

(1) „parallel oder gleich" ist eine Äquivalenzrelation auf der Menge der Geraden der Ebene oder des Raums („parallel" allein ist nicht reflexiv).

(2) „Gleichmächtig" ist eine Äquivalenzrelation auf Klassen von Mengen und verallgemeinert die Beziehung „haben gleich viele Elemente", die nur für endliche Mengen sinnvoll ist.

(3) Zwei Gleichungen sind äquivalent, wenn sie dieselbe Lösungsmenge besitzen. Die meisten Lösungsverfahren beruhen darauf, eine Gleichung oder ein Gleichungssystem durch bestimmte Umformungen in eine äquivalente Gleichung (bzw. ein äquivalentes Gleichungssystem) zu überführen, bei der die Lösungsmenge sofort ersichtlich ist.

(4) Sei M eine beliebige nichtleere Menge von Menschen. „größer als" und „größer oder gleich" sind keine Äquivalenzrelationen auf M.

Durch die Relation „gleicher Zahlungswert" wird auf der Menge aller im Umlauf befindlichen Cent- und Euromünzen bzw. -Scheine eine Äquivalenzrelation festgelegt, die die Menge der Münzen und Scheine vollständig und eindeutig in Teilmengen aufteilt, nämlich die Menge der 1-Cent-Münzen, die Menge der 2-Cent-Münzen usw.

Definition 1.4.7 *Sei M eine Menge. Ist $\sim$ eine Äquivalenzrelation auf M, $a \in M$ beliebig, dann heißt*

$$K_a := \{b \in M;\ a \sim b\}$$

Äquivalenzklasse *von a bezüglich $\sim$.*

Es gilt

Satz 1.4.8 *Ist $\sim$ eine Äquivalenzrelation auf der Menge M, $a \in M$ beliebig, K_a die Äquivalenzklasse von a bezüglich $\sim$, dann gilt*

(a) $\displaystyle\bigcup_{a \in M} K_a = M.$

(b) Zwei Äquivalenzklassen sind entweder disjunkt oder gleich, d.h. es gilt

$$K_a \cap K_b \neq \emptyset \quad \Longleftrightarrow \quad a \sim b \quad \Longleftrightarrow \quad K_a = K_b.$$

Die Äquivalenzrelation „zerlegt" also die Menge M vollständig in disjunkte Teilmengen.

2 Natürliche Zahlen

Die natürlichen Zahlen $1, 2, 3, \ldots$ sind uns so selbstverständlich, dass wir uns nicht vorstellen können, welche kulturelle Leistung der Menschheit die „Erfindung“ oder „Entdeckung“ dieser Zahlen darstellt, vergleichbar mit der Entwicklung der Schrift.

Sie werden im täglichen Leben in vielfältiger Weise benutzt. Mit natürlichen Zahlen bezeichnet man

- Anzahlen: „In dieser Vorlesung sitzen 29 Studenten“, „Max hat noch 4 Euro“, „auf die Fähre passen 250 Autos“ - Kardinalzahl-Aspekt,
- die Reihenfolge: Man nummeriert Seiten eines Buches, Plätze in einer Sitzreihe oder gibt Rangplätze innerhalb einer geordneten Reihe an: „Mittwoch ist der dritte Tag der Woche“, „Silke Meier sitzt in der 8. Reihe“, „Max hat den 2. Platz beim Pokerturnier erreicht“ - Ordinalzahl-Aspekt.
- Man benutzt sie zur Skalierung, d.h. als Maßzahlen auf einer Skala (Lineal, Uhr): „Eine Vorlesung dauert 90 Minuten“, „1 Kilo Kaffee kostet 10 Euro“, „Bei der Klausur hat der Student eine 2 erreicht“.
- Man kodiert Informationen mit ihnen (Telefonnummern, Matrikelnummern): „Siegen-Mitte hat die Postleitzahl 57072“, „mein Girokonto hat die Nummer 134 205 13“, „die PIN-Nummer meiner EC-Karte ist 4711“.
- Man benutzt sie als Operatoren: „die Vorlesung findet zweimal pro Woche statt“, „die Tabletten sind dreimal täglich einzunehmen“, „eine Zehnerkarte ist in der Regel günstiger als eine Einzelkarte“.

Außerdem rechnet man mit ihnen.

Wir benutzen und bezeichnen die natürlichen Zahlen unabhängig vom Zusammenhang und den Gegenständen, mit denen sie zusammen auftreten. Das ist nicht selbstverständlich, wie Untersuchungen alt-babylonischer Texte (ca 3.500 - 3000 v.Chr.) zeigen, wo jeweils vom gewählten Objekt abhängige Zahlzeichen verwendet wurden (s. z.B. Padberg,Danckwerts,Stein, I1). Auch in unserer Umgangssprache sind Reste solcher Kopplungen vorhanden. Z.B. spricht man von einem Dutzend Eier, aber nicht von einem Dutzend Euro.

2.1 Die natürlichen Zahlen als Ordinalzahlen

Schon Kinder im Vorschulalter kennen meist die natürlichen Zahlen (zumindest in einem Ausschnitt) als **Zählreihe**.

Begonnen wird mit der Eins, und durch das Zählen ordnet man jeder genannten Zahl eine nächste zu. Diese neue Zahl (der Nachfolger) ist eindeutig bestimmt und die Anfangszahl Eins sowie alle schon verwendeten Zahlen treten beim Zählen nie wieder auf. Weiter ist festgelegt, dass man durch hinreichend langes Zählen jede natürliche Zahl erreicht.

Man kann sich die natürlichen Zahlen als (unendlich viele) Perlen vorstellen, die auf einer hinreichend langen Schnur aufgefädelt sind. Den Übergang zur Nachfolgerzahl beim Zählen kennzeichnen wir durch einen Pfeil, der auf den Nachfolger zeigt.

Die Bedingungen, die wir unbewußt beim Zählen erfüllen, finden sich in folgenden 5 Forderungen wieder:

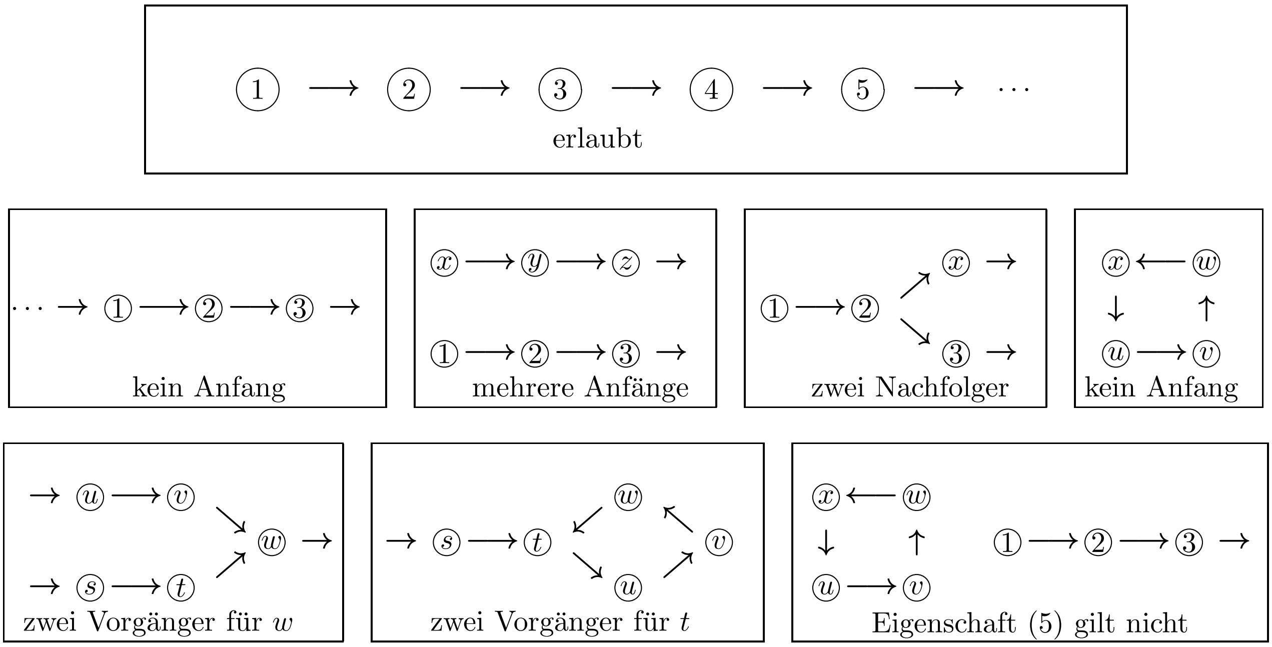
(1) Von jeder Perle geht genau ein Pfeil aus – die Schnur verzweigt sich nicht.

(2) Auf die Eins darf kein Pfeil zeigen, d.h. die Eins ist die Anfangszahl.

(3) Auf keine Perle dürfen zwei Pfeile zeigen – das schließt Kreise aus.

(4) Auf jede Perle, die von Eins verschieden ist, zeigt ein Pfeil, d.h. es gibt nur eine Anfangszahl.

(5) Die Anordnung darf keine echte Teilmenge enthalten, die die Eins und mit jeder Perle auch ihren Nachfolger enthält.



Im **Peanoschen Axiomensystem** werden diese Eigenschaften mengentheoretisch formuliert:

Definition 2.1.1 *Gelten für eine Menge* $\mathbb{N}$ *und eine Funktion* $f : \mathbb{N} \to \mathbb{N}$ *folgende Eigenschaften:*

P1: $1 \in \mathbb{N}$*, d.h. die Eins ist eine natürliche Zahl,*

P2: Für alle $x \in \mathbb{N}$ *gilt* $f(x) \neq 1$*, d.h. die Eins ist kein Nachfolger irgendeiner natürlichen Zahl,*

P3: Für alle $x, y \in \mathbb{N}$ *mit* $x \neq y$ *gilt* $f(x) \neq f(y)$*, d.h. verschiedene Zahlen haben verschiedene Nachfolger,*

P4: Enthält eine Teilmenge $T \subset \mathbb{N}$ *das Element* 1 *und mit jedem* $x \in T$ *auch* $f(x)$*, dann ist* $T = \mathbb{N}$*,*

dann heißt $\mathbb{N}$ **Menge der natürlichen Zahlen**.

Bemerkung 2.1.2 In der Definition wird weder gesagt, dass eine solche Menge existiert, noch, dass es nur eine solche gibt. Intuitiv wissen wir, dass es solche Mengen gibt, z.B. die Menge der entsprechenden deutschen Zahlwörter „eins, zwei, drei, vier, $\cdots$“, der englischen Zahlwörter „one, two, three, four, $\cdots$“, der arabischen Zahlzeichen „$1, 2, 3, 4, \cdots$“ oder der römischen Zahlzeichen „$|, ||, |||, |V, V, X, \cdots$“. Wir identifizieren zwar diese Mengen, aber eigentlich sind es verschiedene Mengen.

Das Axiom P4 heißt **Induktionsaxiom** und ist eng verknüpft mit dem

Axiom 2.1.3 (Beweisprinzip der vollständigen Induktion) *Sei $A(n)$ eine Aussageform über der Grundmenge $\mathbb{N}$. Gilt*

- *$A(1)$ ist wahr* (**Induktionsanfang**),
- *für jede natürliche Zahl n, für die $A(n)$ wahr ist, ist auch $A(n+1)$ wahr* (**Induktionsschritt**),

dann ist $A(n)$ für alle $n \in \mathbb{N}$ wahr.

Bemerkungen 2.1.4 (1) Das Verfahren der vollständigen Induktion ist ein mathematisch strenges Beweisverfahren im Gegensatz zu den üblichen Induktionsschlüssen aus der Naturwissenschaft, bei denen man aus gemachten Beobachtungen auf zukünftige Ergebnisse schließt (Beispiel: Jeden Morgen geht die Sonne auf. Ein Stein fällt immer von oben nach unten).

(2) Ein Beweis mit Hilfe vollständiger Induktion besteht immer aus den beiden Teilen: Induktionsanfang und Induktionsschritt.
Die Notwendigkeit des Induktionsanfangs erkennt man am Beispiel der (falschen) Behauptung

2 teilt jede ungerade natürliche Zahl.

Da für jede durch 2 teilbare natürliche Zahl x auch $x+2$ durch 2 teilbar ist, wäre die Behauptung richtig, wenn 1 durch 2 teilbar wäre.
Und es reicht nicht aus, den Induktionsschritt durch Überprüfung endlich vieler Beispiele zu ersetzen: Die Behauptung:

Für jede natürliche Zahl $n \in \mathbb{N}$ ist $n^2 - n + 41$ Primzahl

ist für $1 \leq n \leq 40$ wahr, aber für $n = 41$ falsch.

(3) Der Induktionsanfang ist nicht auf $n = 1$ festgelegt.
Die Behauptung

Für jede natürliche Zahl $n \in \mathbb{N}$ gilt $n^2 < 2^n$

ist falsch für $n = 2, 3, 4$, gilt aber für alle anderen natürlichen Zahlen. Der Induktionsanfang ist dann für $n = 5$ zu zeigen und der Induktionsschritt für $n \geq 5$.

(4) Seien A und B zwei Aussagen, deren Richtigkeit wir beweisen wollen. Weiter sei A die schärfere Aussage, d.h. aus A folgt B, und wenn wir A bewiesen haben, ist auch die Richtigkeit von B gezeigt. Im allgemeinen wird damit der Beweis von A schwieriger oder aufwendiger sein als der Beweis von B.

Für Induktionsbeweise ist das nicht unbedingt richtig: Es kann sogar leichter sein, die schärfere Aussage zu beweisen, denn im Induktionsschritt wird ja die Gültigkeit der schärferen Aussage für alle kleineren natürlichen Zahlen (und damit eine stärkere Aussage für diese Werte) vorausgesetzt.

Beispiele 2.1.5 (1) Für alle $n \in \mathbb{N}$ gilt

$$\sum_{i=1}^{n} i := 1 + 2 + 3 + \ldots + n = \frac{n \cdot (n+1)}{2}.$$

(2) Für alle $n \in \mathbb{N}$ gilt: Die Summe der ersten n ungeraden natürlichen Zahlen ist gleich n^2.

(3) Das Quadrat jeder ungeraden natürlichen Zahl lässt bei Division durch 8 den Rest 1.

(4) Die Aussage

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdot + \frac{1}{(2n-1) \cdot (2n+1)} = \frac{1}{2} - \frac{1}{2 \cdot (2n+1)} \qquad \text{für alle } n \in \mathbb{N}$$

lässt sich mit Hilfe vollständiger Induktion beweisen, aber nicht die schwächere Aussage

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdot + \frac{1}{(2n-1) \cdot (2n+1)} < \frac{1}{2} \qquad \text{für alle } n \in \mathbb{N}.$$

Bemerkung 2.1.6 Alle diese Behauptungen lassen sich auch ohne das Prinzip der vollständigen Induktion beweisen. Der Vorteil dieses Beweisverfahrens ist unter anderem seine standardisierte Form.

Beim Vergleich der Peano-Axiome mit den Forderungen, die wir für das Perlenketten-Modell aufgestellt haben, findet man keine direkte Entsprechung der 4. Forderung zu einem der Axiome. Mit Hilfe der vollständigen Induktion zeigt man aber leicht

Satz 2.1.7 *Jede natürliche Zahl $n \neq 1$ hat einen Vorgänger (d.h. ist Nachfolger einer anderen natürlichen Zahl).*

Ähnlich einfach folgt aus den Peano-Axiomen die (eigentlich selbstverständliche) Aussage, dass keine natürliche Zahl gleich ihrem Nachfolger ist.

Satz 2.1.8 *Für alle $n \in \mathbb{N}$ gilt $f(n) \neq n$.*

Wir sind es gewohnt, zwei (natürliche, rationale, reelle) Zahlen x und y zu addieren, zu multiplizieren und der Größe nach miteinander zu vergleichen. Man erhält dann die Summe $x + y$ und das Produkt $x \cdot y$, die beide wieder Elemente aus der jeweiligen Zahlenmenge sind, bzw. die Aussage $x < y$, die wahr oder falsch ist. Doch wie kann man diese Operationen bzw. die Kleiner-Relation mit Hilfe des Zählens definieren?

Betrachtet man die natürlichen Zahlen als Ordinalzahlen, dann bedeutet $x < y$, dass die Zahl x beim Zählen vor der Zahl y auftritt. Ebenso kann man Summe und Produkt mit Hilfe der Zählreihe definieren:

Die Summe $x + y$ erhält man, indem man, ausgehend von der Zahl x, y Schritte weiterzählt. Z.B. ist die Summe $7 + 4$ die Zahl, die 4 Plätze hinter der Zahl 7 steht.

Das Produkt $x \cdot y$ erhält man, indem man statt der Zählreihe $\mathbb{N}$ die x-Reihe betrachtet. Das Produkt $x \cdot y$ ist dann die y-te Zahl dieser Reihe.
Z.B. ist das Produkt $7 \cdot 4$ die 4. Zahl der Siebener-Reihe $7, 14, 21, 28, 35, \ldots$.

In der üblichen mathematischen Formulierung lauten diese Definitionen:

Definition 2.1.9 *Gegeben sei die Zählreihe* $\mathbb{N}$ *und die zugehörige Nachfolger-Abbildung* $f : \mathbb{N} \to \mathbb{N}$. *Weiter seien* x *und* y *beliebige natürliche Zahlen.*

(a) Die **Summe** $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *wird definiert durch*

$$x + 1 := f(x); \qquad\qquad x + f(y) := f(x + y).$$

(b) Das **Produkt** $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *wird definiert durch*

$$x \cdot 1 := x; \qquad\qquad x \cdot f(y) := x \cdot y + x.$$

(c) x *heißt kleiner als* y*, wenn es eine natürliche Zahl* z *gibt mit* $x + z = y$*. Schreibweise:* $x < y$*.*

Bemerkungen 2.1.10 (1) Addition und Multiplikation sind rekursiv definiert, d.h. durch die erste Beziehung wird ein Anfangswert definiert, und durch die zweite Beziehung wird jeweils für die Berechnung auf vorher berechnete Werte zurückgegriffen. Sowohl Summe als auch Produkt werden auf die Nachfolger-Abbildung zurückgeführt, und damit folgt ihre Existenz und Eindeutigkeit.

(2) Für den Nachfolger $f(x)$ einer natürlichen Zahl x schreiben wir im folgenden $x + 1$. Trotzdem ist die Zählfunktion f das ursprüngliche. Die Addition baut auf ihr auf, und die Multiplikation wieder auf der Addition.

(3) Für $x < y$ schreibt man auch manchmal $y > x$ (Größer-Relation). Weiter soll $x \leq y$ bedeuten, dass $x = y$ oder $x < y$ gilt (Kleiner-Gleich-Relation).

(4) Addition, Multiplikation und Kleiner-Relation lassen sich sehr gut geometrisch darstellen:
Von einem festen Punkt einer Geraden, den wir vorerst Ursprung nennen wollen, werden in eine Richtung auf der Geraden Punkte gleichen Abstands abgetragen und sukzessive durch die Zahlen $1, 2, 3, \cdots$ benannt. Als Platzgründen stellt man einen solchen „Zahlenstrahl" üblicherweise waagrecht dar. Pädagogisch sinnvoller wäre es, ihn senkrecht darzustellen.

Eine Zahl x ist dann kleiner als die Zahl y, wenn der zu x gehörende Punkt links von bzw. unter dem zu y gehörenden Punkt liegt.
Mit zwei starren gegeneinander beweglichen Zahlenstrahlen kann man einen „Rechenschieber" für die Addition in $\mathbb{N}$ bauen, und mit einem starren Zahlenstrahl und einem Zahlenstrahl aus Gummi einen Rechenschieber für die Multiplikation.

Es gelten die bekannten Rechenregeln, wobei vor allem die Kommutativgesetze nicht selbstverständlich sind, wenn man die Definition von Addition und Multiplikation und die dort vorgenommene Unterscheidung zwischen dem 1. und 2. Summanden bzw. Faktor in Betracht zieht.

Satz 2.1.11 *Für alle natürlichen Zahlen* $x, y, z \in \mathbb{N}$ *gilt*

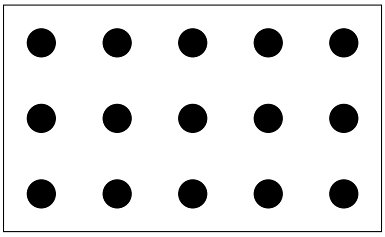
(a) $(x + y) + z = x + (y + z)$ $\quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$ *(Assoziativgesetz)*

(b) $x + y = y + x$ $\quad x \cdot y = y \cdot x$ *(Kommutativgesetz)*

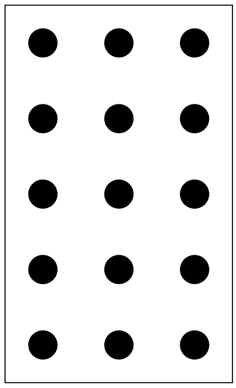
(c) $x \cdot 1 = 1 \cdot x = x$ *(neutrales Element bzgl. der Multiplikation)*

(d) $(x + y) \cdot z = x \cdot z + y \cdot z$ *(Distributivgesetz)*

Bemerkung 2.1.12 Die Gültigkeit des Kommutativgesetzes für die Multiplikation kann man geometrisch verdeutlichen: Die Zahl $x \cdot y$ kann man durch eine Anzahl von Punkten darstellen, die in einem rechteckigen Schema mit y Spalten zu je x Kugeln angeordnet sind. Analog entspricht die Zahl $y \cdot x$ einem Rechteck mit x Spalten und y Zeilen. Da die Rechtecke z.B. durch eine Drehung um 90^0 (und eventuell eine Verschiebung) ineinander überführt werden können, enthalten sie offensichtlich dieselbe Anzahl von Kugeln.



y Spalten a x Kugeln



x Spalten a y Kugeln

Um eine lineare Gleichung wie
$$3x + 2 = 11$$
nach der Unbekannten x auflösen zu können, muss man die Addition bzw. Multiplikation rückgängig machen können.

Satz 2.1.13 *Für alle natürlichen Zahlen $x, y, z \in \mathbb{N}$ gilt*

(a) $x + z = y + z \Longrightarrow x = y$ $\quad$ $x \cdot z = y \cdot z \Longrightarrow x = y$ $\quad$ *(Rechtseindeutigkeit)*

(b) $z + x = z + y \Longrightarrow x = y$ $\quad$ $z \cdot x = z \cdot y \Longrightarrow x = y$ $\quad$ *(Linkseindeutigkeit)*

Je zwei natürliche Zahlen x und y lassen sich bezüglich der Kleiner-Relation eindeutig vergleichen:

Satz 2.1.14 (Trichotomie) *Für zwei beliebige natürliche Zahlen x und y gilt genau eine der folgenden drei Beziehungen:*
$$x < y, \qquad x = y \quad \text{bzw.} \qquad y < x.$$

Das „Rechnen mit Ungleichungen“ ist in folgendem Satz zusammengefaßt:

Satz 2.1.15 *Für alle $x, y, z \in \mathbb{N}$ gilt*

(a) Aus $x < y$ und $y < z$ folgt $x < z$. *(Transitivität)*

(b) Es gilt $x < y$ genau dann, wenn $x + z < y + z$. *(Monotoniegesetz der Addition)*

(c) Es gilt $x < y$ genau dann, wenn $x \cdot z < y \cdot z$. *(Monotoniegesetz der Multiplikation)*

(d) Aus $x \neq 1$ folgt $1 < x$. *(1 ist die kleinste nat.Zahl)*

(e) $x < x + z$.

Nach dem vorigen Satz hat $\mathbb{N}$ ein kleinstes Element, die 1. Auch nach Entfernen der Eins hat die Restmenge ein kleinstes Element, nämlich 2. Eine für $\mathbb{N}$ typische Eigenschaft ist, dass dies sogar für jede nichtleere Teilmenge von $\mathbb{N}$ gilt. Z.B. für die rationalen Zahlen zwischen 0 und 1 ist dies falsch.

Satz 2.1.16 (Prinzip vom kleinsten Element) *Jede nichtleere Teilmenge von $\mathbb{N}$ hat ein kleinstes Element.*

Das Prinzip vom kleinsten Element ist nicht nur ein Satz, d.h. eine Folgerung aus den Peano-Axiomen, sondern sogar gleichwertig zum Prinzip der vollständigen Induktion. Man könnte also das entsprechende Axiom durch das Prinzip vom kleinsten Element ersetzen, und die Aussage ist damit charakteristisch für die Menge der natürlichen Zahlen. Sie gilt weder für die Menge der ganzen Zahlen noch die Menge der positiven rationalen Zahlen.

Als Anwendung und Folgerung wollen wir zwei Aussagen mit Hilfe von Widerspruchbeweisen zeigen:

Satz 2.1.17 *Es gibt nur interessante natürliche Zahlen.*

Satz 2.1.18 *$\sqrt{2}$ ist keine rationale Zahl, d.h. es gibt keine natürliche Zahl n mit $n \cdot \sqrt{2} \in \mathbb{N}$.*

Ebenfalls äquivalent zum Induktionsaxiom bzw. dem Prinzip vom kleinsten Element ist das Kettenprinzip sowie das Dirichlet'sches Schubfachprinzip:

Satz 2.1.19 (Kettenprinzip) *Jede absteigende Kette natürlicher Zahlen bricht nach endlich vielen Schritten ab.*

Satz 2.1.20 (Dirichlet'sches Schubfachprinzip) *Seien $m, n \in \mathbb{N}$ beliebige Zahlen mit $n < m$. Werden m Elemente (Gegenstände) auf n Mengen (Schubfächer) verteilt, dann enthält mindestens eine der Mengen mehr als eines der Elemente.*

Beispiel 2.1.21 Es sei $\dfrac{p}{q}$ mit $p, q \in \mathbb{N}$ ein Bruch mit endlicher Dezimalbruchentwicklung. Ist n die Zahl der Stellen hinter dem Komma, dann gilt $0 \leq n \leq q - 1$.

2.2 Die natürlichen Zahlen als Kardinalzahlen

Die natürlichen Zahlen sind ein wichtiges Hilfsmittel, um zu bestimmen, wie viele Gegenstände in einer Menge zusammengefaßt sind.

Ist eine Menge M von Gegenständen vorgegeben, dann greift man ein beliebiges Element heraus und gibt ihm die Nummer 1 (z.B. durch Beschriften mit einem Etikett). Enthält die Restmenge weitere Elemente, dann greift man wiederum eines davon heraus und gibt ihm die Nummer 2.
Dieses Verfahren wird solange durchgeführt, bis die Restmenge kein Element mehr enthält, also gleich der leeren Menge ist.
Bricht das Verfahren ab, dann sind zum Schluss die Elemente von M durchnummeriert, d.h. geordnet. Die letzte vergebene natürliche Zahl nennt man **Anzahl der Elemente** oder **Kardinalzahl** von M (Bezeichnung $\operatorname{card} M$).
Natürlich gibt es bei einer Menge mit mehr als einem Element auch mehrere Möglichkeiten, die Elemente durchzunummerieren, und theoretisch könnte sich jedesmal eine andere Elementezahl ergeben.

Wir wollen den oben beschriebenen Vorgang des Durchnummerierens mathematisch genauer beschreiben:

Für die Bestimmung der Elementezahl oder Kardinalzahl n einer Menge M haben wir durch das Durchnummerieren eine eineindeutige Zuordnung, d.h. eine bijektive Funktion, zwischen der Menge M und der Teilmenge $\{1, 2, 3, \ldots, n\} \subset \mathbb{N}$ der natürlichen Zahlen hergestellt. Derartige Teilmengen nennen wir im folgenden **Anfangsstück** von $\mathbb{N}$. Ein Anfangsstück von $\mathbb{N}$ ist also eine Teilmenge von $\mathbb{N}$, die eine größte Zahl n enthält und außerdem alle natürlichen Zahlen kleiner als n.

Mit Hilfe von bijektiven Funktionen kann man bei zwei (endlichen) Mengen ohne Abzählen der Elemente feststellen, ob sie gleich viele Elemente enthalten. Steht z.B. eine Anzahl von Personen in einem Raum und sind dort eine Reihe von Stühlen aufgestellt, dann kann man durch den Befehl „Setzen“ feststellen, ob gleich viele Personen und Stühle vorhanden sind, nämlich wenn anschließend keine Person mehr steht und kein Stuhl frei ist. (Das Kinderspiel „Reise nach Jerusalem“ lebt davon, dass genau ein Stuhl weniger als Personen vorhanden ist.)

Definition 2.2.1 *Sei M eine beliebige Menge. Gibt es ein Anfangsstück $\{1, 2, \ldots, n\}$ von $\mathbb{N}$ und eine bijektive Funktion zwischen M und dem Anfangsstück, dann heißt die Menge M* **endlich** *und*

$$\operatorname{card} M := n$$

Elementezahl oder **Kardinalzahl** *von M.*
Ist M die leere Menge $\emptyset$, dann setzt man $\operatorname{card} M = \operatorname{card} \emptyset := 0$.
Sonst heißt M **unendlich**.

Dem direkten Vergleich zweier Mengen bezüglich ihrer Elementezahl (im Beispiel Stühle und Personen) entspricht

Satz 2.2.2 *Es seien A und B nichtleere endliche Mengen. Dann gilt $\operatorname{card} A = \operatorname{card} B$ genau dann, wenn es eine bijektive Funktion zwischen A und B gibt.*

Bemerkung 2.2.3 Haben zwei Mengen dieselbe Kardinalzahl, dann bedeutet das nicht, dass beide gleich sein müssen, d.h. dieselben Elemente haben. $\operatorname{card} A = \operatorname{card} B$ bedeutet also etwas anderes als $A = B$.
Z.B. ist $\operatorname{card}\{2, 4, 6\} = \operatorname{card}\{3, 4, 29\} = 3$, aber $\{2, 4, 6\}$ und $\{3, 4, 29\}$ sind verschiedene Mengen.

Kennt man die Kardinalzahlen einer Klasse von Mengen, dann kann man durch Konstruktion einer geeigneten bijektiven Funktion die Kardinalzahlen weiterer Mengen bestimmen.

Beispiel 2.2.4 Wie viele symmetrische Konstellationen von 5 Ziffern der Form [0 4 7 4 0] bzw. [3 7 0 7 3] gibt es?
Jede Konstellation ist offensichtlich durch die ersten 3 Ziffern festgelegt. Durch die Vorschrift „Lasse die letzten beiden Ziffern weg“ ordnen wir jeder dieser Konstellationen eineindeutig ein 3-stelliges Zahlwort von 000 bis 999 zu. Diese neue Menge hat die Kardinalzahl 1000, also ist die Kardinalzahl der gesuchten Menge auch 1000.

Bemerkungen 2.2.5 (1) Für unendliche Mengen ist bisher die Kardinalzahl nicht definiert. Mit Hilfe der bijektiven Funktionen ist aber auch dies möglich:

Existiert zwischen zwei beliebigen Mengen eine bijektive Funktion, dann nennt man sie **gleichmächtig**. Dadurch wird ein Äquivalenzrelation definiert, und die entsprechende Äquivalenzklasse heißt **Kardinalzahl**.
Die Kardinalzahl von $\mathbb{N}$ heißt **abzählbar**, und man kann zeigen, dass die Menge der rationalen Zahlen ebenfalls abzählbar ist, die Menge der reellen Zahlen aber nicht (sie ist „überabzählbar").

(2) Für eine unendliche Menge ist charakteristisch, dass sie eine echte Teilmenge besitzt, die zu ihr gleichmächtig ist. Zum Beispiel ist die Menge $\mathbb{G}$ der geraden natürlichen Zahlen eine echte Teilmenge von $\mathbb{N}$ und die Zuordnung von $\mathbb{N}$ nach $\mathbb{G}$ mit $n \to 2n$ eineindeutig.

Für die Kardinalzahlen sind Addition, Multiplikation und Kleiner-Relation mit Hilfe der Mengenoperationen erklärt.

Definition 2.2.6 *Es seien die disjunkten (elementfremden) Mengen A und B gegeben, d.h. es gilt $A \cap B = \emptyset$. Dann heißt*

$$\operatorname{card} A + \operatorname{card} B := \operatorname{card}(A \cup B)$$

Summe *der Kardinalzahlen von A und B.*

Bemerkungen 2.2.7 (1) Für nicht disjunkte Mengen führt die Definition 2.2.6 zu nicht gewollten Ergebnissen, wie man leicht an Beispielen mit endlichen Mengen erkennt:

$$\operatorname{card}\{1,2,3,4\} = 4, \quad \operatorname{card}\{3,4,5,6\} = 4, \quad \operatorname{card}\Big(\{1,2,3,4\} \cup \{3,4,5,6\}\Big) = \{1,2,3,4,5,6\} = 6.$$

(2) Wie man die Addition auf Hinzufügen von neuen Objekten (von Elementen der zur Ausgangsmenge A disjunkten Menge B) zurückführt, kann man durch „Wegnehmen" die **Subtraktion** einführen: Für Mengen A, B mit $A \subset B$ heißt

$$\operatorname{card} B - \operatorname{card} A := \operatorname{card}(B \setminus A) := \operatorname{card}\{x \in B; x \notin A\}$$

Differenz der Kardinalzahlen von B und A.

Definition 2.2.8 *Es sei $m \in \mathbb{N}_0$ und $A_1, A_2, \ldots, A_m$ paarweise disjunkte Mengen mit jeweils n Elementen. Dann heißt*

$$m \cdot n := \operatorname{card}(A_1 \cup A_2 \cup \ldots \cup A_m)$$

Produkt *von m und n.*

Bemerkungen 2.2.9 (1) $m = 0$ bedeutet, dass man keine Menge vorliegen hat. Als Vereinigung betrachtet man dann die leere Menge, d.h. man setzt $0 \cdot n = 0$ für alle $n \in \mathbb{N}$.
Analog bedeutet $m = 1$, dass nur eine Menge mit n Elementen vorliegt, d.h. $1 \cdot n = n$.

(2) „Paarweise disjunkt" ist bei mehr als zwei Mengen eine stärkere Voraussetzung als „disjunkt". Zum Beispiel sind die Mengen $A = \{1,2,3\}$, $B = \{2,3,4\}$, $C = \{1,4,5\}$ disjunkt, aber nicht paarweise disjunkt.

(3) Die Multiplikation kann man nach Definition auffassen als wiederholte Addition von paarweise disjunkten Mengen mit gleicher Kardinalzahl, d.h. es gilt

$$m \cdot n = \underbrace{n + n + \ldots + n}_{m}.$$

Eine andere (äquivalente) Einführung der Multiplikation ist: Für endliche Mengen M, N sei

$$\mathrm{card}\,(M) \cdot \mathrm{card}\,(N) := \mathrm{card}\,(M \times N).$$

Definition 2.2.10 *Es seien A und B Mengen mit $\mathrm{card}\, A = m$, $\mathrm{card}\, B = n$. Gibt es eine bijektive Funktion zwischen A und einer echten Teilmenge $B' \subset B$, $B' \neq B$, dann nennt man m* **kleiner als** *n. Schreibweise $m < n$.*

Bemerkung 2.2.11 Durch die Definition der Kardinalzahl (bijektive Abbildung der Elemente einer Menge auf ein Anfangsstück der Zählreihe) sind Kardinal- und Ordinalzahleigenschaft von $\mathbb{N}$ miteinander verbunden. Man kann leicht zeigen, dass die jeweils verschieden definierten, aber gleich bezeichneten Verknüpfungen *Addition* und *Multiplikation* dieselben Ergebnisse liefern, also übereinstimmen. Dasselbe gilt für die Kleiner-Relation.

In der Definition der Summe von Kardinalzahlen haben wir die Disjunktheit der beteiligten Mengen vorausgesetzt. Allgemein gilt

Satz 2.2.12 *Für beliebige Mengen A, B gilt*

$$\mathrm{card}\,(A \cup B) = \mathrm{card}\, A + \mathrm{card}\, B - \mathrm{card}\,(A \cap B).$$

Beispiel 2.2.13 Jeder Schüler einer Klasse nimmt an einer der AG's Theater oder Werken teil. Die Theater-AG hat 17 Teilnehmer, die Werk-AG 23, und 9 Schüler besuchen beide AG's. Wie viele Schüler sind in der Klasse?
Es gilt

$$\begin{aligned} \mathrm{card}\,(\text{Klasse}) &= \mathrm{card}\,(\text{Theater-AG}) + \mathrm{card}\,(\text{Werk-AG}) - \mathrm{card}\,(\text{Theater-AG + Werk-AG}) \\ &= 17 + 23 - 9 = 31. \end{aligned}$$

Der vorige Satz lässt sich auf mehr als zwei Mengen verallgemeinern:

Satz 2.2.14 (Ein-Ausschließungsprinzip) *Sei $n \in \mathbb{N}$ mit $n > 2$ und $A_1, A_2, \ldots, A_n$ beliebige Mengen. Dann gilt*

$$\begin{aligned} \mathrm{card}\,(A_1 \cup A_2 \cup \ldots \cup A_n) &= \sum_{i=1}^{n} \mathrm{card}\, A_i - \sum_{1 \le i < j \le n} \mathrm{card}\,(A_i \cap A_j) + \sum_{1 \le i < j < k \le n} \mathrm{card}\,(A_i \cap A_j \cap A_k) \\ &\quad - \ldots + (-1)^{n-1} \mathrm{card}\,(A_1 \cap A_2 \cap \ldots \cap A_n). \end{aligned}$$

2.3 Darstellung natürlicher Zahlen

Wir kennen verschiedene schriftliche Bezeichnungen natürlicher Zahlen, z.B. bezeichnen wir mit *vier*, 4 und |||| dieselbe Zahl, ebenso gilt $1\,000\,000 = 10^6$.

Ursprünglich wurden natürliche Zahlen mit Hilfe des **Bündelungsprinzips** dargestellt, das z.B. beim Auszählen von abgegebenen Stimmen nach einem Wahlgang angewendet wird:
Für jede Stimme, das gezählt wird, wird ein Strich (oder ein vergleichbares Zeichen) gemacht. Ist eine bestimmte Anzahl von Strichen erreicht, ersetzt man sie durch ein anderes Zeichen – man fasst die Striche zu einem „Bündel" zusammen.
Mehrere solcher Bündel werden wieder zu einem größeren Bündel zusammengefaßt usw.

Zum Beispiel fasst man bei der Massenbestimmung 500 Gramm zu einem Pfund zusammen, 100 Pfund zu einem Zentner und 20 Zentner zu einer Tonne.

Bekannte Bündelungssysteme sind das antike ägyptische System (3000 v.Chr.) mit einer Zehner-, Hunderter-, Tausender- usw. Bündelung sowie das antike römische System (500 v.Chr.) mit Fünfer-, Zehner- usw. Bündelung und den Zahlzeichen

Einer	Fünfer	Zehner	Fünfziger	Hunderter	Fünfhunderter	Tausender
I	V	X	L	C	D	M

.

Grundlage für das Bündelungsprinzip ist, dass - nach Verständigung darüber, wie viele Gegenstände man jeweils zusammenfaßt, - jede Menge in solche Bündel und eine Restmenge aufgespalten werden kann, und dass bei einer vorgegebenen Anzahl von Elementen man immer dieselbe Anzahl von Bündeln und dieselbe Anzahl von Rest-Gegenständen erhält.

Satz 2.3.1 (Division mit Rest) *Seien $a \in \mathbb{N}_0, b \in \mathbb{N}$. Dann gilt*

(a) Es gibt Zahlen $q, r \in \mathbb{N}_0$, so dass gilt $a = q \cdot b + r$ *und* $r < b$. *(Existenz von q und r)*

(b) Gilt für $q, q', r, r' \in \mathbb{N}_0$

$$a = q \cdot b + r \quad \textit{mit } r < b \quad \textit{und} \quad a = q' \cdot b + r' \quad \textit{mit } r' < b,$$

dann ist $q = q'$ *und* $r = r'$. *(Eindeutigkeit von q und r)*

Bemerkungen 2.3.2 (1) Für $r = 0$ heißt b **Teiler** von a bzw. a **Vielfaches** von b.

(2) Für die Division von a durch b mit Rest schreibt man auch $a : b = q$ Rest r.

$$13 : 4 = 3 \text{ Rest } 1.$$

Die Schreibweise mit dem Gleichheitszeichen ist eigentlich nicht korrekt. Es gilt nämlich auch $7 : 2 = 3$ Rest 1. Mit der Transitivität der Gleichheit würde $13 : 4 = 7 : 2$ folgen.

(3) Der im Beweis von (a) angewandte Algorithmus führt die Division mit Rest auf wiederholte Subtraktion zurück. Dies wird bei (digitalen) Rechnern technisch ausgenutzt.

(4) Zwar kann man sich leicht überlegen, dass der Algorithmus im Beweis für jedes Paar (a, b) dasselbe Ergebnis liefert, d.h. dass q und r eindeutig bestimmt sind. Erst der Eindeutigkeitsbeweis aber sichert, dass auch bei anderen Verfahren zur Darstellung von a als Vielfachem von b plus einem Rest (schriftliche Division, Taschenrechner usw.) sich keine anderen Werte von q und r ergeben.

(5) Probleme des Bündelungsprinzips:

- (i) Bei Vergrößerung der betrachteten Zahlenmenge werden immer neue Symbole für neue Bündel benötigt.
- (ii) Die Bündelschreibweisen sind teilweise nicht eindeutig.
- (iii) Bei großen Zahlen braucht man entweder viele Bündel oder die Bündel sind so groß, dass man die Anzahl der verwendeten Zeichen eines Typs nicht mit einem Blick erfassen kann; man muss sie zählen. Dabei dienen Zahlzeichen doch im Prinzip dazu, das Ergebnis eines Zählakts festzuhalten!

Wir benutzen heutzutage ein Stellenwertsystem auf der Basis 10 mit 10 Zahlzeichen und Zehner-, Hunderter-, Tausender- usw. Bündel. Dabei repräsentiert eine Ziffer in der Zahldarstellung die entsprechende Anzahl von Bündeln, und die Stelle, auf der die Ziffer steht, gibt Auskunft darüber, welche Art von Bündel gemeint ist.

Beispiel:

$$328012 = 2 \text{ Einer } + 1 \text{ Zehner } + 8 \text{ Tausender } + 2 \text{ Zehntausender } + 3 \text{ Hunderttausender } .$$

Das spiegelt sich auch in der sprachlichen Angabe der Zahl wider.

Ein solches Stellenwertsystem wurde schon im antiken Babylon (ab 3000 v.Chr.) entwickelt.
Zahlen wurden im Sexagesimalsystem dargestellt, einem Stellenwertsystem mit Basis 60, mit Ziffern für 1 und 10. Reste dieses Zahlensystems finden sich noch heute in unserer Darstellung von Winkeln ($1° = 60'$, $1' = 60''$) und Uhrzeiten.
Da $60 = 4 \times 3 \times 5$ als Teiler die Zahlen 1, 2, 3, 4, 5, 6, 10, 12, 15, 20 und 30 hat, können wesentlich mehr Brüche als im Dezimalsystem in endlicher Darstellung geschrieben werden, was numerische Berechnungen sehr erleichtert hat. Zahlen wurden wie heute ziffernweise von links nach rechts geschrieben, wobei links die Ziffern mit größerem Stellenwert standen.

Eine Ziffer für die Null kannten die Babylonier nicht. Trat in einer Zahldarstellung eine bestimmte Potenz von 60 nicht auf, dann wurde das Nichtvorhandensein mit einem Leerzeichen dargestellt, was zu mehrdeutigen Interpretationen der Darstellung führen konnte.

Erst mit Einführung der „Zahl“ 0 durch die Inder konnte dies Problem gelöst werden. Sie benutzten unser bekanntes Stellenwertsystem auf der Basis 10. Es wurde durch die Araber um 1000 n.Chr. in den damals von ihnen beherrschten südlichen und westlichen Mittelmeerraum eingeführt und in Italien durch Fibonacci (um 1200 n.Chr.) und im deutschen Sprachraum durch Adam Riese (um 1500 n.Chr.) bekannt gemacht.

Allgemein benutzt ein Stellenwertsystem die Potenzen einer beliebigen festen natürlichen Zahl $b \neq 1$, der **Basis**.

Erhält man bei Division mit Rest einer beliebigen natürlichen Zahl a durch b die Werte q_0 und r_0, dann kann man a eineindeutig durch das Symbol $(q_0 r_0)_b$ darstellen.

Ist $q_0 \geq b$, dann lässt sich q_0 wieder darstellen durch $q_0 = q_1 \cdot b + r_1$, also insgesamt gilt

$$a = (q_1 \cdot b + r_1) \cdot b + r_0 = (q_1 q_0 r_0)_b.$$

Man erhält bei Fortführung des Verfahrens eine abnehmende Folge $a, q_0, q_1, \dots$ in $\mathbb{N}$, und diese hat nach dem Prinzip vom kleinsten Element ein kleinstes Element. Die wiederholte Division mit Rest endet also nach endlich vielen Schritten mit einem $q_k < b$.

Insgesamt ergibt sich

$$a = (\dots(((q_k \cdot b + r_k) \cdot b + r_{k-1}) \cdot b + r_{k-2}) \cdot b + \dots + r_1) \cdot b + r_0 = (q_k r_k r_{k-1} \dots r_1 r_0)_b$$

mit $1 \leq q_k < b$ und $0 \leq r_i < b$, $0 \leq i \leq k$.

Zum Beispiel ergibt sich für $b = 6$ und $a = 83$

$$83 = 13 \cdot 6 + 5 = (2 \cdot 6 + 1) \cdot 6 + 5 = 2 \cdot 6^2 + 1 \cdot 6^1 + 5 \cdot 6^0 = (215)_6.$$

Man kann $q_k < b$ als Rest einer weiteren Division durch b auffassen ($q_k = 0 \cdot b + r_{k+1}$), d.h. in der verkürzten Darstellung von a benutzt man die Reste als Ziffern. $(215)_6$ ist dann **Zifferndarstellung** der Zahl 83 bezüglich der Basis 6.

Die Bestimmung der Zifferndarstellung einer Zahl bezüglich einer Basis erfolgt also durch einen Algorithmus, und daher lassen sich die Ziffern am besten mit Hilfe einer Tabelle bestimmen.
Beispiel $b = 7, a = 38\,704$:

Schritt	Division mit Rest durch 7 $a = q \cdot 7 + r$	Rest	$q > 0$?
1	$38\,704 = 5\,529 \cdot 7 + 1$	1	ja
2	$5\,529 = 789 \cdot 7 + 6$	6	ja
3	$789 = 112 \cdot 7 + 5$	5	ja
4	$112 = 16 \cdot 7 + 0$	0	ja
5	$16 = 2 \cdot 7 + 2$	2	ja
6	$2 = 0 \cdot 7 + 2$	2	nein

Damit ergibt sich $38\,704 = (220\,561)_7$.

Ein Vergleich des ausmultiplizierten Ausdrucks

$$\begin{aligned} a &= (\dots(((0 \cdot b + r_k) \cdot b + r_{k-1}) \cdot b + r_{k-2}) \cdot b + \dots + r_1) \cdot b + r_0 \\ &= r_k b^k + r_{k-1} b^{k-1} + \dots + r_1 b + r_0 = \sum_{i=0}^{k} r_i b^i \end{aligned}$$

mit der Zifferndarstellung $(r_k r_{k-1} r_{k-2} \dots r_1 r_0)_b$ zeigt:

Steht an der i-ten Stelle im Stellenwertsystem die Ziffer r_i (wenn man von rechts zählt und mit 0 anfängt), dann entspricht dies r_i Bündeln der Größe b^i. Zum Beispiel ist

$$38\,704 = 2 \cdot 7^5 + 2 \cdot 7^4 + 0 \cdot 7^3 + 5 \cdot 7^2 + 6 \cdot 7^1 + 1 \cdot 7^0,$$

die 38 704 Elemente einer entsprechenden Menge werden also zu

- 2 Bündeln der Größe $7^5 = 16\,807$,
- 2 der Größe $7^4 = 2\,401$,
- 5 der Größe $7^2 = 49$,
- 6 der Größe $7^1 = 7$ und
- 1 einzelnen Element zusammengefaßt.

Wir haben die Zifferndarstellung einer Zahl a bezüglich der Basis b auf eine bestimmte Weise konstruiert. Erhält man durch eine andere Methode ebenfalls eine Zifferndarstellung in dem Stellenwertsytem mit Basis b, dann stimmen diese Darstellungen überein:

Satz 2.3.3 *Sei $b \in \mathbb{N}$, $b \neq 1$. Zu jedem $a \in \mathbb{N}$ gibt es eine Stellenzahl $s \in \mathbb{N}$ und Ziffern $z_0, z_1, z_2, \ldots, z_{s-1} \in \{0, 1, \ldots, b-1\}$, so dass gilt*

$$z_{s-1} \neq 0 \quad \textit{und} \quad a = \sum_{i=0}^{s-1} z_i b^i.$$

Die Stellenzahl s und die Ziffern $z_0, z_1, \ldots, z_{s-1}$ sind durch a und b eindeutig bestimmt.

Bemerkungen 2.3.4 (1) Die Eindeutigkeitsaussage wäre natürlich falsch, wenn man bei der Zifferndarstellung nicht grundsätzlich führende Nullen weglassen, d.h. nicht $z_{s-1} \neq 0$ verlangen würde. Zum Beispiel wären

$$(021)_5 = (21)_5$$

zwei verschiedene Zifferndarstellungen der Zahl 11 bezüglich der Basis 5.

(2) Aus biologischen Gründen (10 Finger) benutzt man heute im allgemeinen Zifferndarstellungen bezüglich der Basis 10 (Dezimalsystem) und lässt dabei die Benennung der Basis weg, schreibt also z.B. statt $(2436)_{10}$ kurz 2436.

Da die Rechenoperationen der elektronischen Rechner auf den zwei Zuständen *eingeschaltet* und *ausgeschaltet* beruhen, ist in der Informatik das Binärsystem (Zifferndarstellungen bezüglich der Basis 2) wichtig. Diese Zifferndarstellungen können sehr lang und damit unübersichtlich werden. Daher ist auch das Hexadezimalsystem (Zifferndarstellungen bezüglich der Basis 16) gebräuchlich, in dem immer je 4 Binär-Ziffern zu einer Hexadezimalziffer zusammengefaßt werden.

(3) Die zum Stellensystem gehörenden Algorithmen der schriftlichen Addition und Multiplikation sind unabhängig von der Wahl der Basis b. Sie lassen sich sofort aus der Darstellung der zu addierenden bzw. zu multiplizierenden Zahlen als Potenzsummen von b herleiten.

2.4 Rechnen im Stellenwertsystem

Vorteile von Stellenwertsystemen sind einfache Größenvergleiche und algorithmisches Rechnen.

Der Größenvergleich von zwei Zahlen lässt sich vollständig auf die jeweiligen Ziffern und die Anzahl der Ziffern reduzieren, ist also algorithmisch möglich:

Wir betrachten zwei beliebige natürliche Zahlen a und c mit Darstellung im Stellenwertsystem mit Basis b.

(i) Hat a mehr Ziffern als c, so gilt $a > c$ (und umgekehrt).

(ii) Haben a und c gleich viel Ziffern und ist die erste Ziffer (von links) von a größer als die erste Ziffer von c, dann ist $a > b$ (und umgekehrt).

(iii) Sonst überprüft man die nächsten entsprechenden Ziffern von a und c, bis sich zwei unterscheiden, und schließt wie in (ii).

Beispiel 2.4.1 $123456 > 345, \qquad (54366)_8 < (67522)_8, \qquad (32421)_5 > (32414)_5.$

Um zwei im Stellenwertsystem mit Basis b gegebene Zahlen a und c zu addieren, betrachten wir jede der beiden Zahlen als Summe der entsprechenden Potenzen von b, addieren dies und bündeln gegebenfalls das Ergebnis neu.

Beispiel 2.4.2 Für $a = 27 = (123)_4$ und $c = 54 = (312)_4$ ergibt sich

$$\begin{aligned} a + b &= (1 \cdot 4^2 + 2 \cdot 4^1 + 3 \cdot 4^0) + (3 \cdot 4^2 + 1 \cdot 4^1 + 2 \cdot 4^0) = (4 \cdot 4^2 + 3 \cdot 4^1 + 5 \cdot 4^0) \\ &= (1 \cdot 4^3 + 1 \cdot 4^2 + 0 \cdot 4^1 + 1 \cdot 4^0) = (1101)_4 = 81. \end{aligned}$$

Beim tabellarischen Addieren geschieht die Neubündelung schon beim Addieren der Bündel durch entsprechende **Überträge**:

Beispiel 2.4.3 Wieder für $a = (123)_4$ und $c = (312)_4$ ergibt sich

$$\begin{array}{cccc|c} & 1 & 2 & 3 & a \\ & 3 & 1 & 2 & b \\ & 1 & 1 & & \text{Übertrag} \\ \hline 1 & 1 & 0 & 1 & a+b \end{array}.$$

Um entsprechend zwei im Stellenwertsystem mit Basis b gegebene Zahlen a und c zu multiplizieren, betrachten wir wieder jede der beiden Zahlen als Summe der entsprechenden Potenzen von b, multiplizieren diese und bündeln gegebenfalls das Ergebnis neu.

Beispiel 2.4.4 Für $a = 27 = (123)_4$ und $c = 54 = (312)_4$ ergibt sich

$$\begin{aligned} a \cdot b &= (1 \cdot 4^2 + 2 \cdot 4^1 + 3 \cdot 4^0) \cdot (3 \cdot 4^2 + 1 \cdot 4^1 + 2 \cdot 4^0) \\ &= (1 \cdot 4^2 + 2 \cdot 4^1 + 3 \cdot 4^0) \cdot 3 \cdot 4^2 + (1 \cdot 4^2 + 2 \cdot 4^1 + 3 \cdot 4^0) \cdot 1 \cdot 4^1) + (1 \cdot 4^2 + 2 \cdot 4^1 + 3 \cdot 4^0) \cdot 2 \cdot 4^0 \\ &= 3 \cdot 4^4 + 7 \cdot 4^3 + 13 \cdot 4^2 + 7 \cdot 4^1 + 6 \cdot 4^0 = 1 \cdot 4^5 + 1 \cdot 4^4 + 2 \cdot 4^3 + 3 \cdot 4^2 + 0 \cdot 4^1 + 2 \cdot 4^0 \\ &= (112302)_4 = 1458. \end{aligned}$$

Tabellarisch ergibt sich das bekannte System, wobei der 1. Faktor a jeweils mit den Ziffern des 2. Faktors c einzeln multipliziert wird und die Überträge gleich (im Kopf) gebildet werden. Die Produkte werden untereinander geschrieben, wobei die „Wertigkeit" der multiplizierenden Ziffer durch waagrechtes Verschieben dargestellt wird, und anschließend wird die Summe (mit entsprechenden Überträgen) gebildet:

Beispiel 2.4.5 Wieder für $a = (123)_4$ und $c = (312)_4$ ergibt sich mit

$$\begin{array}{cccccc} \multicolumn{6}{c}{(123)_4 \cdot (312)_4} \\ \hline & & & 2 & 4 & 6 \\ & & 1 & 2 & 3 & \\ & 3 & 6 & 9 & & \\ \hline & & & & & \end{array} \qquad \text{bzw.} \qquad \begin{array}{cccccc} \multicolumn{6}{c}{(123)_4 \cdot (312)_4} \\ \hline & & & 3 & 1 & 2 \\ & & 1 & 2 & 3 & \\ 1 & 1 & 0 & 1 & & \\ \hline 1 & 1 & 2 & 3 & 0 & 2 \end{array}$$

$$a \cdot c = 27 \cdot 54 = (123)_4 \cdot (312)_4 = (112302)_4 = 1458.$$

Erwachsene haben diese Verfahren im Zehnersystem in der Regel völlig internalisiert. Man kann sich aber mit einem Trick in die Situation von Schülern zurückversetzen, indem man in anderen Stellenwertsystemen rechnet.

2.5 Teilbarkeitsregeln

Wir betrachten den Fall, dass für zwei natürliche Zahlen a und b die Division mit Rest von a durch b den Rest 0 ergibt:

Definition 2.5.1 *Gegeben seien zwei natürliche Zahlen $a, b \in \mathbb{N}$.*
Gibt es eine weitere natürliche Zahl $k \in \mathbb{N}$ mit

$$a = k \cdot b,$$

dann heißt b **Teiler** *von a, und a heißt* **Vielfaches** *von b.*

k heißt **Komplementärteiler** *von a zu b.*
Man sagt: „b teilt a" oder „a ist Vielfaches von b" oder „Die Division von a durch b geht auf".

Beispiele 2.5.2

(1) 18 hat die Teiler

$$1, 2, 3, 6, 9, 18.$$

Die zugehörigen Komplementärteiler sind

$$18, 9, 6, 3, 2, 1.$$

(2) 1 ist Teiler jeder natürlichen Zahl.

Bemerkungen 2.5.3

(1) Die Teilbarkeit ist eine Relation, d.h. eine Beziehung zwischen den beteiligten Zahlen a und b. Im folgenden schreiben wir kurz

$$b \mid a \qquad :\Longleftrightarrow \qquad b \text{ teilt } a.$$

(2) „b teilt a“ und „a ist Vielfaches von b“ sind nur verschiedene Bezeichnungen für die **Teilbarkeitsrelation** $b \mid a$.

(3) Die Teilbarkeitsdefinition lässt sofort auf ganze Zahlen übertragen. Für das Rechnen in der Menge $\mathbb{Q}$ der rationalen Zahlen ist die obige Definition sinnlos, da jede rationale Zahl außer 0 Teiler jeder anderen rationalen Zahl ist.

„Teilbarkeit“ hat ähnliche Eigenschaften wie die Ordnungsrelation „$\leq$“ auf $\mathbb{N}$:

Satz 2.5.4 *Für alle $a, b, c \in \mathbb{N}$ gilt:*

(a) $a \mid a$. *(Reflexivität)*

(b) Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$. *(Transitivität)*

(c) Aus $a \mid b$ und $b \mid a$ folgt $a = b$.

Weiter gilt

Satz 2.5.5 *Seien $a, b, c, d \in \mathbb{N}$. Dann gilt:*

(a) Aus $b \mid a$ und $d \mid c$ folgt $(b \cdot d) \mid (a \cdot c)$.

(b) Ist c gemeinsamer Teiler von a und b, d.h. es gilt $c \mid a$ und $c \mid b$, dann teilt c auch die Summe $a + b$, die Differenz $a - b$ und jedes Vielfache von $k \cdot a$ mit $k \in \mathbb{N}$.

(c) Gilt $a = b + c$ und d teilt zwei der Zahlen a, b, c, dann teilt d auch die dritte.

Bekanntlich ist eine im Stellenwertsystem mit Basis 10 dargestellte natürliche Zahl genau dann durch 5 teilbar, wenn ihre letzte (Einer-) Ziffer eine 5 oder eine 0 ist, und durch 2 teilbar (d.h. sie ist gerade), wenn ihre letzte Ziffer durch 2 teilbar ist.

Für manche andere Zahlen kann man fast ebenso einfach feststellen, ob sie Teiler einer vorgegebenen natürlichen Zahl sind:

Satz 2.5.6 *Sei $d \in \mathbb{N}$ und*

$$a \in \mathbb{N} \quad \text{mit} \quad a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_n \cdot 10^n, \quad n \in \mathbb{N}_0, \quad a_i \in \{0, 1, \ldots, 9\}.$$

(a) $d = 2$ oder $d = 5$: d Teiler von a $\Leftrightarrow$ d Teiler von a_0. *(Endstellenregel)*

(b) $d = 2^2$ oder $d = 5^2$: d Teiler von a $\Leftrightarrow$ d Teiler von $(a_1 a_0)_{10} = a_1 \cdot 10 + a_0$.

(c) $d = 2^3$ oder $d = 5^3$: d Teiler von a $\Leftrightarrow$ d Teiler von $(a_2 a_1 a_0)_1 0 = a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$.

(d) $d = 3$ oder $d = 9$:
d Teiler von a $\Leftrightarrow$ d Teiler der **Quersumme** $a_0 + a_1 + a_2 + \ldots + a_n$ *von a.*
(Quersummenregel)

(e) $d = 11$:
d Teiler von a $\Leftrightarrow$ d Teiler der **alternierenden Quersumme** $a_0 - a_1 + a_2 - \ldots + (-1)^n a_n$ *von a.*
(alternierende Quersummenregel)

Beispiele 2.5.7

(1) $a = 3035220$ ist durch 2, 3, 4 und 5 und damit durch 6, 10 und 12 teilbar, aber nicht durch 8, 9, 11 oder 25.

(2) $a = 22374$ ist durch 2, 3, 9 und 11 und damit durch 6, 18, 22, 33 teilbar, aber nicht durch 4 oder 8.

2.6 Primzahlen

Jede natürliche Zahl $a \in \mathbb{N}$ ist durch a und durch 1 teilbar, denn es gilt $a = a \cdot 1$. Man nennt die beiden Faktoren a und 1 **triviale Teiler** von a. Wir betrachten nun die Zahlen, die nur triviale Teiler besitzen.

Definition 2.6.1 *Eine natürliche Zahl $a \in \mathbb{N}$, $a \neq 1$, heißt* **prim***, wenn sie nur die trivialen Teiler* 1 *und a besitzt. Sonst heißt sie* **zusammengesetzt***.*

Bemerkungen 2.6.2 (1) Die Eins hat als neutrales Element bezüglich der Multiplikation eine Sonderrolle. Sie ist weder prim noch zusammengesetzt und heißt **Einheit**.

(2) $a \in \mathbb{N}$ ist prim genau dann, wenn a genau zwei (verschiedene) Teiler hat.

(3) Ist $a \in \mathbb{N}$ zusammengesetzt und M eine Menge mit a Steinen, dann kann man aus diesen Steinen ein Rechteck mit Seitenlängen > 1 legen. Für eine Primzahl a ist das nicht möglich.

Einfaches Probieren ergibt die ersten Primzahlen $2, 3, 5, 7, 11$. Bei großen Zahlen ist dieses Verfahren mühsam.
Ein einfacher Algorithmus, um alle Primzahlen in einem Anfangsstück von $\mathbb{N}$, d.h. unterhalb einer gegebenen Zahl n, zu bestimmen, ist das Sieb des Eratosthenes (von Kyrene, ca. 275-194 v.Chr.).

Sieb des Eratosthenes:

Schritt 1: Schreibe alle natürlichen Zahlen von 1 bis n auf. Streiche die 1.

Schritt 2: Ist das Quadrat der kleinsten Zahl, die weder gestrichen noch gekennzeichnet ist, größer als n, dann ist die Menge der nicht gestrichenen Zahlen gleich der Menge der Primzahlen $\leq n$, und man ist fertig.

Schritt 3: Sonst kennzeichnet man diese kleinste Zahl (als Primzahl) und streicht alle ihren echten Vielfachen.

Schritt 4: Fahre mit Schritt 2 fort.

Beispiel 2.6.3 $n = 99$. $\boxed{7}$ bedeutet die gekennzeichnete Primzahl 7, 4 die gestrichene Zahl 4, **73** die sich nach Abbruch ergebende Primzahl 73. Es gilt $\sqrt{99} < 10$.

	$\boxed{2}$	$\boxed{3}$	4	$\boxed{5}$	6	$\boxed{7}$	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	

Betrachtet man die Folge der Primzahlen, dann lassen sich nur schwer Gesetzmäßigkeiten feststellen.

Es gibt immer wieder sogenannte Primzahlzwillinge, d.h. Paare von Primzahlen, deren Differenz 2 ist (also kleinstmöglich mit Ausnahme des Paares $(2, 3)$), z.B. $(3, 5)$, $(5, 7)$, $(11, 13)$, $(41, 43)$.

Andererseits gibt es auch immer wieder sehr große Abschnitte in $\mathbb{N}$, in denen keine Primzahl enthalten ist. Wählt man nämlich eine beliebige natürliche Zahl $n \in \mathbb{N}$, $n \neq 1$, dann ist keine der Zahlen $n! + 2, n! + 3, \ldots, n! + n$ prim.

Es ist noch nicht einmal offensichtlich, ob die Folge der Primzahlen abbricht, d.h. endlich ist, oder nicht. Seit Euklid (ca. 300 v.Chr.) ist aber bekannt:

Satz 2.6.4 (Euklid) *Die Menge der Primzahlen ist unendlich.*

Wir wollen nun zeigen, dass die Primzahlen die elementaren Bausteine für die Menge der natürlichen Zahlen bezüglich der Multiplikation sind.
Dazu zeigen wir zuerst, dass sich jede natürliche Zahl $a > 1$ als Produkt von Primzahlen schreiben lässt, wobei einerseits die 1 als Faktor ausgeschlossen ist, andererseits Produkte zugelassen sind, die nur aus einem Faktor bestehen.

Satz 2.6.5 (Existenz der Primfaktorzerlegung) *Jede Zahl $a > 1$ kann man als Produkt von endlich vielen (nicht notwendigerweise verschiedenen) Primzahlen darstellen. Dieses Produkt heißt* **Primfaktorzerlegung** *von a.*

Beispiel 2.6.6 Der Algorithmus aus dem Beweis ergibt $1960 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 7 \cdot 7$.

Die Zahl 12 lässt sich auf verschiedene Arten als Primzahlprodukt schreiben, z.B.

$$12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2.$$

Diese Darstellungen unterscheiden sich aber nur in der Reihenfolge der Faktoren. Interessant sind eigentlich nur *wesentlich verschiedene* Primfaktorzerlegungen einer natürlichen Zahl, die sich durch die auftretenden Primfaktoren oder ihre Anzahl unterscheiden.

Der nächste Satz zeigt, dass in dieser Hinsicht verschiedene Primfaktorzerlegungen natürlicher Zahlen nicht existieren:

Satz 2.6.7 (Eindeutigkeit der Primfaktorzerlegung) *Hat eine natürliche Zahl $a \in \mathbb{N}$, $a \neq 1$, zwei Primfaktorzerlegungen*

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_m = q_1 \cdot q_2 \cdot \ldots \cdot q_n$$

mit Primfaktoren $p_1, p_2, \ldots, p_m$ bzw. $q_1, q_2, \ldots, q_n$ und $p_1 \leq p_2 \leq \ldots \leq p_m$ und $q_1 \leq q_2 \leq \ldots \leq q_n$, dann gilt $m = n$ und $p_i = q_i$ für alle i, $1 \leq i \leq m$.

Bemerkungen 2.6.8

(1) Satz 2.6.5 und Satz 2.6.7 fasst man zusammen zum **Hauptsatz der elementaren Zahlentheorie**: Jede natürliche Zahl $a > 1$ hat eine Primfaktorzerlegung und diese ist (bis auf Reihenfolge der Primfaktoren) eindeutig.

(2) Der Hauptsatz wäre natürlich i.a. nicht richtig, wenn man die Eins zu den Primzahlen rechnen würde.

(3) Im allgemeinen sortiert man in der Primfaktorzerlegung einer Zahl die Faktoren nach ihrer Größe und fasst gleiche Faktoren zu Potenzen zusammen. Die Primfaktorzerlegung hat damit die Gestalt

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m}.$$

Für $a = 1400$ ergibt sich zum Beispiel

$$1400 = 2^3 \cdot 5^2 \cdot 7^1.$$

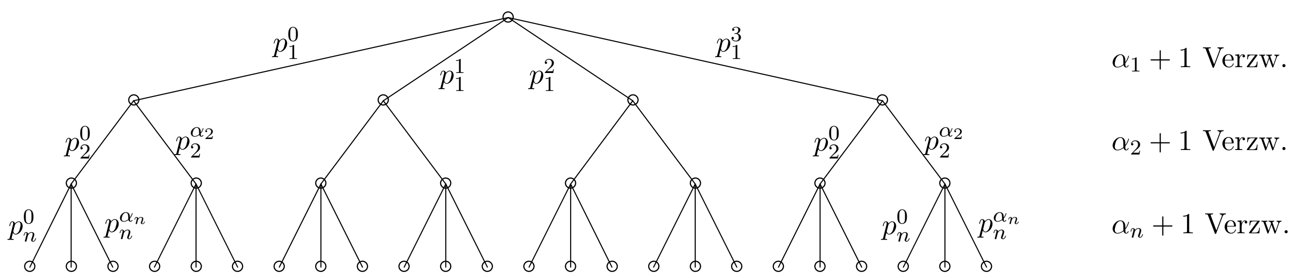
Mit der Vereinbarung $x^0 := 1$ kann man die Primfaktorzerlegung jeder natürlicher Zahl $a > 1$ als Produkt von Potenzen aller Primzahlen schreiben, also

$$1400 = 2^3 \cdot 3^0 \cdot 5^2 \cdot 7^1 \cdot 11^0 \cdot \ldots .$$

Mit Hilfe der eindeutigen Primfaktorzerlegung einer natürlichen Zahl kann man alle Teiler dieser Zahl bestimmen: Zu einer Zahl

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n} \quad \text{mit } p_1, \ldots, p_n \text{ prim}, \alpha_1 > 0, \ldots, \alpha_n > 0$$

betrachtet man das Baumdiagramm (hier skizziert für $1960 = 2^3 \cdot 5^1 \cdot 7^2$)



Dann gilt: *Jeder Weg von der Wurzel des Baumdiagramms zu einem Endpunkt entspricht einem Teiler und umgekehrt.*

Damit erhält man

Satz 2.6.9 *Ist* $a \in \mathbb{N} \setminus \{1\}$ *und hat die eindeutige Primfaktorzerlegung*

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n},$$

dann hat a genau $(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots (\alpha_n + 1)$ *verschiedene Teiler.*

Beispiel 2.6.10 1960 hat genau 24 verschiedene Teiler. Der kleinste ist $1 = 2^0 \cdot 5^0 \cdot 7^0$, der größte $1960 = 2^3 \cdot 5^1 \cdot 7^2$.

Zu je zwei natürlichen Zahlen a und b gibt es immer mindestens einen gemeinsamen Teiler, nämlich die Zahl 1. Andererseits gilt für jeden gemeinsamen Teiler d sowohl $d \leq a$ als auch $d \leq b$, d.h. es gibt höchstens endlich viele gemeinsame Teiler und damit auch einen größten. Diesen kann man mit Hilfe der Primfaktorzerlegungen von a und b bestimmen.

Satz 2.6.11 *Seien* $a, b \in \mathbb{N} \setminus \{1\}$ *mit Primfaktorzerlegungen*

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}, \qquad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}, \qquad \alpha_i, \beta_1 \in \mathbb{N}_0, \quad 1 \leq i \leq n.$$

Weiter sei für jedes $1 \leq i \leq n \quad \gamma_i := \min(\alpha_i, \beta_i)$. *Dann ist* $\qquad d := p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_n^{\gamma_n}$

der **größte gemeinsame Teiler** *von a und b.*

Beispiel 2.6.12 Für

$$a = 1960 = 2^3 \cdot 5^1 \cdot 7^2, \qquad b = 686 = 2^1 \cdot 5^0 \cdot 7^3$$

ist

$$d = 2^1 \cdot 5^0 \cdot 7^2 = 98$$

der größte gemeinsame Teiler.

Bemerkungen 2.6.13 (1) Man bezeichnet den größten gemeinsamen Teiler von a und b im allgemeinen mit $\mathbf{ggT(}\boldsymbol{a, b}\mathbf{)}$.

(2) Ganz analog kann man das **kleinste gemeinsame Vielfache** $\mathbf{kgV(}\boldsymbol{a, b}\mathbf{)}$ zweier natürlicher Zahlen a und b bestimmen:
Setzt man (für dieselben Primfaktorzerlegungen wie im vorigen Satz) $\delta_i := \max(\alpha_i, \beta_i)$, $1 \leq i \leq n$, dann gilt

$$\mathrm{kgV}(a, b) = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \ldots \cdot p_n^{\delta_n}.$$

(3) Aus dem vorigen Satz und der vorigen Bemerkung folgt für alle $a, b \in \mathbb{N}$

$$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = a \cdot b.$$

Die Bestimmung der Primfaktorzerlegungen der Zahlen a und b kann recht mühsam sein. Eine i.a. einfachere Methode zur Berechnung des größten gemeinsamen Teilers liefert der euklidische Algorithmus, der auf einer fortgesetzten Division mit Rest beruht.

Euklidischer Algorithmus:

Schritt 1: Setze $x := a$ und $y := b$.

Schritt 2: Teile x durch y mit Rest r. Ist $r = 0$, dann breche man ab.

Schritt 3: Sonst setze $x := y$ und $y := r$ und fahre mit Schritt 2 fort.

Beispiel 2.6.14 $a = 64\,589$, $b = 3\,178$:

Schritt	x	y	Division mit Rest $a = q \cdot b + r$	Rest r	$r > 0$?
1	64 589	3 178	$64\,589 = 20 \cdot 3\,178 + 1\,029$	1 029	ja
2	3 178	1 029	$3\,178 = 3 \cdot 1\,029 + 91$	91	ja
3	1 029	91	$1\,029 = 11 \cdot 91 + 28$	28	ja
4	91	28	$91 = 3 \cdot 28 + 7$	7	ja
5	28	7	$28 = 4 \cdot 7 + 0$	0	nein

Bemerkungen 2.6.15 (1) Ob man im 1. Schritt a durch b oder b durch a mit Rest dividiert, hat auf die Abschlußwerte von x und y keine Auswirkung. Ist $a < b$ und teilt man a durch b, dann läuft der Algorithmus genau einen Schritt länger, als wenn man b durch a teilt.

(2) Bei jedem Schritt ist der Rest kleiner als der Divisor. Beim nächsten Schritt wird dieser Rest neuer Divisor, d.h. der neue Rest ist wieder kleiner. Die Reste bilden also eine abnehmende Folge in $\mathbb{N}$, d.h. nach dem Wohlordnungsprinzip bricht der Algorithmus nach endlich vielen Schritten ab.

Satz 2.6.16 *Seien $a, b \in \mathbb{N}$. Führt man den euklidischen Algorithmus für a und b durch, dann ist der Abschlußwert y gleich dem größten gemeinsamen Teiler von a und b.*