

Elemente der Arithmetik und Algebra I

Wintersemester 2003/2004

Vorlesungsmanuskript

zur Vorlesung von Maria Specovius

Dieses Vorlesungsmanuskript beruht auf dem Skript von Reinhard Hochmuth zur gleichnamigen Vorlesung für das WS 2002/2003, ihm sei an dieser Stelle herzlich für das Überlassen seines Skriptes gedankt.

FB Mathematik/Informatik, Universität Gesamthochschule Kassel

Inhaltsverzeichnis

1	Zu Beginn	4
2	Zahlaspekte	5
3	Mengen	6
4	Endliche Mengen und Anzahl	9
5	Abbildungen	11
6	Unendliche Mengen	17
6.1	Grundlegendes	17
6.2	Die Menge der rationalen Zahlen	18
6.3	Die Menge der reellen Zahlen oder: was ist ∞ ?	20
7	Kardinalzahlen	22
7.1	Äquivalenzrelationen	22
7.2	Kardinalzahlen als Äquivalenzklassen	23
8	Rechnen mit Kardinalzahlen	26
8.1	Addition	26
8.2	Multiplikation	28
8.3	Kleinerbeziehung	30
9	Relationen, Äquivalenzrelation und Partitionen	31
9.1	Relationen	31
9.2	Eigenschaften von Relationen	33
10	Darstellung von Zahlen I: Die natürlichen Zahlen und Brüche	36
10.1	Geschichtliche Vorbemerkung	36
10.2	Dezimalsystem	38
10.3	Stellenwertsysteme zur Basis $b \in \mathbb{N}$ mit $b \neq 1$	42
10.4	Dezimalbrüche	44
10.5	Darstellungen von Rechnungen in Stellenwertsystemen	47
10.5.1	Addition	47

10.5.2 Subtraktion	49
10.5.3 Multiplikation	51
10.5.4 Division	52
11 Teilbarkeitsregeln	53
12 Hauptsatz der elementaren Zahlentheorie	61
13 GgT und kgV	65
14 Zahlen und Muster, Polynomialzahlen	71
14.1 Dreieckzahlen	71
14.2 Quadratzahlen	71
14.3 Sechseckzahlen	76
15 Vollständige Induktion	79

1 Zu Beginn

Elemente der Arithmetik und Algebra – was bedeuten die Worte eigentlich?

Das Wort Arithmetik stammt von dem griechischen Wort *arithmòs* (= Zahl) ab, das Lexikon der Mathematik gibt hierzu folgende Auskunft:

„In klassischer Sicht dasjenige Teilgebiet der Mathematik, das sich mit dem Rechnen mit Zahlen bez Variablen befasst. Unter Rechnen versteht man hierbei meist die Grundrechenarten. Manchmal findet man den Begriff Arithmetik auch als Synonym zur Zahlentheorie verwendet. . . .“

Unter dem Stichwort „Zahlentheorie“ findet man dann

„Der Gegenstand der Zahlentheorie ist es, Eigenschaften der natürlichen Zahlen $1, 2, 3, \dots$ und der Verknüpfungen (vor allem Addition, Multiplikation und Potenzbildung) aufzuspüren, zu beweisen oder zu widerlegen. . . .“

Schaut man in einem nicht ganz so speziellen Nachschlagewerk – in diesem Fall Meyers großes Taschlexikon, so findet man die Erklärung

„Teilgebiet der Mathematik, das sich mit den Zahlen, und ihren Verknüpfungen nach bestimmten Rechengestzen beschäftigt; umfasst die Grundrechenarten und die Potenzrechnung mit ihren Umkehrungen sowie Folgen und Reihen und die Kombinatorik“

ist also viel großzügiger mit dem Begriff, anschließend wird aber zugegeben:

„ungenau abgegrenzt zu Algebra, Zahlentheorie und Analysis.“

Das Wort „Algebra“ dürften die meisten noch aus der Schule kennen, und es in der Regel mit dem „Buchstabenrechnen“ verbinden. Das Wort „Algebra“ leitet sich aus dem Arabischen *al-dschabr* her, was so viel wie „Einrenkung“ (von Brüchen) bedeutet. Das Lexikon der Mathematik sagt hierzu:

„Ursprünglich verstand man (unter dem mathematischen Gebiet) Algebra das Lösen algebraischer Gleichungen, d.h. die Bestimmung der Nullstellen von Polynomen mit ganz oder rationalzahligen Koeffizienten. . . .“

Heute umfaßt die Algebra ein Fülle von Teilgebieten, die sich im weitesten Sinne mit Verknüpfungen auf Mengen und deren Strukturen beschäftigt.

In dieser Vorlesung geht vor allem um Zahlen:

- Wie und warum sind sie entstanden?
- Was verstehen Mathematiker heute darunter?
- Wie kann man Zahlen darstellen?
- Wie rechnet man mit ihnen, insbesondere auch: Wie begründen sich die Rechen-techniken?
- Welche Beziehungen bestehen zwischen Zahlen – z. B. was sind *befreundete*(??) Zahlen?

2 Zahlaspekte

Der genaue Ursprung der Zahlen liegt im Dunkeln, wieweit z. B. in der Steinzeit gezählt wurde, wissen wir nicht genau. Untersuchungen mit heutigen, sich noch auf einer vergleichbaren Stufe befindenden Ureinwohnern verschiedener Gegenden (z.B. Brasilien, Bolivien) weisen darauf hin, dass die Menschen ursprünglich nur zwischen eins, evtl. zwei und „vielen“ unterschieden. Am Ende der 30er des vorigen Jahrhunderts wurde in der damaligen Tschechoslowakei ein ca 30 000 Jahre alter Wolfsknochen (vergl. [?]) mit 55 eingeritzten Kerben gefunden, diese Kerben sind in 5er Gruppen angeordnet, nach 5×5 Gruppen befand sich eine weitere längere Kerbe. Dies lässt darauf schließen, dass hier schon mit einem gewissen System gezählt wurde.

Heute zählen wir mit

$$\mathbb{N} := \{1, 2, 3, \dots\}, \quad \mathbb{N}_0 := \{0, 1, 2, 3, \dots\}$$

Wofür und wie verwenden wir natürliche Zahlen?

- a) Zum Bestimmen von **Anzahlen**: Wieviele Bonbons bekomme ich? (Kardinalzahlen)
- b) Zum **Numerieren** und **Ordnen**: Die wievielte Seite ist dies? Welchen Platz hat er beim Marathonlauf erreicht? (Ordinalzahlen)
- c) Zum **Rechnen**: Wieviele Bonbons habe ich heute abend, wenn ich nach jedem Essen zwei bekomme und nur jeweils eines lutsche? (Rechenzahlen)
- d) Zum Bestimmen von **Größen**: Wie lange dauert die Vorlesung? Was kostet das Eis? Wie groß ist meine Wohnung? (Maßzahlen)
- e) Zum **Kodieren** von Information: PKW-Kennzeichen, Telefonnummer, Zugnummer, S-Bahnlinien (Zahlen als Codes)

Jeder der Zahlaspekte könnte nun zum Ausgangspunkt einer weiteren Behandlung und Diskussion natürlicher Zahlen genommen werden. Was der Höhlenmensch mit seinem Wolfsknochen gezählt hat, wissen wir nicht, auch nicht, ob die Zahlen schon verschiedene Namen hatten (dies ist nach dem oben gesagten sogar eher unwahrscheinlich.) Was aber auch schon unsere Vorfahren benutzt haben, ist das, was wir heute als Mächtigkeit von Mengen bezeichnen. Selbst wenn ich kein Wort für die Zahl 5 kenne, so kann ich doch feststellen, ob ich genauso viel erlegte Hasen wie Finger an einer Hand habe. Dieser Aspekt der Zahlen soll zunächst weiterverfolgt werden. Dazu beschäftigen wir uns zunächst mit Mengen.

Erinnert sei zuvor noch an die Zeichen \Rightarrow und \Leftrightarrow . Hat man zwei Aussagen A und B , so bedeutet

$A \Rightarrow B$: aus A folgt B , oder anders formuliert: Wenn A gilt, muss auch B gelten. $A \Leftrightarrow B$: A gilt genau dann, wenn B gilt.

Beispiel:

- (A) Alle Studierenden der Mathematik können Bruchrechnen.
- (B) Alle Studierenden der Mathematik können addieren.

(C) Alle Studierenden in Kassel können Bruchrechnen.

(D) Alle Studierenden in Kassel können addieren.

Welche Aussagen lassen sich nun sinnvoll mit \Leftrightarrow oder \Rightarrow verbinden?

3 Mengen

Definition 3.1 *Eine Menge ist eine Zusammenfassung bestimmter wohl unterschiedener Objekte. Für jedes Objekt muß feststehen, ob es zur Menge gehört oder nicht. Ein Objekt x , das zu einer Menge M gehört, heißt Element von M . Wir schreiben: $x \in M$. Falls x kein Element von M ist, schreiben wir: $x \notin M$.*

Einschub: Aristoteles über den Begriff der Definition

Kommentar zu Aristoteles:

lebte von 384 – 322 v. Christus, berühmtester Schüler von Platon, und Lehrer Alexanders des Großen. Bis heute jemand, der die Philosophie entscheidend beeinflusst.

Mengen können auf verschiedene Weise eingeführt bzw. festgelegt werden.

i) Aufzählend: $M = \{1, 2, 3, 7\}$, $\mathbb{N} = \{1, 2, 3, \dots\}$, $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$.

ii) Verbal:

- S Menge an der Uni Kassel immatrikulierten Studenten
- \mathbb{N} Menge der natürlichen Zahlen
- \mathbb{Z} Menge der ganzen Zahlen
- \mathbb{Q} Menge der rationalen Zahlen, also der Brüche mit ganzzahligen Zählern und Nennern mmit von Null verschiedenen Nennern.

iii) Charakterisierend durch Angabe einer Eigenschaft:

- $A = \{x \in S \mid x \text{ studiert}\}$
- $\mathbb{Q} = \{x \in \mathbb{R} \mid x = \frac{p}{q}, p, q \in \mathbb{Z}, q \neq 0\}$

Also: Definition einer Menge durch Aussonderung aus einer größeren Menge durch Prüfen, ob eine (oder mehrere) Bedingungen erfüllt sind.

Die Definition 3.1 einer Menge entspricht dem sog. „naiven Mengenbegriff“. Diese Formulierung verweist auf grundlagentheoretische Probleme bei der Einführung von Mengen. Immerhin erlaubt unsere Formulierung folgende „Objekte“ von der weiteren Diskussion auszuschließen:

Russelsche Antinomie: B sei die Menge aller Mengen, die sich nicht selbst als Element enthalten. Formal: $B = \{M \mid M \notin M\}$. Frage: Enthält B sich selbst als Element oder nicht?

Überlegen uns: Angenommen es gilt $B \in B$. Daraus folgt $B \notin B$. Andererseits folgt aus $B \notin B$, daß gilt $B \in B$.

Bei B handelt es sich also um kein sinnvoll definiertes Objekt und in unserem Sinne insbesondere um keine Menge. (Bertrand Russel (1872-1970): englischer Mathematiker und Philosoph)

Erinnert sei im folgenden an einige Begriffe mittels denen man Beziehungen zwischen Mengen herstellen kann oder aus gegebenen Mengen neue Mengen „erzeugen kann“.

Definition 3.2 A, B seien Mengen. A heißt Teilmenge von B genau dann, wenn jedes Element aus A auch in B liegt, in Zeichen $A \subset B$. (lies: ist Teilmenge von)

Für alle Mengen A gilt: $A \subset A$.

Eine wichtige Visualisierung für Beziehungen und Verknüpfungen bei Mengen sind sog. Venn-Diagramme, in denen Mengen durch ebene ovale Figuren dargestellt werden. (Von Britischem Mathematiker John Venn (1843–1923) 1881 eingeführt. 1859 Priester, 1862 Professor für Moralphilosophie in Cambridge, widmete sich nach 1883 ganz Vorlesungen und Forschungen über Logik.) Die folgende Abbildung visualisiert $A \subset B$.

Definition 3.3 Zwei Mengen A, B heißen gleich (in Zeichen: $A = B$), wenn sie dieselben Elemente haben, das heißt

1. jedes Element aus A gehört auch zu B
2. jedes Element aus B gehört auch zu A .

Etwas formaler ausgedrückt

Gilt $A \subset B$, aber $A \neq B$, so heißt A „echte“ Teilmenge von B . Manchmal schreiben wir $A \subsetneq B$.

Offensicht gilt: $A = B \iff A \subset B$ und $B \subset A$.

Beispiele

1. Die Mengen $\{13, 4, 5, 13\}$ und $\{4, 13, 5\}$ sind gleich, da sie dieselben Elemente enthalten.
2. $A = \{5, 6\}$, $B = \{x \in \mathbb{R} \mid x^2 - 11x + 30 = 0\}$. Es gilt: $A = B$.
3. Zahlbereiche $\mathbb{N} \subsetneq \mathbb{N}_0 \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$

Definition 3.4 Die Menge der gemeinsamen Elemente zweier Mengen A, B heißt Durchschnitt (Durchschnittsmenge) von A und B , in Zeichen $A \cap B$.

(Bildchen)

Definition 3.5 Wenn zwei Mengen A, B keine gemeinsamen Elemente haben, so heißen die Mengen disjunkt. In Zeichen: $A \cap B = \emptyset$.

Im letzten Fall spricht man auch von der “leeren Menge”. Statt \emptyset schreibt man alternativ auch $\{\}$.

Definition 3.6 *Seien A, B Mengen. Die Vereinigungsmenge $A \cup B$ ist die Menge aller Elemente, die zu A oder zu B gehören.*

(Bildchen)

Definition 3.7 *A, B seien Mengen. $A \setminus B$ (lies: A minus B , A ohne B) bezeichnet diejenige Menge, die nur die Elemente aus A enthält, die nicht auch in B liegen.*

(Bildchen)

Beispiel

Seien $A = \{1, 2, 3, 8\}$, $B = \{2, 3, 100, 70\}$. Dann gilt $A \setminus B = \{1, 8\}$, $B \setminus A = \{70, 100\}$, $A \cap B = \{2, 3\}$, $A \cup B = \{1, 2, 3, 8, 70, 100\}$.

4 Endliche Mengen und Anzahl

Die Anzahl von Elementen einer endlichen Menge kann man durch **Zählen** bestimmen. Beim Zählen ordnet man die Elemente durch sukzessive Auswahl in einer bestimmten Weise an. Die letzte Zahl beim Zählen ergibt die Anzahl der Elemente. Durch ein solches Zählen ordnet man den Elementen einer Menge M die Zahlen eines Anfangsstückes von \mathbb{N} , also eine Menge der Form $\{1, 2, 3, \dots, n\}$, zu. Wir schreiben

$$|M| := \text{card}M := n \quad (4.1)$$

und bezeichnen n auch als die Kardinalzahl von M . Offenbar gibt es Mengen für die diese Definition keine Anzahl (oder Kardinalzahl) liefert, z.B. für \mathbb{N} selbst.

Wir nennen eine Menge endlich, wenn das Zählen erfolgreich ist, das heißt das Zählen zu einem Ende kommt, und unendlich, wenn das nicht der Fall ist.

Bemerkung In (4.1) verwendeten wir die natürlichen Zahlen, um für eine endliche Menge die Anzahl ihrer Elemente zu definieren. Diese Definition nutzt den Kardinalzahlaspekt der natürlichen Zahlen. Unser Ziel wird es im folgenden sein, dies in gewissem Sinne umzukehren, also natürliche Zahlen über Mengen und gewisse Eigenschaften derselben, nämlich solche die mit dem Begriff der Anzahl zusammenhängen, zu definieren.

Die eingeführte Methode der Anzahlbestimmung mittels Zählen läßt sich auch als Entnahmeverfahren beschreiben, siehe z.B. []. Dabei bezeichnen wir als **Entnahmeverfahren** für eine Menge M ein Verfahren, das wie folgt vorgeht: Gegeben sei eine nichtleere Menge M .

1. Aus M wird ein Element m_1 ausgewählt. Man erhält $M_1 := M \setminus \{m_1\}$.
2. Aus M_1 wird ein Element m_2 ausgewählt. Man erhält $M_2 := M_1 \setminus \{m_2\}$.
- ⋮
- k. Aus M_{k-1} wird ein Element m_k ausgewählt. Man erhält $M_k := M_{k-1} \setminus \{m_k\}$.

Wir sagen, das Entnahmeverfahren bricht ab, wenn für ein gewisses $n \in \mathbb{N}$ gilt: $A_n = \emptyset$.

Klar:

- i) Zählen ist genau dann erfolgreich, wenn das Entnahmeverfahren abbricht.
- ii) $\text{card}M = n$ genau dann, wenn $M_n = \emptyset$.

Nun stellt sich eine (evtl. auf manche kleinlich wirkende) Frage: Erhalte ich durch anderes Zählen (also eine andere sukzessive Auswahl von Elementen) eine andere Anzahl von Elementen? Wir „wissen“, daß dies nicht so ist und haben dieses Wissen auch schon unserer Definition zugrundegelegt. Würde nämlich ein anderes Zählen zu einem anderen Ergebnis führen, würde die Schreibweise $|M|$ ohne Vermerken der „Zählart“ keinen Sinn ergeben.

Eine auf unserem „Wissen“ gegründete vergewissernde Argumentation könnte etwa folgendermaßen aussehen: Wir zählen, indem wir die jeweils zugeordneten Zahlen nicht nur denken oder diese aussprechen, sondern kleben auf jedes ausgewählte Element einen Zettel mit der jeweiligen Ziffer. Jede beliebige andere sukzessive Auswahl erhalten wir nun indem wir die Zettel gegebenenfalls (also wenn die Zuordnung nicht stimmt) entfernen und auf das jeweils richtige Element kleben. Da durch dieses Tun („Operieren“) keine Elemente verschwinden oder entstehen, reichen die Zettel aus und es wird auch keiner überflüssig.

Manchmal können wir auch unmittelbar die Anzahl der Elemente einer Menge bestimmen ohne wirklich zu zählen. Im obigen Beispiel nämlich z.B. dann, wenn wir die Anzahl der „Zettel“ kennen. Wir kleben einfach auf jedes Element genau einen. Reichen sie aus und bleibt keiner übrig so ist die Anzahl der Element durch die Anzahl der Zettel gegeben. Anderes Beispiel: Sitzplätze im Hörsaal.

Zwei endliche zählbare Mengen besitzen also die gleiche Anzahl von Elementen, wenn wir deren Elemente einander eineindeutig zuordnen können. Vernachlässigen wir nun die „Zettel“ und die Frage, ob wir überhaupt mit dem Zählen zu einem Ende kommen, so bleibt als zentraler Begriff der der „eineindeutigen Zuordnung“.

Definition 4.1 *Wir sprechen von einer **eineindeutigen Zuordnung** zwischen zwei Mengen A und B , wenn gilt:*

1. *Jedem Element von A ist genau ein Element von B zugeordnet.*
2. *Jedes Element von B kommt genau einmal als zugeordnetes Element vor.*

*Gibt es eine solche eineindeutige Zuordnung, so nennt man die Mengen A und B **gleichmächtig**.*

Beispiel. Sitzplätze im Theater: Die Zuordnung Platz \leftrightarrow Zuschauer ist eineindeutig, wenn das Theater ausverkauft ist und niemand jemand auf dem Schoß hat.

Endliche Mengen M mit $\text{card}M = n$ können in eineindeutiger Weise der Menge $\{1, 2, \dots, n\}$ zugeordnet werden. M und $\{1, 2, \dots, n\}$ sind also gleichmächtige Mengen:

$$\text{card}M = n \iff M \text{ und } \{1, 2, \dots, n\} \text{ sind gleichmächtig.}$$

Offenbar kann der Begriff der eineindeutigen Zuordnung auch auf Mengen angewendet werden, die nicht endlich sind.

Beispiel Die Mengen \mathbb{N} und $G :=$ Menge der geraden natürlichen Zahlen sind gleichmächtig:

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & \dots & n & \dots \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & & \uparrow & \\ 2 & 4 & 6 & 8 & 10 & \dots & 2n & \dots \end{array}$$

Zwei Menge können also gleichmächtig sein, auch wenn es uns nicht gelingt die Anzahl ihrer Elemente durch Zählen oder das Entnahmeverfahren zu bestimmen.

Eineindeutige Zuordnungen können als Abbildungen aufgefaßt werden. Bevor wir weitergehen, wollen wir uns mit diesen ein wenig genauer beschäftigen.

5 Abbildungen

Definition 5.1 Gegeben seien zwei nichtleere Mengen A und B . Ist in einer bestimmten Weise jedem Element x aus A genau ein (wohlbestimmtes) Element y aus B zugeordnet, so nennt man diese Zuordnung eine Abbildung f mit Definitionsmenge (Definitionsbereich) A und Zielmenge B oder auch eine Funktion f von (der Menge) A in (die Menge) B . In Zeichen: $f : A \rightarrow B$, $x \mapsto y$ oder auch $x \mapsto f(x)$. $f(x)$ heißt auch Wert der Funktion f an der Stelle x oder Bildpunkt von x bei der Abbildung f .

Beispiele

1. A sei eine Menge von Studierenden, die eine Klausur schreiben müssen, B die Menge der zur Verfügung stehenden Plätze in einem passenden Hörsaal. Die Aufsicht weist jedem Studierenden einen Platz zu.
2. A_1 sei die Menge der Fahrgäste, die heute mit dem Thalys um 10.54 von Aachen nach Lüttich fahren; B_2 die Menge der zur Verfügung stehenden Platznummern, $f_1 : A_1 \rightarrow B_1, a \mapsto \text{Platznummer auf der Reservierung}$.
 A_2 sei die Menge der Fahrgäste, die heute um 10.00 mit dem IC von Kassel nach Weimar fahren, B_2 ebenfalls die Menge der zur Verfügung stehenden Platznummern, und $f_2(a) = \text{Nummer auf der Reservierung}$. Welche der zwei Zuordnungen definiert eine Funktion? Hinweis: Im Thalys besteht Reservierungspflicht!
Was passiert, wenn ich das zweite Beispiel abändere durch $B_2 = \text{Menge der Sitzplätze}$, und die Zuordnungsvorschrift: $f(x) = \text{Platz, den man belegt hat}$, oder $g(x) = \text{Platz, auf dem die Gäste wirklich sitzen}$.
Voraussetzung: Der Zug ist nicht überfüllt. Ändert sich etwas, wenn Mütter ihre Babies auf dem Schoß haben?
3. $A = B = \mathbb{N}$, $f : A \rightarrow B, n \mapsto 2n$ (Abbildung)
4. $A = B = \mathbb{N}$, $f : A \rightarrow B, n \mapsto n/2$ (keine Abbildung)
5. $A = \text{Menge der geraden Zahlen}$, $B = \mathbb{N}$, $f : A \rightarrow B, n \mapsto n/2$ (Abbildung)
6. Die identische Abbildung id_A einer nichtleeren Menge A ist definiert durch $\text{id}_A : A \rightarrow A, x \mapsto x$.

Definition 5.2 Zwei Funktionen $f_1 : A_1 \rightarrow B_1$ und $f_2 : A_2 \rightarrow B_2$ heißen gleich (in Zeichen: $f_1 = f_2$), wenn gilt $A_1 = A_2$, $B_1 = B_2$ und für alle $x \in A_1$ ist $f_1(x) = f_2(x)$.

Bemerkung: Hierdurch wird eigentlich erst das mathematische Objekt „Abbildung“ (oder auch „Funktion“) definiert in Abgrenzung zum Begriff „Zuordnungsvorschrift“.

Beispiele Im Lichte dieser Definition sehe man sich noch einmal die Beispiele von eben an.

1. Seien $f_1 : \mathbb{Z} \rightarrow \mathbb{Z}, x \mapsto (x-3)^2$ und $f_2 : \mathbb{Z} \rightarrow \mathbb{Z}, x \mapsto x^2 - 6x + 9$. Es gilt für alle $x \in \mathbb{Z}$ $(x-3)^2 = x^2 - 6x + 9$, also (da auch Definitions- und Zielmenge) übereinstimmen) $f_1 = f_2$.
2. $f_3 : \mathbb{Z} \rightarrow \mathbb{Z}, x \mapsto \text{sign}(x-3)(x-3)^2$, hierbei soll $\text{sign}(x-3)$ das Vorzeichen von $x-3$ sein:

$$\text{sign}(z) = \begin{cases} -1 & z < 0, \\ +1 & z \geq 0 \end{cases} \quad \text{also} \quad \text{sign}(x-3) = \begin{cases} -1 & x < 3, \\ +1 & x \geq 3 \end{cases}$$

Für $x < 3$ ist $(x-3)^2 \neq \text{sign}(x-3)(x-3)^2 = -(x-3)^2$, also $f_1 \neq f_3$ und $f_2 \neq f_3$.

Eine Funktion $f : A \rightarrow B$ ordnet nicht nur jedem Element von A ein Element von B zu, sondern auch jeder Teilmenge X von A eine Teilmenge $f(X)$ von B und jeder Teilmenge Y von B eine Teilmenge $f^{-1}(Y)$ von A :

$$f(X) := \{y \in B \mid \text{Es ex. ein } x \in X \text{ mit } y = f(x)\} = \{f(x) \mid x \in X\}$$

und

$$f^{-1}(Y) := \{x \in A \mid f(x) \in Y\}.$$

Die Menge $W = f(A)$ heißt dann **Wertemenge** (oder Bildmenge) von A für die Abbildung f .

Beispiel $\sin : \mathbb{R} \rightarrow \mathbb{R}$ besitzt die Wertemenge $W = [-1, 1]$. (Bildchen)

Definition 5.3 Eine Abbildung $f : A \rightarrow B$ heißt **surjektiv** genau dann, wenn gilt $f(A) = B$.

Definition 5.4 Eine Abbildung $f : A \rightarrow B$ heißt **injektiv** genau dann, wenn für alle $x_1, x_2 \in A$ mit $x_1 \neq x_2$ gilt $f(x_1) \neq f(x_2)$.

Klar: $f : A \rightarrow B$ ist injektiv \iff Für alle $x_1, x_2 \in A$ gilt: Aus $f(x_1) = f(x_2)$ folgt $x_1 = x_2$.

Beispiel. Nochmal der nicht überfüllte IC von Kassel nach Weimar und die Abbildung $f : \text{Fahrgäste} \rightarrow \text{mögliche Plätze}; a \mapsto \text{belegter Platz}$. Die Wertemenge sind die belegten Plätze. Die Abbildung ist injektiv, wenn jeder einen eigenen Platz belegt, und nicht injektiv, wenn eine Mutter ihr Baby die ganze Zeit auf dem Schoß hat. Die Abbildung ist surjektiv, wenn jeder genau einen Platz hat und der Zug damit voll ist.

Frage: Was ist, wenn jemand mit seinem Gepäck noch einen Platz zusätzlich belegt? (Keine Abbildung im mathematischen Sinn!) Was passiert weiter, wenn der Zug überfüllt ist? (entweder keine Abbildung im mathematischen Sinn: Es gibt Leute, die keinen Platz belegen können, oder wenn sie alle einen besetzen, kann die Abbildung nicht surjektiv sein: Es muss dann jemand geben, der jemand anders auf dem Schoß hat.

Ist $f : A \rightarrow B$ injektiv, so gibt es nach Definition zu jedem $y \in f(A)$ genau ein $x \in A$ mit $f(x) = y$. Für injektives $f : A \rightarrow B$ kann man also die Abbildung

$$g : f(A) \rightarrow A, \quad f(x) \mapsto x$$

definieren. Diese Funktion nennt man die **Umkehrfunktion** oder die **Umkehrabbildung** von f und schreibt dafür f^{-1} .

Klar: Für $x \in A$ gilt $f^{-1}(f(x)) = x$ und für $y \in f(A)$ gilt $f(f^{-1}(y)) = y$.

Definition 5.5 Eine Abbildung $f : A \rightarrow B$ heißt **bijektiv**, wenn sie injektiv und surjektiv ist.

Beispiele

1. $f : \mathbb{N} \rightarrow \mathbb{N} : n \mapsto 2n$ ist injektiv, aber nicht surjektiv:
Ist $2n_1 = 2n_2 \Rightarrow$ (teilen durch 2): $n_1 = n_2$, also ist f injektiv. Die Zahl 3 kommt nicht im Bild vor: angenommen, es gäbe ein n mit $2n = 3 \Rightarrow n = 3/2$, das ist keine natürliche Zahl.
2. $f : \mathbb{N} \rightarrow \{n \in \mathbb{N} : n \text{ gerade Zahl}\} : n \mapsto 2n$ ist bijektiv, wir haben die Zielmenge gerade auf die Wertemenge reduziert.
3. $A :=$ Studierende im Hörsaal 298 am 5.11.2003 um 12 Uhr, $B := \mathbb{N}_0$. Für $s \in A$ bezeichne $f(s)$ das Alter von s (in Jahren). Dadurch ist eine Abbildung $f : A \rightarrow B$ definiert. Vermutlich ist dann folgendes wahr:

- Für $Y_1 := [10, 100]$ gilt $f^{-1}(Y_1) = A$.
- Für $Y_2 := [2000, 5000]$ gilt $f^{-1}(Y_2) = \emptyset$.
- Sind genau 10 der Studenten jünger als 20, so gilt für $Y_3 := [0, 19]$

$$\text{card } f^{-1}(Y_3) = |f^{-1}(Y_3)| = 10.$$

- Die Abbildung ist weder injektiv noch surjektiv.
4. Die Abbildung $s_1 : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto \sin x$ ist nicht surjektiv, da es beispielsweise für $y = 10$ kein $x \in \mathbb{R}$ mit $\sin x = 10$ gibt: $\{x \in \mathbb{R} \mid \sin x = 10\} = \emptyset$. Für alle $x \in \mathbb{R}$ gilt ja $-1 \leq \sin x \leq 1$. Die Abbildung s_1 ist auch nicht injektiv, da beispielsweise $\sin(0) = \sin(\pi) = 0$ ist.
 5. Die Abbildung $s_2 : \mathbb{R} \rightarrow [-1, 1], x \mapsto \sin x$ ist surjektiv, aber nicht injektiv.

Zusammenfassend:

Eine eineindeutige Zuordnung definiert also eine bijektive Abbildung und umgekehrt. Man unterscheide hier sorgfältig zwischen den Begriffen Zuordnung, Abbildung (Funktion), Zuordnungsvorschrift, etwas eindeutig zuordnen, eineindeutige Zuordnung.

Nochmal das Beispiel nach 5.1: Fahrgäste im Thalys und im IC: in beiden Fällen liefert die Vorschrift

Fahrgast \mapsto Nummer auf der Reservierung

eine eindeutige Zuordnung (es wird, wenn überhaupt, genau eine Nummer zugewiesen und nicht etwa 3 Plätze zur Auswahl.). Im Thalys erhält man eine Funktion: *Jeder* Fahrgast muss eine Nummer haben. Im IC ist das keine Funktion, (es gibt auch Fahrgäste ohne Reservierung, die Tatsache, dass es es auch Plätze gibt, die ohne Reservierung sind,

widerspricht hier aber nicht dem Funktionsbegriff - das kann auch im Thalys passieren). Die Zuordnung ist eineindeutig, wenn jeder Fahrgast eine Reservierung hat und der Zug damit ausgebucht ist.

Bildchen

In der Sprache der Abbildungen haben wir: Zwei nichtleere Mengen A und B sind gleichmächtig, wenn es eine bijektive Abbildung $f : A \rightarrow B$ gibt. Wollte man „Gleichmächtigkeit“ mittels bijektiver Abbildungen *einführen*, sollte man ergänzen: \emptyset ist nur zu sich selbst gleichmächtig.

Der folgende Satz formuliert eine weitere Möglichkeit Injektivität zu definieren.

Satz 5.6 *Eine Abbildung $f : A \rightarrow B$ ist injektiv genau dann, wenn für jedes $y \in B$ die Menge $f^{-1}(y)$ höchstens ein Element von A enthält.*

Beweis. „ \implies “ Angenommen, es gibt ein $y \in B$, so daß $f^{-1}(y)$ mehr als ein Element von A enthält, d.h., es gibt $x_1, x_2 \in A$ mit $x_1 \neq x_2$ und $f(x_1) = f(x_2) = y$. Also ist f nicht injektiv. Widerspruch!

„ \impliedby “ Angenommen, f ist nicht injektiv, d.h. es gibt $x_1 \neq x_2$ in A mit $f(x_1) = f(x_2)$. Für $y := f(x_1) = f(x_2) \in B$ gilt dann $\{x_1, x_2\} \subset f^{-1}(\{y\})$. Widerspruch! ■

Definition 5.7 *Gegeben seien nichtleere Mengen A, B, C, D und Abbildungen $f : A \rightarrow B$ und $g : C \rightarrow D$. Gilt $f(A) \subset C$, so kann man jedem $x \in A$ das Element $(g \circ f)(x) := g(f(x))$ in D zuordnen. Die so definierte Funktion $g \circ f : A \rightarrow D$ heißt **Komposition** oder **Hintereinanderausführung** der Abbildungen g, f . (Lies $g \circ f$ als „ g nach f “.)*

(Bildchen)

Bemerkung. $f : A \rightarrow B$ injektiv. Dann gilt

$$f^{-1} \circ f = \text{id}_A \quad \text{und} \quad f \circ f^{-1} = \text{id}_{f(X)}.$$

Lemma 5.8 *Seien $A, B, C \neq \emptyset$ und $f : A \rightarrow B$, $g : B \rightarrow C$ bijektive Abbildungen. Dann gilt: $g \circ f : A \rightarrow C$ ist bijektiv.*

Beweis: Seien $a, b \in A$, $a \neq b \implies f(a) \neq f(b)$, da f injektiv, $\implies (g \circ f)(a) = g(f(a)) \neq g(f(b)) = (g \circ f)(b)$, da g injektiv, also $g \circ f$ injektiv.

Sei $c \in C \implies$ existiert ein $b \in B$ mit $g(b) = c$, da g surjektiv. Weiter existiert ein $a \in A$ mit $f(a) = b$, da f surjektiv, somit $(g \circ f)(a) = g(f(a)) = c$, also ist $g \circ f$ auch surjektiv. ■

Definition 5.9 *Gegeben seien eine Abbildung $f : A \rightarrow B$ und $X \subset A$ nichtleer. Dann heißt die Abbildung $f|_X : X \rightarrow B$, $x \mapsto f(x)$ die **Einschränkung von f auf X** . Umgekehrt heißt f **Fortsetzung von $f|_X$** .*

Satz 5.10 *Sei $f : A \rightarrow B$ surjektiv. Dann existiert $A_0 \subset A$, $A_0 \neq \emptyset$, so daß $f|_{A_0} : A_0 \rightarrow B$ bijektiv ist.*

Beweis. Definiere für $y \in B$

$$K_y := f^{-1}(\{y\}) = \{x \in A \mid f(x) = y\}.$$

Es gilt

- $K_y \neq \emptyset$ für jedes $y \in B$, da f surjektiv ist,
- $K_{y_1} \cap K_{y_2} = \emptyset$ für $y_1 \neq y_2$, da f eine Abbildung ist.

Wähle nun aus jedem K_y genau ein Element und fasse diese in der Menge $A_0 \subset A$ zusammen. Dann gilt: $f|_{A_0} : A_0 \rightarrow B$ ist injektiv und surjektiv. ■

Beispiel. $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $B = \{0, 1, 2, 3\}$,

$$f : A \rightarrow B, x \mapsto f(x) = [x/3].$$

Dabei bezeichnet $[y]$ die größte ganze Zahl, die kleiner oder gleich y ist. Wir suchen $A_0 \subset A$, so daß $f|_{A_0} \rightarrow B$ bijektiv ist. Dazu erstellen wir eine Wertetabelle:

x	0	1	2	3	4	5	6	7	8	9
f(x)	0	0	0	1	1	1	2	2	2	3

An dieser erkennen wir, daß wir zum Beispiel $A_0 := \{0, 3, 7, 9\}$ wählen könnten. Es wären aber auch die Mengen $\{1, 3, 7, 9\}$ oder $\{1, 5, 6, 9\}$ möglich. Insgesamt gibt es 27 Möglichkeiten für die Wahl von A_0 .

Nun noch etwas über Abbildungen zwischen endlichen Mengen.

Satz 5.11 Gegeben seien endliche Mengen A, B mit $|A| = m$ und $|B| = n$. Dann gilt:

- i) Es existiert eine injektive Abbildung $f : A \rightarrow B$ genau dann, wenn $m \leq n$.
- ii) Es existiert eine surjektive Abbildung $f : A \rightarrow B$ genau dann, wenn $m \geq n$.
- iii) Es existiert eine bijektive Abbildung $f : A \rightarrow B$ genau dann, wenn $m = n$.

Beweis. Zu i) „ \Leftarrow “ Wir zählen die Elemente der Mengen $A = \{a_1, a_2, \dots, a_m\}$ und $B = \{b_1, b_2, \dots, b_n\}$, und ordnen sie nacheinander und untereinander an:

$$\begin{array}{cccccccc} a_1 & a_2 & a_3 & a_4 & \dots & a_m & & \\ b_1 & b_2 & b_3 & b_4 & \dots & b_m & b_{m+1} & \dots & b_n. \end{array}$$

Wir definieren $f : A \rightarrow B$, $a_i \mapsto b_i$. Die Abbildung f ist nach Konstruktion injektiv. „ \Rightarrow “ Wir definieren $b_i := f(a_i) \in B$. Die b_i sind, wegen der Injektivität von f , alle paarweise verschieden. Also muß gelten $n = |B| \geq m$.

Zu ii) „ \Leftarrow “ Wir zählen wieder die Elemente der Mengen A und B und ordnen sie nacheinander und untereinander an:

$$\begin{array}{cccccccc} a_1 & a_2 & a_3 & a_4 & \dots & a_n & b_{n+1} & \dots & a_m \\ b_1 & b_2 & b_3 & b_4 & \dots & b_n & & & \end{array}$$

Diesmal definieren wir

$$f : A \rightarrow B, a_i \mapsto \begin{cases} b_i, & 1 \leq i \leq n \\ b_n, & i > n. \end{cases}$$

Die so definierte Funktion f ist surjektiv.

„ \implies “ Da f surjektiv ist, gilt für jedes $b_i \in B$: $f^{-1}(\{b_i\}) \neq \emptyset$. Wir wählen nun jeweils ein $a_i \in f^{-1}(\{b_i\})$. Diese sind alle paarweise verschieden. Also ist $m = |A| \geq n$.

(iii) zur Übung. ■

Satz 5.12 *Eine Abbildung einer endlichen Menge in sich ist surjektiv genau dann, wenn sie injektiv ist.*

Beweis. Gegeben seien $f : A \rightarrow A$ und $A = \{a_1, a_2, \dots, a_n\}$, also $|A| = n$.

„ \implies “ f sei surjektiv, also gilt $|f^{-1}(\{a_i\})| \geq 1$ für jedes $a_i \in A$. Ferner sind die Mengen $f^{-1}(\{a_i\})$ alle paarweise disjunkt. Angenommen, f ist nicht injektiv, d.h., es gibt ein $a_i \in A$ mit $|f^{-1}(\{a_i\})| \geq 2$. Dann gilt $|A| \geq n + 1$. Widerspruch!

„ \impliedby “ f sei injektiv, also $|\{f(a_1), f(a_2), \dots, f(a_n)\}| = n$. Angenommen, f ist nicht surjektiv, d.h., es gibt ein $a \in A \setminus \{f(a_1), f(a_2), \dots, f(a_n)\}$. Dann gilt $|A| \geq n + 1$. Widerspruch! ■

6 Unendliche Mengen

6.1 Grundlegendes

Endliche Mengen sind für uns Mengen, von denen wir die Anzahl der Elemente durch Zählen erfolgreich angeben können. Statt von erfolgreichem Zählen könnten wir auch von abbrechenden Entnahmeverfahren sprechen. Schaut man sich das Entnahmeverfahren in Abschnitt 4 genau an, so sieht man, dass man das für jede Menge durchführen kann, unabhängig davon, wie groß sie ist.

Definition 6.1 *Unendliche Mengen sind solche Mengen, die nicht endlich sind. M.a.W.: Eine Menge M ist unendlich, wenn das Entnahmeverfahren nicht abbricht. (Also: Egal, wie oft ich ein Element herausnehme, es bleibt immer noch etwas übrig in der Menge).*

Wir wollen nun etwas mehr über unendliche Mengen in Erfahrung bringen. Jeder bringt sicher Vorstellungen über folgende Mengen mit, auch die, dass es sich hierbei um unendliche Mengen handelt: \mathbb{N} , \mathbb{Q} und \mathbb{R} .

Zunächst wollen wir der Frage nachgehen, ob sich endliche bzw. unendliche Mengen auch ohne explizites Verwenden natürlicher Zahlen mit Hilfe von Abbildungen charakterisieren lassen.

Sei M eine unendliche Menge (von Zahlen, der Einfachheit halber). Das Entnahmeverfahren liefert uns dann eine Menge von paarweise verschiedenen Zahlen $a_i \in M$, $i \in \mathbb{N}$, die wir in einer Menge $X \subset M$ zusammenfassen:

$$X = \{a_1, a_2, a_3, \dots\}.$$

Wir können also eine Abbildung $f : \mathbb{N} \rightarrow M$ durch $f(i) = a_i$ einführen, diese Abbildung ist in jedem Fall injektiv. Nach Definition ist $f : \mathbb{N} \rightarrow X$ sogar bijektiv, daher sind die Mengen \mathbb{N} und X gleichmächtig. Damit haben wir schon eine Richtung des folgenden Satzes bewiesen.

Satz 6.2 *Eine Menge M ist unendlich $\Leftrightarrow M$ enthält eine zu \mathbb{N} gleichmächtige Teilmenge.*

Beweis. „ \Rightarrow “ s.o.

„ \Leftarrow “ Indirekt: Wenn M endlich ist, kann M keine zu \mathbb{N} gleichmächtige Menge enthalten.

■

Wieviel ist aber ∞ ? Im Zusammenhang mit diesem Satz können wir insbesondere formulieren, daß es keine unendliche Menge gibt, die „weniger“ Elemente als \mathbb{N} enthält.

Versetzen wir uns in ein berühmtes Gedankenexperiment:

Hilberts Hotel:

In einem Hotel gibt es unendlich viele nummerierte Zimmer, und alle sind belegt. Abends spät kommt ein völlig abgehetzter Gast an. Der Manager bedauert: „Alles schon belegt“. „Kein Problem, „ sagt der Gast, „lassen Sie doch alle in das nächste Zimmer umziehen!“ Zur Verblüffung des Managers funktioniert das, er muss niemand abweisen und niemand

herausschmeißen. Jeder Gast zieht ein Zimmer weiter, dann ist Zimmer 1 frei für den späten Gast...

Abstrakt: Sei M eine unendliche Menge und $f : \mathbb{N} \rightarrow X$, $X = \{a_1, a_2, a_3, \dots\} \subset M$ wie oben. Wir schreiben nun die Elemente von X zweimal untereinander und ordnen die Elemente der oberen Reihe Elementen der unteren Reihe zu:

$$\begin{array}{cccccccc} a_1 & & a_2 & & a_3 & & a_4 & & \cdots & & a_n & & \cdots \\ & \searrow & & \searrow & & \searrow & & \searrow & & \searrow & & \searrow & & \searrow \\ a_1 & & a_2 & & a_3 & & a_4 & & \cdots & & a_n & & \cdots \end{array}$$

Formal definieren wir $X' := \{a_2, a_3, a_4, \dots\} = X \setminus \{a_1\}$ durch $g : X \rightarrow X'$ mit $g(a_n) := a_{n+1}$ für alle $n \in \mathbb{N}$. Die Abbildung g ist bijektiv, also sind die beiden Mengen X und X' gleichmächtig, obwohl X' eine echte Teilmenge von X bildet.

Wir setzen g nun zu einer Abbildung auf ganz M fort. Dazu sei $M' := M \setminus \{a_1\}$ und $h : M \rightarrow M'$ sei definiert durch

$$h(x) := \begin{cases} g(x), & x \in X, \\ x, & x \in M \setminus X. \end{cases}$$

Die Abbildung ist offenbar injektiv und wegen $M' = X' \cup (M \setminus X)$ ist sie auch surjektiv. Also sind auch die Mengen M und M' gleichmächtig, obwohl M' eine echte Teilmenge von M bildet.

Dies ist für endliche Mengen M nicht möglich: Wenn $|M| = n \in \mathbb{N}$, $M' \subset M$ und $M \setminus M' \neq \emptyset$ gilt, so muss $|M'| \leq n - 1$ sein. Damit haben wir folgenden Satz bewiesen.

Satz 6.3 *Eine Menge M ist unendlich genau dann, wenn M eine echte Teilmenge M' enthält, die zu M gleichmächtig ist.*

Den zweiten Teil des Satzes könnten wir zur Definition unendlicher Mengen (und damit auch endlicher Mengen) verwenden. Diese Definition hätte offensichtlich den Vorteil, daß sie ohne die natürlichen Zahlen (explizit) zu verwenden auskommt. Wir können nun auch (unabhängig von \mathbb{N}) erklären, was eine endliche Menge ist: Eine Menge heißt endlich, wenn sie zu keiner echten Teilmenge gleichmächtig ist. Diese Definition geht auf Richard Dedekind zurück. Bevor wir weiter endliche Mengen behandeln wollen wir wichtige Beispiele für unendliche Mengen diskutieren.

6.2 Die Menge der rationalen Zahlen

Das Symbol \mathbb{Q} bezeichnet die Menge der rationalen Zahlen (in *unseren* Köpfen, die Griechen der Antike hatten eine ganz andere Vorstellung davon) also

$$\mathbb{Q} := \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N} \right\}.$$

Für $\mathbb{Q}_+ := \left\{ \frac{p}{q} \mid p \in \mathbb{N}, q \in \mathbb{N} \right\}$ und $\mathbb{Q}_- := \{-x \mid x \in \mathbb{Q}_+\}$ gilt

- $\mathbb{Q}_+ \cap \mathbb{Q}_- = \emptyset$, $0 \notin \mathbb{Q}_+ \cup \mathbb{Q}_-$;

- $\mathbb{Q} = \mathbb{Q}_+ \cup \mathbb{Q}_- \cup \{0\}$.

Die Mengen \mathbb{Q}_+ und \mathbb{Q}_- sind gleichmächtig, da $x \mapsto -x$ eine bijektive Abbildung von \mathbb{Q}_+ auf \mathbb{Q}_- definiert. Die Elemente von \mathbb{Q}_+ sind in der folgenden Tabelle enthalten: Startend

	1	2	3	4	5	6	7	8	9	p
1	1	2	3	4	5	6	7	8	9	p
2	1/2	1	3/2	2	5/2	3	7/2	4	P/2	P/2
3	1/3	2/3	1	4/3	5/3	2	7/3	8/3	3	P/3
4	1/4	1/2	3/4	1	5/4	3/2	7/4	2	9/4	P/4
5	1/5	2/5	3/5	4/5	1	6/5	7/5	8/5	9/5	P/5
6	1/6	1/3	1/2	2/3	5/6	1	7/6	4/3	9/6	P/6
7	1/7	2/7	3/7	4/7	5/7	6/7	1	8/7	9/7	P/7
q	1/q	2/q	3/q	4/q	5/q	6/q				p/q

bei 1 liegen auf dem skizzierten Weg alle Elemente aus \mathbb{Q}_+ . Weglassen derjenigen Elemente der Tabelle, die schon vorher auf dem Weg lagen, liefert schließlich eine bijektive Abbildung $g : \mathbb{N} \rightarrow \mathbb{Q}_+$, die jedem $n \in \mathbb{N}$ auf eineindeutige Weise eine positive rationale Zahl g_n zuordnet. Eine bijektive Abbildung $f : \mathbb{N} \rightarrow \mathbb{Q}$ erhält man dann durch die Definition

$$f(m) := \begin{cases} 0, & m = 1, \\ g_n, & m = 2n, n \in \mathbb{N}, \\ -g_n, & m = 2n + 1, n \in \mathbb{N}. \end{cases}$$

Damit erweist sich \mathbb{Q} als gleichmächtig zu \mathbb{N} .

Definition 6.4 Mengen, die gleichmächtig zu \mathbb{N} sind, nennen wir abzählbar unendlich.

Satz 6.5 \mathbb{Q} ist abzählbar unendlich.

Da unendliche Mengen immer eine zu \mathbb{N} gleichmächtige Teilmenge enthalten, bilden die abzählbar unendlichen Mengen (im Sinne der Gleichmächtigkeit) die „kleinsten“ unendlichen Mengen.

Bemerkung Der angegebenen Beweis der Abzählbarkeit von \mathbb{Q} stammt von Georg Cantor. Die Methode nennt man erstes Cantorsches Diagonalverfahren.

6.3 Die Menge der reellen Zahlen oder: was ist ∞ ?

Das Symbol \mathbb{R} bezeichnet die Menge der reellen Zahlen, diese haben wir noch nicht konstruiert, oder mathematisch definiert, wir arbeiten zunächst einmal mit der Vorstellung, die wir in unseren Köpfen haben.

Da $\mathbb{N} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$, ist \mathbb{R} mindestens abzählbar unendlich. Hat \mathbb{R} nun genauso viele Zahlen wie \mathbb{Q} , (d.h. genauso viele wie \mathbb{N} im Sinne von gleichmächtig) – oder mehr?

Hier eine Erinnerung an die Schule: Die Abbildung $f : \mathbb{R} \rightarrow (0, 1)$, $x \mapsto \frac{\arctan x + \pi/2}{\pi}$ bijektiv ist. (Bildchen) Daraus folgt sofort, daß \mathbb{R} gleichmächtig zu $(0, 1)$ ist. Die Elemente des Intervalls $(0, 1)$ entsprechen gerade den Dezimalzahlen

$$0, a_1 a_2 a_3 a_4, \dots, \quad a_i \in \{0, 1, 2, 3, \dots\},$$

wobei nicht alle $a_i = 0$ sein können und kein Endstück aus lauter Neunen vorkommt (Begründung ebenfalls später).

Wir wollen im folgenden zeigen, daß $(0, 1)$ nicht abzählbar unendlich ist. Dazu führen wir einen Widerspruchsbeweis. Wir nehmen an, daß $(0, 1)$ abzählbar unendlich ist, d.h., daß es eine bijektive Abbildung von \mathbb{N} auf $(0, 1)$ gibt. Damit können wir die angegebenen Dezimalzahlen (in einer gewissen Reihenfolge) untereinander schreiben:

$$\begin{aligned} &0, a_{11} a_{12} a_{13} a_{14} a_{15} \dots \\ &0, a_{21} a_{22} a_{23} a_{24} a_{25} \dots \\ &0, a_{31} a_{32} a_{33} a_{34} a_{35} \dots \\ &0, a_{41} a_{42} a_{43} a_{44} a_{45} \dots \\ &\vdots \end{aligned}$$

Nun definieren wir

$$b := 0, b_1 b_2 b_3 b_4 b_5 \dots$$

durch $b_n := \begin{cases} 1, & a_{nn} \neq 1, \\ 2, & a_{nn} = 1. \end{cases}$ Es ist $b \in (0, 1)$. Nach Konstruktion kommt b aber nicht in der obigen Aufzählung vor. Wir hatten aber vorausgesetzt, daß in jener alle Elemente von $(0, 1)$ auftreten. Widerspruch! Also ist $(0, 1)$ und damit \mathbb{R} nicht abzählbar unendlich.

Bemerkung. Auch dieser Beweis geht auf Georg Cantor zurück. Man spricht auch vom zweiten Cantorschen Diagonalverfahren.

Mengen, die gleichmächtig zu \mathbb{R} sind, werden manchmal auch kontinuum-unendlich genannt. Zum Beispiel erweist sich $\mathbb{R} \times \mathbb{R}$ als gleichmächtig zu \mathbb{R} , also auch als kontinuum-unendlich.

Naheliegend ist nun folgende Frage: Gibt es eine unendliche Teilmenge von \mathbb{R} , die weder abzählbar unendlich noch gleichmächtig zu \mathbb{R} ist? Auf diese auch Kontinuumproblem genannte Frage kennt man bis heute keine Antwort! P.J. Cohen bewies 1963: Es ist unmöglich, mit den bekannten Methoden der Mengenlehre eine solche Menge zu bestimmen, und: es ist unmöglich mit diesen Methoden zu beweisen, daß es eine solche Menge nicht gibt!

Noch eine Zusatzüberlegung für Hartgesottene. (War nicht Bestandteil der Vorlesung)

Gibt es Mengen, die mehr Elemente als \mathbb{R} enthalten, also z.B. eine Menge, die \mathbb{R} selbst enthält, aber nicht gleichmächtig zu \mathbb{R} ist?

Eine Antwort auf unsere Frage liefert die folgende Überlegung: Gegeben sei eine nichtleere Menge M . Bezüglich dieser Menge definieren wir

$$\mathcal{P}(M) := \{T \mid T \subset M\}.$$

Diese Menge heißt **Potenzmenge** von M .

Beispiel $M = \{1, 2, 3\}$, dann ist $\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$. Hier ist also $|M| = 3$, $|\mathcal{P}(M)| = 8 = 2^3$. Nach der gleichen Strategie kann man $\mathcal{P}(\mathcal{P}(M))$ bilden und erhält eine Menge mit $2^8 = 256$ Elementen, zu viele, sie alle aufzuführen, aber es geht so los:

$$\mathcal{P}(\mathcal{P}(M)) = \{\emptyset, \{\emptyset\}, \{\{1\}\}, \{\{2\}\}, \{\{3\}\}, \{\{1, 2\}\}, \{\{1, 3\}\}, \{\{2, 3\}\}, \{\{1, 2, 3\}\}, \{\emptyset, \{1\}\}, \dots\}.$$

Die Potenzmenge ist also „viel größer“ als Menge selbst. Bei endlichen Mengen kann man das leicht sehen. Es gilt aber auch bei beliebigen Mengen.

Satz 6.6 *Es gibt keine surjektive Abbildung von M nach $\mathcal{P}(M)$.*

Beweis. Angenommen, es existiert eine surjektive Abbildung $f : M \rightarrow \mathcal{P}(M)$, d.h. für jedes $m \in M$ sei $f(m) \subset M$. Für jedes $m \in M$ gilt entweder $m \in f(m)$ oder $m \notin f(m)$. Wir definieren

$$G := \{m \in M \mid m \notin f(m)\}.$$

Offenbar ist $G \in \mathcal{P}(M)$. Also gibt es wegen der Surjektivität von f ein $g \in M$ mit

$$f(g) = G.$$

Aus $g \in f(g)$ folgt dann $g \in G$, also nach Definition von G ist $g \notin f(g)$. Andererseits, wäre $g \notin f(g)$, so wäre (wiederum nach Definition von G) $g \in G$ also $g \in f(g)$. Demnach gilt weder $g \in f(g)$ noch $g \notin f(g)$.

Aufgrund dieses Widerspruchs muß unsere Annahme falsch sein. Also: Es gibt keine surjektive Abbildung von M auf $\mathcal{P}(M)$. ■

Diese Überlegung zeigt insbesondere, daß \mathbb{R} nicht gleichmächtig zu $\mathcal{P}(\mathbb{R})$ ist. Da sich \mathbb{R} aber als Teilmenge von $\mathcal{P}(\mathbb{R})$ auffassen läßt, $\mathcal{P}(\mathbb{R})$ enthält ja insbesondere alle $\{r\}$, $r \in \mathbb{R}$, enthält $\mathcal{P}(\mathbb{R})$ (im Sinne der Gleichmächtigkeit) mehr Elemente. Analog enthält $\mathcal{P}(\mathcal{P}(\mathbb{R}))$ natürlich „mehr“ Elemente als $\mathcal{P}(\mathbb{R})$.

Mittels der Potenzmengen können wir uns nun nochmal überlegen, daß es die Menge aller Mengen „nicht gibt“, bzw. so ein (wie auch immer definiertes) Objekt nicht sinnvoll ist: Wäre nämlich G diese Menge, so könnten wir G als echte Teilmenge von ihrer Potenzmenge $\mathcal{P}(G)$ auffassen. Andererseits enthält G sicherlich alle Teilmengen von sich selbst als Element. Wir hätten also

$$G \subsetneq \mathcal{P}(G) \subset G.$$

7 Kardinalzahlen

7.1 Äquivalenzrelationen

Was sind nun eigentlich natürliche Zahlen? Um zu verstehen, wie Mathematiker diese Frage heute beantworten, wollen wir nun wieder zum Kardinalzahlaspekt natürlicher Zahlen zurückkehren, der durch die Frage „Wieviele?“ angesprochen wurde. Diesen Aspekt wollen wir nach Möglichkeit beschreiben, ohne dabei die natürlichen Zahlen selbst (explizit) zu verwenden.

Was passiert beim „Zählen“ einer endlichen Menge? Es wird eine abstrakte Eigenschaft (nämlich die Anzahl der Elemente) einer Menge nachgeprüft, unabhängig davon, ob es sich um eine Menge von Äpfeln, Bonbons, Autos, Studierenden, Wörter oder Ideen handelt. Mit Blick auf diese Eigenschaft werden zwei Mengen als gleichwertig oder äquivalent angesehen, wenn sie „gleich groß“ sind, mathematisch also, wenn sie gleichmächtig sind. Dabei stellen wir folgendes fest: Haben wir eine Menge A (von Kindern, z.B.) und eine Menge B (von Bonbons), und ist A gleichmächtig mit B , so ist auch B gleichmächtig mit A , haben wir dann eine dritte Menge C (z.B. von Zahnbürsten), die gleichmächtig ist zu B , so ist C auch gleichmächtig zu A (wir wissen dann sofort, ohne noch einmal „nachzählen“ zu müssen: genausoviele Zahnbürsten wie Kinder.) Natürlich ist jede Menge zu sich selbst gleichmächtig.

Durch das Abprüfen „ A ist genauso groß wie B “ oder „ A ist gleichmächtig mit B “ werden somit gewisse endliche Mengen zueinander in Beziehung gesetzt. Weiterhin stellen wir fest: Die Eigenschaft, gleichmächtig zu sein, sortiert die endlichen Mengen in gewisse Klassen, die voneinander verschieden sind: Die Mengen mit einem Element, die Mengen mit zwei Elementen, die Mengen mit drei Elementen... Beim Zählen selbst wird die zu zählende Menge mit einer nur in unserem Kopf vorhandenen Referenzmenge verglichen, z.B. mit der Menge der Wörter { eins, zwei, drei, vier, ... }

Mathematiker formalisieren diesen Prozess über die Begriffe: Äquivalenzrelation, Bilden einer Äquivalenzklasse, Auswählen eines Repräsentanten einer Äquivalenzklasse. Diese Begriffe sind fundamental in vielen Bereichen der Mathematik. Uns ermöglichen sie es, die natürlichen Zahlen zu konstruieren, und wir wir später noch sehen werden, auch die rationalen und die reellen Zahlen.

Definition 7.1 Sei A eine Menge. Bei einer Relation auf A werden gewissen Elementen aus A weitere Elemente aus A zugeordnet (sie werden „zueinander in Beziehung gesetzt“). Ist ein $b \in A$ einem $a \in A$ auf diese Weise zugeordnet, so schreiben wir $a R b$. (Lies: a ist in Relation zu b .) Statt R kann auch ein anderes Symbol zwischen a und b stehen, je nach Zusammenhang. Eine Relation heißt **Äquivalenzrelation**, hier verwenden wir jetzt das Zeichen \sim statt R , wenn folgendes gilt:

1. $a \sim a$ für alle $a \in A$. (Reflexivität)
2. $a \sim b \Leftrightarrow b \sim a$. (Symmetrie)
3. $a \sim b$ und $b \sim c \Rightarrow b \sim c$. (Transitivität)

- Beispiele 7.2**
1. Sei A_1 die Menge der Studierenden im Hörsaal. Wir setzen $a \sim b \Leftrightarrow a$ hat die gleiche Haarfarbe wie b . Offensichtlich ist das eine Äquivalenzrelation.
 2. Wieder sei A_2 die Menge der Studierenden im Hörsaal. Wir setzen jetzt $a \heartsuit b \Leftrightarrow a$ ist befreundet mit b . Das definiert offensichtlich eine Relation auf A , wahrscheinlich keine Äquivalenzrelation (Transitivität?), und welche Teile der Definition einer Äquivalenzrelation erfüllt sind, kann schon zu philosophischen Grundsatzdiskussionen führen.
 3. Sei $A_3 = \{1, 2, \dots, 100\}$, mit $a \sim b \Leftrightarrow$ beim Teilen durch 4 bleibt derselbe Rest übrig. Dies definiert ebenfalls eine Äquivalenzrelation.

Definition 7.3 Sei $A \neq \emptyset$ eine Menge mit einer Äquivalenzrelation \sim . Für $a \in A$ heißt die Menge $[a] := \{b \in A \mid a \sim b\}$ die **Äquivalenzklasse von a**

Satz 7.4 Sei $A \neq \emptyset$ eine Menge mit einer Äquivalenzrelation \sim . Dann ist A die Vereinigung aller Äquivalenzklassen. Keine Äquivalenzklasse ist leer, und für zwei Elemente $a \neq b$ gilt: Entweder $[a] \cap [b] = \emptyset$ oder $[a] = [b]$.

Beweis. Da für jedes $a \in A$ gilt: $a \in [a]$, ist keine Äquivalenzklasse leer, und A ist die Vereinigung aller dieser Klassen.

Seien jetzt $a \neq b$ gegeben. Wenn $[a] \cap [b] = \emptyset$, sind wir fertig. Wenn das nicht so ist, so gibt es $c \in ([a] \cap [b])$, dh. $a \sim c$ und $b \sim c$. Ist nun $a_1 \in [a]$, so gilt $a \sim a_1 \Rightarrow a_1 \sim a \Rightarrow a_1 \sim c \Rightarrow a_1 \sim b$, also $a_1 \in [b]$. Genauso zeigt man: $b_1 \in [b] \Rightarrow b_1 \sim c \Rightarrow b_1 \sim a$. (Bildchen)

■

Beispiele 7.2'

1. Offensichtlich sind in einer Äquivalenzklasse alle Studies mit derselben Haarfarbe enthalten. Wieviele Klassen man erhält, hängt davon ab, wieviel Differenzierung wir bei der Haarfarbe zulassen. Wenn nur die Farben blond, braun, schwarz und rot zugelassen sind, erhält man diese vier Klassen. (Zur Klassifizierung braucht man dann allerdings eine(n) Friseur(in)...)
2. Beim dritten Beispiel waren vier mögliche Reste übrig: 0, 1, 2, 3. Man erhält auch hier vier Äquivalenzklassen, (die offensichtlich disjunkt sind!). In diesem Beispiel hat man $[1] = [5] = [9] = \dots$. Die Zahlen 1, 5, 9 sind hier sogenannte **Repräsentanten** der Äquivalenzklasse der Zahlen, bei denen der Rest eins übrigbleibt.

7.2 Kardinalzahlen als Äquivalenzklassen

Wir betrachten im folgenden als Grundmenge G die Menge aller endlichen Mengen (beachte: Ein Element von G ist jetzt selbst eine Menge!). (Wir erinnern uns: Endliche Mengen waren solche, wo das Entnahmeverfahren aus Abschnitt 4 abbricht.) Diese Menge ist offensichtlich nicht leer: Jeder „sieht um sich herum“ solche Mengen. Auf G definieren wir eine Äquivalenzrelation: $A \sim B \Leftrightarrow A$ und B sind gleichmächtig, d.h. $A \sim B \Leftrightarrow$ es gibt

eine bijektive Abbildung $f : A \rightarrow B$. Das das eine Äquivalenzrelation ist, haben wir uns oben schon plausibel gemacht, formal argumentiert man wie folgt:

Zu Eigenschaft 1. (Reflexivität) Sei $A \in G$: $A \sim A$, denn die identische Abbildung $id_A : A \rightarrow A, a \mapsto a$ ist bijektiv.

2. Symmetrie: Seien $A, B \in G$, und es gelte $A \sim B$. Dann gibt es eine bijektive Abbildung $h : A \rightarrow B$, also ist $h^{-1} : B \rightarrow A$ bijektiv, und somit $B \sim A$.

3. Transitivität: Sind $A, B, C \in G$, und $A \sim B, B \sim C \Rightarrow$ es gibt bijektive Abbildungen $h_1 : A \rightarrow B, h_2 : B \rightarrow C$, dann ist nach Lemma 5.8 die Abbildung $h_2 \circ h_1 : A \rightarrow C$ bijektiv.

Offensichtlich liegt dann eine Menge mit 5 Elementen in einer anderen Äquivalenzklasse als eine Menge mit 6 Elementen, (allgemein für $n \neq m$, ist eine Menge mit n Elementen in einer anderen Äquivalenzklasse als die Mengen mit m Elementen), aber das wissen wir, weil in unserem Kopf schon eine Vorstellung von 5 oder 6 vorhanden ist, wir haben sozusagen schon Repräsentanten dieser Äquivalenzklassen parat. Wenn wir das einfach „vergessen“ und nur mit dem arbeiten, was wir schon definiert oder bewiesen haben, so wissen wir aus Satz 7.4: Die Menge G zerfällt in disjunkte Äquivalenzklassen, und für $M \in G$ definieren wir:

Definition 7.5

$$[M]$$

ist die **Kardinalzahl von M** , M ist dann Repräsentant der Kardinalzahl $[M]$.

Jetzt müssen wir für jede endliche Menge M noch einen passenden Repräsentanten von $[M]$ angeben, außerdem geben wir diesen Repräsentanten Namen. Wir führen die **natürlichen Zahlen als Kardinalzahlen** (endlicher Mengen) ein: Für die Menge mit einem Element wählen wir als Repräsentant eine Menge mit einem Pik-As als einzigem Element:

$$1 := [\{\spadesuit\}].$$

Betrachten wir jetzt $\{\spadesuit\spadesuit\}$ als möglichen Repräsentanten für 2, so stellt sich die Frage: Wie unterscheiden sich \spadesuit und \spadesuit ? Man erinnere sich daran, dass wir z.B. die Mengen $\{a, b\}$ und $\{a, a, b, b, b\}$ als gleich angesehen hatten. Hingegen waren die Mengen $\{a, b\}$ und $\{a, \{a\}, b\}$ verschieden, für einen Mathematiker sind a und die einelementige Menge $\{a\}$ verschiedene Objekte. So setzen wir

$$2 := [\{\spadesuit, \{\spadesuit\}\}],$$

die beiden Elemente sind also ein Pik-As und die einelementige Menge mit einem Pik-As. Entsprechend ist

$$3 := [\{\spadesuit, \{\spadesuit\}, \{\spadesuit, \{\spadesuit\}\}].$$

Allgemein setzen wir

$$k := [\{\spadesuit, \{\spadesuit\}, \{\spadesuit, \{\spadesuit\}\}, \dots, \{\spadesuit, \{\spadesuit\}, \dots\}, \dots] \quad (\text{„am Ende } k \text{ Klammern“}).$$

Natürlich hätten wir auch $2 := \{\clubsuit, \spadesuit\}$, $3 := \{\clubsuit, \spadesuit, \heartsuit\}$ nehmen können, dann kämen wir aber bei 5 schon ins Grübeln. Die obige Konstruktion, die übrigens von dem Mathematiker John von Neumann¹ stammt, hat den Vorteil eines klaren Bildungsgesetzes: „ $k + 1$ “ = $[k \cup \{k\}]$. Außerdem spiegelt sie zwei Erfahrungen (?) wieder: Die natürlichen Zahlen werden beim Zählen „immer größer“, außerdem „hören sie nie auf“. Wir werden das später in den Peano-Axiomen wiederfinden. Ergänzend definieren wir noch $0 := [\emptyset]$.

Bemerkung. Unser Vorgehen verwendete übrigens nicht die Endlichkeit der betrachteten Mengen. Wir könnten also die Menge G erweitern durch Hinzunehmen unendlicher Mengen. Dadurch erhielten wir Kardinalzahlen unendlicher Mengen wie $[\mathbb{N}]$ oder $[\mathbb{R}]$ sowie zum Beispiel die Identität $[\mathbb{N}] = [\mathbb{Q}]$.

Im folgenden werden wir noch Addition, Multiplikation und die Kleinerbeziehung für Kardinalzahlen behandeln.

¹Von Neumann hat allerdings kein Pik As benutzt, sondern die leere Menge, und ist wie folgt vorgegangen: $1 := \{\emptyset\}$, $2 := \{\emptyset, \{\emptyset\}\}$, ...

8 Rechnen mit Kardinalzahlen

Im vorhergehenden Abschnitt ist es uns gelungen, natürliche Zahlen als Kardinalzahlen einzuführen. Es ist nun naheliegend zu fragen und zu untersuchen, ob und wie auf dieser Grundlage die uns bekannten Grundrechenarten und ihre Eigenschaften (für auf die obige Weise eingeführten natürlichen Zahlen) begründet werden können. Exemplarisch wollen wir die Addition noch ausführlich behandeln.

8.1 Addition

Die Addition natürlicher Zahlen als Kardinalzahlen beruht auf der Vorstellung der Vereinigung von Mengen, beziehungsweise der Vorstellung des Zusammenlegens von Objekten: Wollen wir z.B. die Summe $2 + 3$ bilden, so wählen wir eine Menge, welche die Zahl 3 repräsentiert, z.B. also $\{a, b, c\}$ und eine Menge, welche die Zahl 2 repräsentiert, z.B. also $\{d, e\}$. Nun vereinigen wir die beiden Mengen

$$\{a, b, c\} \cup \{d, e\} = \{a, b, c, d, e\}.$$

„Anwenden“ der „Klammern“ $[\]$ führt auf

$$[\{a, b, c\} \cup \{d, e\}] = [\{a, b, c, d, e\}].$$

Die Addition „+“ als etwas, das mit den Zahlen als Kardinalzahlen „gemacht“ werden soll, läßt sich schreiben als

$$3 + 2 = [\{a, b, c\}] + [\{d, e\}].$$

Nun berücksichtigen wir noch

$$[\{a, b, c, d, e\}] = 5.$$

Als sinnvolles Bindeglied, schließlich wollen wir ja, daß $3 + 2 = 5$ ist, erscheint nun die Festlegung

$$[\{a, b, c\}] + [\{d, e\}] = [\{a, b, c\} \cup \{d, e\}]. \quad (8.2)$$

Wir bemerken, daß wir nicht irgendwelche Repräsentanten für 3 bzw. 2 wählen dürfen. So liefern $\{a, b, c\}$ und $\{a, b\}$

$$[\{a, b, c\} \cup \{a, b\}] = [\{a, b, c\}] = 3$$

nicht das von uns gewünschte Ergebnis 5. Notwendig ist also die Wahl disjunkter Repräsentanten für die zu addierenden Zahlen.

Man kann sich das sehr gut daran klar machen, wenn man sich vorstellt, wie Kinder mit den Fingern addieren!

Damit (8.2) (bzw. die nachfolgende Verallgemeinerung in Definition 8.6) sinnvoll ist, muß diese Festlegung von den gewählten Repräsentanten unabhängig sein: oder mit anderen Worten: Bei der Wahl anderer Repräsentanten für die gleiche (Kardinal-) Zahl sollte das gleiche Ergebnis herauskommen. Ob wir $2+3$ Äpfel, $2+3$ Autos oder $2+3$ Finger addieren, immer sollte eine Menge von der Mächtigkeit 5 herauskommen. Formal drückt man das so aus: Die Operation „+“ muss **wohldefiniert** sein. Das ist so, wie wir jetzt sehen werden.

Definition 8.6 Seien m und n zwei Kardinalzahlen mit $m = [M]$ und $n = [N]$. Sind M und N nicht disjunkt, so wählen wir N' mit $[N'] = [N]$ und $N' \cap M = \emptyset$. Dann definieren wir

$$m + n := [M \cup N'].$$

Im folgenden wählen wir stets disjunkte Repräsentanten.

Satz 8.7 Gegeben seien Kardinalzahlen m und n mit $m = [M] = [M']$ und $n = [N] = [N']$ und es gelte $M \cap N = M' \cap N' = \emptyset$. Dann gilt

$$[M \cup N] = [M' \cup N']. \quad (8.3)$$

Beweis. $[M] = [M']$ und $[N] = [N']$ bedeutet, daß bijektive Abbildungen

$$f : M \rightarrow M' \text{ bzw. } g : N \rightarrow N'$$

existieren. (8.3) ist gezeigt, wenn wir eine bijektive Abbildung $h : M \cup N \rightarrow M' \cup N'$ finden. Eine solche ist aber gegeben durch die Definition

$$h(x) = \begin{cases} f(x), & x \in M, \\ g(x), & x \in N, \end{cases}$$

da x entweder zu M oder zu N gehört. ■

Weiter möchten wir, dass die so eingeführte Addition den uns bekannten Rechenregeln genügt. Welche sind die „wesentlichen“ Rechenregeln und welche können aus diesen abgeleitet werden? Welche gelten überhaupt bzw. sind „charakterisierend“ für die natürlichen Zahlen? Insbesondere: Ist die von uns eingeführte Addition überhaupt („wirklich“) „dieselbe“ die wir „kennen“?

Satz 8.8 Für (endliche) Kardinalzahlen m, n, p gilt

- i) $m + n = n + m$ (Kommutativgesetz der Addition)
- ii) $(m + n) + p = m + (n + p)$ (Assoziativgesetz der Addition)
- iii) $m + 0 = m$ (Gesetz vom neutralen Element der Addition)

Beweis.

Zu i: Wählen $M, N \in G$ mit $M \cap N = \emptyset$ und $m = [M]$, $n = [N]$. Dann gilt

$$m + n = [M] + [N] = [M \cup N] = [N \cup M] = [N] + [M] = n + m.$$

(„Vereinigen ist kommutativ.“)

Zu ii: M, N und P seien paarweise disjunkte endliche Mengen mit $m = [M]$, $n = [N]$ und $p = [P]$. Es gilt

$$(m + n) + p = ([M] + [N]) + [P] = [M \cup N] + [P] = [(M \cup N) \cup P] = [M \cup N \cup P]$$

und

$$[M \cup N \cup P] = [M \cup (N \cup P)] = [M] + [N \cup P] = [M] + ([N] + [P]) = m + (n + p).$$

(„Vereinigen ist assoziativ.“)

Zu iii: Für $m = [M]$ ist

$$m + 0 = [M] + [\emptyset] = [M \cup \emptyset] = [M] = m.$$

■

Wir stellen folgendes fest: Diese Rechengesetze haben wir auf Gesetze im Umgang mit Mengen zurückgeführt. Bei der Subtraktion kann man sich jetzt schon überlegen, wann man begrifflich in Schwierigkeiten kommt.

Im Zusammenhang mit der Subtraktion steht die folgende Beobachtung.

Satz 8.9 Für (endliche) Kardinalzahlen m, n, p gilt (Rechtseindeutigkeit der Addition / Streichungsregel der Addition)

$$m + p = n + p \implies m = n.$$

Einen Beweis für diese Behauptung findet man z.B. in F.Padberg, R.Danckwerts, M.Stein, *Zahlbereiche – Eine elementare Einführung*.

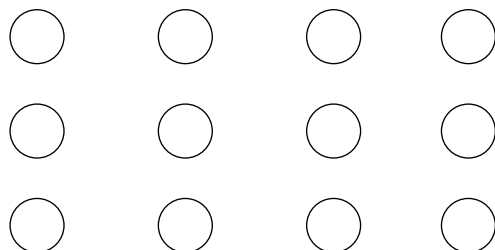
Bemerkung. Assoziativgesetz, Kommutativgesetz und das Gesetz vom neutralen Element würden auch für Kardinalzahlen unendlicher Mengen gelten. Das ist aber nicht für die Streichungsregel richtig: Für $\omega = [\mathbb{N}]$ gilt

$$1 + \omega = [\{\spadesuit\}] + [\mathbb{N}] = [\{\spadesuit\} \cup \mathbb{N}] = [\mathbb{N}] = [\emptyset \cup \mathbb{N}] = 0 + \omega,$$

obwohl $1 \neq 0$.

8.2 Multiplikation

Die Definition der Multiplikation für Kardinalzahlen kann man unter anderem durch geometrische Überlegungen motivieren. Wie können wir uns $3 \cdot 4$ durch „Mengen“ veranschaulichen? Z.B. eben so:



Bei der Formalisierung der Multiplikation wird uns das sogenannte „kartesische Produkt“ weiterhelfen.

Definition 8.10 i) Wenn a und b Elemente einer Grundmenge sind, so heißt (a, b) das **geordnete Paar aus a und b** .

ii) Wenn M und N zwei nichtleere Mengen sind, so heißt

$$M \times N = \{(x, y) \mid x \in M, y \in N\}$$

das **karthesische Produkt von M und N** .

Nun zum Produkt von Kardinalzahlen.

Definition 8.11 Für (endliche) Kardinalzahlen m und n mit $m = [M]$ und $n = [N]$ definieren wir

$$m \cdot n := [M \times N].$$

Auch das Produkt $m \cdot n$ ist wohldefiniert. Es gelten die folgenden Rechenregeln.

Satz 8.12 Für (endliche) Kardinalzahlen m, n, p gilt

- i)** $m \cdot n = n \cdot m$ (Kommutativgesetz der Multiplikation)
- ii)** $(m \cdot n) \cdot p = m \cdot (n \cdot p)$ (Assoziativgesetz der Multiplikation)
- iii)** $m \cdot 1 = m$ (Gesetz vom neutralen Element der Multiplikation)
- iv)** $m \cdot p = n \cdot p \implies m = n$ (Rechtseindeutigkeit der Multiplikation/Streichungsregel der Multiplikation)
- v)** $p(m + n) = p \cdot m + p \cdot n$ (Distributivgesetz)

Beweis.

Zu i) Sei $m = [M]$ und $n = [N]$. Zu zeigen ist $m \cdot n = n \cdot m$, also $[M \times N] = [N \times M]$. Wir müssen eine bijektive Abbildung $f : M \times N \rightarrow N \times M$ angeben. Eine solche ist aber definiert durch $(x, y) \mapsto (y, x)$.

Zu ii) Sei $m = [M]$, $n = [N]$ und $p = [P]$. Zu zeigen ist $(m \cdot n) \cdot p = m \cdot (n \cdot p)$, also $[(M \times N) \times P] = [M \times (N \times P)]$. Dies ist aber richtig, da $f : (M \times N) \times P \rightarrow M \times (N \times P)$ mit $f(((x, y), z)) = (x, (y, z))$ bijektiv ist.

Zu iii) Sei $m = [M]$. Zu zeigen ist $m \cdot 1 = m$, also $[M \times \{\emptyset\}] = [M]$. Dies gilt aber, da die Abbildung $f : M \times \{\emptyset\} \rightarrow M$ mit $f((x, \emptyset)) = x$ bijektiv ist.

Wegen iv) und v) vergleiche man wieder F.Padberg, R.Danckwerts, M.Stein, *Zahlbereiche – Eine elementare Einführung*. ■

Bemerkung. Lediglich die Streichungsregel der Multiplikation würde nicht für unendliche Kardinalzahlen gelten.

8.3 Kleinerbeziehung

Definition 8.13 Für (endliche) Kardinalzahlen m und n mit $m = [M]$ und $n = [N]$ definieren wir

$$m < n :\Leftrightarrow \text{es gibt ein } M' \subsetneq N \text{ mit } [M] = [M'].$$

Bemerkung. Für unendliche Kardinalzahlen wäre diese Definition nicht hinreichend: So gilt ja zum Beispiel $[\mathbb{N}] = [\mathbb{N} \setminus \{1\}]$. Für unendliche Kardinalzahlen muß man deshalb die Bedingung $[M] \neq [N]$ ergänzen.

Für endliche Kardinalzahlen gelten die folgenden Gesetze bezüglich der Kleinerbeziehung.

Satz 8.14 Seien m, n, p (endliche) Kardinalzahlen.

i) Es gilt stets genau eine der folgenden drei Beziehungen

$$m < n, \quad m = n, \quad n < m. \quad (\text{Trichotomie})$$

ii) Aus $m < n$ und $n < p$ folgt $m < p$. (Transitivität)

iii) $m < n \iff m + p < n + p$. (Monotoniegesetz der Addition)

iv) $m < n \iff m \cdot p < n \cdot p$. (Monotoniegesetz der Multiplikation)

(ohne Beweis)

Bemerkung. Nur die Monotoniegesetze würden nicht für unendliche Kardinalzahlen gelten.

„Wesentlich“ für die natürlichen Zahlen sind die folgenden Gesetze (Axiome):

- Assoziativgesetze der Addition und Multiplikation
- Kommutativgesetze der Addition und Multiplikation
- Gesetz vom Neutralen der Multiplikation
- Distributivgesetz
- Trichotomiegesetz
- Transitivitätsgesetz
- Monotoniegesetze der Addition und Multiplikation

Allerdings reicht das noch nicht um die natürlichen Zahlen zu charakterisieren: Es fehlt noch die sogenannte vollständige Induktion (oder ein dazu äquivalentes Prinzip). Darauf werden wir aber erst später eingehen.

9 Relationen, Äquivalenzrelation und Partitionen

9.1 Relationen

Wir wollen einige Begriffe des letzten Abschnitts noch einmal genauer ansehen und präzisieren, insbesondere werden wir das kartesische Produkt benutzen, um uns die Begriffe *Relation*, *Äquivalenzrelation* und *Funktion* noch einmal anzuschauen. Betrachten wir einige Beispiele von Relationen:

Beispiele:

- i) Geometrische Figuren in der Ebene und „ist deckungsgleich mit“.
- ii) Gewicht von Körpern und „ist schwerer als“.
- iii) Menschen und „ist älter als“ oder „ist genauso alt wie“ oder „ist mindestens so alt wie“.
- iv) Verwandtschaftsbeziehungen wie „ist Kind von“ oder „ist Mutter von“.
- v) Kleinerrelation „ $<$ “ in \mathbb{N} , \mathbb{Z} , \mathbb{Q} oder \mathbb{R} .

All diesen Beispielen ist gemeinsam, daß je zwei Elemente einer gewissen Menge zueinander in Beziehung gesetzt werden und man jeweils feststellt (bzw. feststellen kann), ob die betrachtete Beziehung gilt oder nicht. Dies kann in folgender Weise präzisiert werden.

Hierzu erinnern wir uns: Für eine Menge M ist $M \times M = \{(a, b) | a, b \in M\}$

Definition 9.1 *Unter einer Relation R in einer Menge M versteht man eine Teilmenge von $R \subset M \times M$. In dieser Festlegung gilt: $aRb \Leftrightarrow (a, b) \in R$.*

Beispiele

- i) Teilerrelation „ $|$ “ in \mathbb{N} .

$$a, b \in \mathbb{N}: a|b : \Leftrightarrow \text{Es existiert ein } n \in \mathbb{N} \text{ mit } na = b.$$

Sprich „ a teilt b “. Wir könnten auch festlegen: $| \subset \mathbb{N} \times \mathbb{N}$ enthält genau die Paare $(a, b) \in \mathbb{N} \times \mathbb{N}$, für die ein $n \in \mathbb{N}$ mit $na = b$ existiert.

Wenn wir hier als endliche Grundmenge $M = \{1, \dots, 6\}$ festlegen, und die Teilerrelation betrachten, so erhalten wir als zugehörige Menge für die Relation $a|b$:

$$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (2, 2), (2, 4), (2, 6), (3, 3), (3, 6)\}.$$

- ii) Teilerfremdheit in \mathbb{N} .

$$a, b \in \mathbb{N}: a \text{ teilerfremd } b : \Leftrightarrow \text{Es existiert kein } n \in \mathbb{N} \text{ mit } n > 1, n|a \text{ und } n|b.$$

Bei dieser Relation stellt man fest, dass die 1 zu keiner Zahl teilerfremd ist. Wenn wir diese Relation jetzt wieder auf die gleiche Menge M wie oben einschränken, so gilt

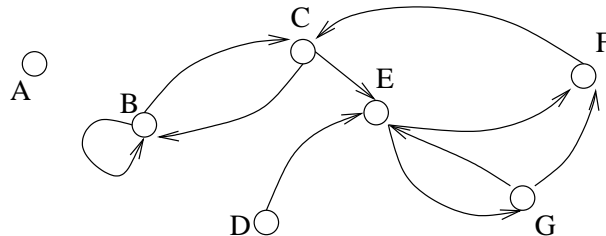
$$R = \{(2, 3), (2, 5), (3, 2), (3, 4), (3, 5), (4, 3), (4, 5), (5, 2), (5, 3), (5, 4), (5, 6), (6, 5)\}.$$

Da Relationen in einer Menge M nichts anderes als gewisse Teilmengen von $M \times M$ sind, kann man die üblichen Mengenoperationen unmittelbar auf Relationen anwenden. (Vgl. dazu A. Kirsch, *Mathematik wirklich verstehen*, S. 237–241.)

Relationen können auf verschiedene Weisen dargestellt bzw. veranschaulicht werden:

i) Pfeildiagramme: aRb entspricht einem Pfeil von a nach b .

Beispiel: $M = \{A, B, C, D, E, F, G\}$, $R = \{(B, B), (B, C), (C, B), (C, E), (F, C), (E, F), (G, F), (G, E), (E, G), (D, E)\}$



ii) Tabelle: Die Elemente von $M \times M$, d.h. die geordneten Paare $(a, b) \in M \times M$, können als Elemente einer quadratischen Tabelle aufgefaßt werden. $(a, b) \in R$ bzw. $(a, b) \notin R$ wird dann in geeigneter Weise (z.B. durch + und -) an der entsprechenden Stelle in der Tabelle notiert:

M	A	B	C	D	E	F	G
A	-	-	-	-	-	-	-
B	-	+	+	-	-	-	-
C	-	-	+	-	+	-	-
D	-	-	-	-	+	-	-
E	-	-	-	-	-	+	+
F	-	-	+	-	-	-	-
G	-	-	-	-	+	+	-

Die Anzahl möglicher Relationen bezüglich einer endlichen Menge M mit $|M| = n$ ist 2^{n^2} . Dies kann man sich zum Beispiel durch die Tabellendarstellung von Relationen klar machen: Die entsprechende quadratische Tabelle enthält Einträge für n^2 geordnete Paare. Für jeden Eintrag gibt es genau zwei Möglichkeiten: Entweder gehört ein Paar zu R oder eben nicht. Dies ergibt insgesamt 2^{n^2} Möglichkeiten.

Schon für relativ kleine n wird 2^{n^2} sehr groß. Dies zeigt, daß der Relationsbegriff sehr allgemein ist. Deshalb sind Einschränkungen sinnvoll auf

- Relationen, die inhaltlich bedeutsam sind, und/oder
- Relationen, die gewisse „schöne“ Eigenschaften besitzen.

9.2 Eigenschaften von Relationen

Betrachten wir im Sinne dieser Präzisierung noch einmal die einzelnen Eigenschaften von Äquivalenzrelationen. Sei M eine Menge und $R \subset M \times M$ eine Relation.

Reflexivität: aRa heißt: $(a, a) \in R$ für alle $a \in M$.

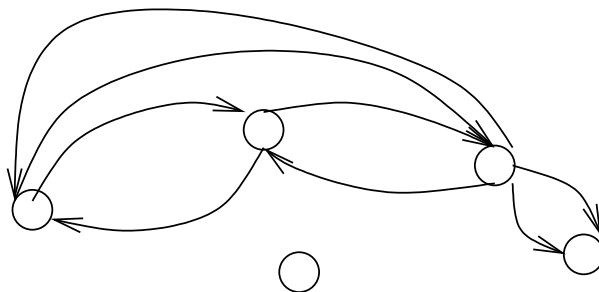
Symmetrie: $aRb \Leftrightarrow bRa$ heißt: $(a, b) \in R \Leftrightarrow (b, a) \in R$.

Transitivität: aRb und $bRc \Rightarrow aRc$ heißt: $(a, b), (b, c) \in R \Rightarrow (a, c) \in R$.

Natürlich können diese Eigenschaften auch unabhängig voneinander existieren. So sind z.B. die Relationen „|“, „ \leq “ und „gleichmächtig“ reflexiv.

Nicht alle Relationen besitzen diese Eigenschaft, insbesondere z.B. nicht „ $<$ “ oder „ist Tochter von“, oder Beispiel „ a teilerfremd mit b “. Bei einer reflexiven Relation in M besitzen alle Elemente von M Pfeile (sog. Ringpfeile) zu sich selbst. In der Tabellendarstellung kommt im Fall einer reflexiven Relation in der Diagonalen nur „+“ vor.

Bei symmetrischen Relationen sehen die Pfeildiagramme so aus:



Hier gibt es zu jedem vorhandenen Pfeil den zugehörigen Umkehrpfeil.

Beispiele. „=“, „ist im selben Raum“, „gleichmächtig“, oder „ a ist teilerfremd mit b “ besitzen diese Eigenschaft, nicht aber „ $<$ “ oder „ist Kind von“.

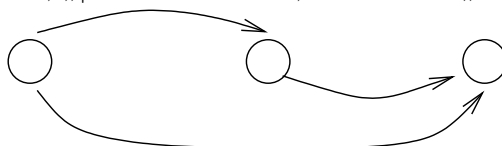
Hier kann man noch hinzufügen: Eine Relation $R \subset M \times M$ heißt **antisymmetrisch** genau dann, wenn gilt:

$$\text{Für alle } a, b \in M \text{ ist: } aRb \text{ und } bRa \implies a = b.$$

Beispiele. „ \leq “, „|“, „ \subset “ sind antisymmetrisch.

Schließlich zur letzten Eigenschaft, der Transitivität:

Beispiele. „ $<$ “, „ \leq “, „ \subset “, „|“ sind transitiv, nicht aber „ist Kind von“.



Es existieren Überbrückungspfeile.

Liegen alle drei Eigenschaften vor, so hat man eine Äquivalenzrelation. Eine Tabellendarstellung sieht z.B. so aus:

M	A	B	C	D	E	F	G
A	+	-	-	-	-	-	-
B	-	+	+	-	-	-	-
C	-	+	+	-	-	-	-
D	-	-	-	+	+	+	+
E	-	-	-	+	+	+	+
F	-	-	-	+	+	+	+
G	-	-	-	+	+	+	+

Zur Erinnerung: Äquivalenzrelationen werden in der Regel durch das Zeichen \sim (anstelle von R) ausgedrückt.

Weitere Beispiele für Relationen:

- i) Verwandtschaftsbeziehungen sind in der Regel nicht reflexiv oder symmetrisch (z.B. die Beziehung „A ist Mutter von B“.)
- ii) Die Relation „ \subset “ ist reflexiv, (wenn man damit nicht ausdrücklich \subsetneq bezeichnet) und transitiv.
- iii) Die Teilerrelation in \mathbb{N} ist reflexiv und transitiv, aber nicht symmetrisch.
- iv) Ein ähnliches Beispiel wie in 7.2 (3): Definiere in \mathbb{N} : $n \sim m \iff$ Es existiert ein $k \in \mathbb{Z}$ mit $n - m = 3k$. Mit anderen Worten: $n \in \mathbb{N}$ und $m \in \mathbb{N}$ stehen in Relation „ \sim “ zueinander, wenn sie bei Division durch 3 den gleichen Rest besitzen. Wir zeigen, daß „ \sim “ tatsächlich eine Äquivalenzrelation darstellt:

- \sim ist reflexiv, wegen $n - n = 0 \cdot 3$.
- \sim ist symmetrisch: $n - m = 3k \implies m - n = 3 \cdot (-k)$.
- \sim ist transitiv: $n - m = 3k_1$ und $m - z = 3k_2 \implies$

$$n - z = n - m + m - z = 3k_1 + 3k_2 = 3(k_1 + k_2).$$

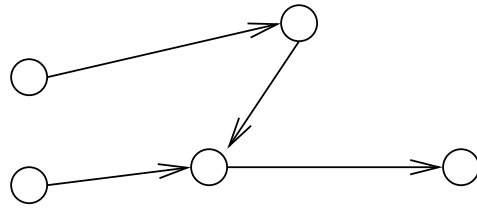
Statt $n \sim m$ schreibt man häufig auch $n = m \pmod{3}$ (Sprich: n gleich m modulo 3). Statt „3“ hätten wir auch jede andere natürliche Zahl wählen können.

Wie sieht nun eine Äquivalenzklasse aus, wenn $R \subset M \times M$ eine Äquivalenzrelation ist? $[a] = \{b \mid a \sim b\} = \{b \mid (a, b) \in R\}$. In der obigen Tabelle gibt es drei Äquivalenzklassen: $\{A\}$, $\{B, C\}$, $\{D, E, F, G\}$ Zwei weitere wichtige Typen von Relationen sind:

Definition 9.2 Eine transitive und antisymmetrische Relation nennt man **Ordnungsrelation**.

Beispiele sind „ \leq “ und „ \subset “.

Funktionen können auch als spezielle Relationen aufgefaßt werden:



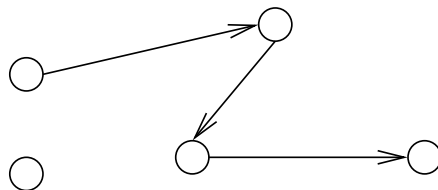
Von jedem Element in M geht genau ein Pfeil aus.

Definition 9.3 Eine Relation R in M heißt Funktion auf M , wenn für jedes $x \in M$ genau ein $y \in M$ existiert mit $(x, y) \in R$.

Insbesondere hat man bei einer Funktion folgende Implikation:

$$(x, y_1) \in R \text{ und } (x, y_2) \in R \implies y_1 = y_2.$$

Manchmal wird auch das als Definition für eine Funktion genommen.



Von jedem Element in M geht höchstens ein Pfeil aus.

Für eine Funktion f heißt dann

- $D := \{x \in M \mid \text{Es existiert } y \in M \text{ mit } (x, y) \in f\}$ Definitionsmenge von f und
- $W := \{y \in M \mid \text{Es existiert } x \in M \text{ mit } (x, y) \in f\}$ Wertemenge von f .

f heißt auch Abbildung von D in M oder von D auf W .

Bemerkung. Für eine Funktion $f : D \rightarrow W$ bezeichnet man die Menge $\{(x, y) \in M \times M \mid y = f(x)\}$ auch als den Graphen der Funktion f . Klar: Der Graph kann geometrisch interpretiert werden.

10 Darstellung von Zahlen I: Die natürlichen Zahlen und Brüche

10.1 Geschichtliche Vorbemerkung

Betrachtet man die Darstellungen von Zahlen in frühen Kulturen, so wird sehr schnell klar, dass die Arithmetik – hier im Sinne der praktischen Ausführung von Rechenoperationen – entscheidend von der Darstellung der Zahlen abhängt. Die ältesten Kulturen, die genug Material hinterlassen haben, um Rückschlüsse auf ihre Arithmetik und die entsprechenden mathematischen Fähigkeiten ziehen zu können, waren die ägyptische und die babylonische Kultur.

Die Ägypter benötigten ein ausgeprägtes Rechnungswesen: Kontrolle der Produktion, Verteilung von Einnahmen und Wirtschaftsgütern. Auch Grundkenntnisse in der Geometrie waren erforderlich: nach den Überflutungen durch den Nil musste ja jedesmal das Land neu vermessen werden. Die Zahlendarstellung der Ägypter bestand aus einem *additiven System* von Hieroglyphen zur Basis 10, d.h. es wurden unterschiedliche Symbole für 1, 10, 100, ... verwandt. Hierbei wurde jedes Symbol so oft wiederholt wie es nötig war. Da jede 10erpotenz ein eigenes Symbol besaß, war die Reihenfolge der Symbole nicht wichtig, Zahlen wurden sowohl horizontal als auch vertikal angeordnet. Allerdings beobachtet man durchaus eine Einteilung in Gruppen von Symbolen, die das „Erfassen“ der Zahlen erleichtern.

Folie (aus dem Papyros Rhind, ca 1650 vor Christus)

Die Ägypter benutzten bei ihren Rechnungen mit natürlichen Zahlen nur die Operationen Addition, Subtraktion, Verdoppeln und Halbieren. Beim Rechnen mit Brüchen benutzten sie nur Stammbrüche, also Brüche von der Form $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$ etc. Für das Addieren von Stammbrüchen gab es Tabellen. Außerdem waren sie in der Lage, $\frac{2}{3}$ eines Stammbruchs mit Hilfe der Regel

$$\frac{2}{3} \frac{1}{n} = \frac{1}{2n} + \frac{1}{6n}$$

zu ermitteln (wobei sie natürlich diese Regeln nicht so dargestellt haben!)

Folie

vergl. Peiffer, Dahan-Dalmedico: *Wege und Irrwege - Eine Geschichte der Mathematik*

Die nachfolgenden einführenden Bemerkungen zu den Babyloniern finden sich in M. Neubrand, M. Möller, *Einführung in die elementare Arithmetik*.

Etwa um 3000 v. Chr. entwickelten im sogenannten Zweistromland Mesopotamien zwischen Euphrat und Tigris die Babylonier eine Schrift einschließlich verschiedener Zahlzeichen, die auf Tontafeln geschrieben und eingebrannt wurden. Diese Entwicklung steht unter anderem im Zusammenhang mit der Entstehung von hochdifferenzierten, arbeitsteiligen, im gegenseitigen Handel stehenden Stadtkulturen. Etwa um 1800 v. Chr. bildeten sich von verschiedenen Maßsystemen unabhängige und diesem Sinne abstrakte Zahlen heraus, die durch einheitliche Schreibweisen ausgedrückt wurden.

Als Zählzeichen wurden | für 1 und < (sog. Winkelhaken) für 10 verwendet. Größere

Zahlen konnten durch Nebeneinanderschreiben ausgedrückt werden:

$$||| \text{ für } 3, \quad < ||| \text{ für } 14, \quad <<< ||| \text{ für } 33.$$

Der erste entscheidende Fortschritt bestand darin, daß dieses Nebeneinanderschreiben bei Zahlen über 60 durch eine Erhöhung des Stellenwerts ausgedrückt wird:

$$\begin{aligned} | << || & \text{ für } 1 \cdot 60 + 22 = 82, \\ ||| <<< ||| & \text{ für } 3 \cdot 60 + 34 = 214. \end{aligned}$$

Bei einem solchen System spricht man von einem *Positionssystem* oder *Stellenwertsystem*. Im Vergleich zu unserer Dezimalschreibweise fehlte allerdings eine unzweideutige Angabe der jeweiligen Position. In der babylonischen Darstellung konnte

$$< || << ||$$

sowohl $12 \cdot 60 + 22$, aber auch $12 \cdot 60^2 + 22 \cdot 60$ bedeuten. Der jeweilige Sinn musste sich aus dem jeweiligen Kontext ergeben. Übrigens wäre auch $12 + 22 \cdot \frac{1}{60}$ möglich gewesen, da ursprünglich neben dem Zeichen für die Null auch ein Zeichen *Komma* fehlte.

Immerhin ermöglichte diese Zahldarstellung ein algrithmisches, das heißt nach festen Regeln erfolgreiches, Rechnen und damit das (historisch vermutlich erstmalige) Auftreten von **Rechenzahlen**. Für die Multiplikation und die Division bediente man sich verschiedener Tafeln und Tabellen, in denen die benötigten Zwischenergebnisse aufgeschrieben waren. Neben Vielfachentafeln gab es auch sogenannte Reziprokentafeln:

2	30
3	20
4	15
⋮	⋮
8	7'30
9	6'40
⋮	⋮

Zur Interpretation dieser Tabelle:

$$\begin{aligned} \frac{1}{2} &= \frac{30}{60} \\ \frac{1}{3} &= \frac{20}{60} \\ \frac{1}{8} &= \frac{7}{60} + \frac{30}{60^2} \\ \frac{1}{9} &= \frac{6}{60} + \frac{40}{60^2} \end{aligned}$$

Dank des Positionssystems war bei den Babylonieren Rechnen nach festen (mechanischen) Regeln mittels verschiedener Tafeln einfach durchführbar. Zahlen- bzw. Rechenoperationen erschienen so als Manipulationen an Zahlenreihen.

Vertrauter sind uns noch die römischen Zahlen. Diese finden sich bei uns vor allem an historischen Gebäuden

$$I = 1, V = 5, X = 10, L = 50, C = 100, D = 500, M = 1000.$$

An der römischen Zählchrift beobachtet man eine *alternierende Fünfer-Zweier-Bündelung*, d.h. es werden abwechselnd 5 und 2 Elemente zu einer nächst höheren Einheit zusammengebunden:

$$IIIII \rightarrow V, VV \rightarrow X.$$

Charakteristisch sind ebenfalls eine additive Zusammensetzung von Zahlen, d.h.

$$XXIII = 23, DLXII = 562,$$

und die sogenannte *verminderte Zusammensetzung*, wie sie z.B. auch bei den Sumerern verwendet wurde:

$$IV = 4, XL = 40, XLVIII = 48, MIM = 1999.$$

Vergleicht man *VI* und *IV*, so sieht man: hier spielt die Reihenfolge der Zahlen schon eine Rolle, sie sind der Größe nach geordnet, und steht ein Symbol für eine kleinere Zahl vor einem Symbol einer größeren Zahl, so bedeutet dies Verminderung – die Sumerer benutzten ein eigenes zusätzliches Zeichen, (Winkelhaken) um diese Verminderung auszudrücken. Auch bei der römischen Zählchrift ist es ein Problem, dass sie in der Regel zu langen Darstellungen natürlicher Zahlen führt. Bei der römischen Zählchrift handelt es sich um kein Stellenwertsystem.

10.2 Dezimalsystem

Was bedeutet 5342? Natürlich folgendes

$$5342 = 5000 + 300 + 40 + 2 = 5 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 2 \cdot 10^0.$$

Zu dieser Interpretation kann man algorithmisch auf zwei Arten kommen:

Von links nach rechts:

$$\begin{aligned} 5342 &= \mathbf{5} \cdot 10^3 + 342 \\ 342 &= \mathbf{3} \cdot 10^2 + 42 \\ 42 &= \mathbf{4} \cdot 10 + 2 \\ 2 &= \mathbf{2} \cdot 10^0 + 0. \end{aligned}$$

Von rechts nach links:

$$\begin{aligned} 5342 &= 534 \cdot 10 + \mathbf{2} \\ 534 &= 53 \cdot 10 + \mathbf{4} \\ 53 &= 5 \cdot 10 + \mathbf{3} \\ 5 &= 0 \cdot 10 + \mathbf{5}. \end{aligned}$$

Von rechts nach links kann als fortgesetzte Division durch 10 mit Rest verstanden werden: $a = q \cdot 10 + r$ mit $0 \leq r < 10$. Auf diese Weise kann man sich auch Positionsdarstellungen bezüglich anderer Basiszahlen verschaffen. Grundlage dafür ist der folgende Satz.

Satz 10.1 Zu gegebenen $a \in \mathbb{N}_0$ und $b \in \mathbb{N}$ existieren eindeutige $q, r \in \mathbb{N}_0$ mit $a = q \cdot b + r$ und mit $0 \leq r < b$.

Beweis. Wir zeigen zunächst die Existenz geeigneter q und r . Ist $0 \leq a < b$, so gilt offensichtlich $a = 0 \cdot b + a$, also $q = 0$ und $r = a$. Für $a \geq b$ gehen wir folgendermaßen vor.

1. Schritt: $r_1 := a - b$. Ist $r_1 < b$, so gilt

$$a = 1 \cdot b + r_1$$

und wir haben die gewünschte Darstellung gefunden.

2. Schritt: $r_2 := r_1 - b = a - 2 \cdot b$. Ist $r_2 < b$, so gilt

$$a = 2 \cdot b + r_2$$

und wir haben die gewünschte Darstellung gefunden.

⋮

n .ter Schritt ($n \geq 2$): $r_n := r_{n-1} - b = a - n \cdot b$. Ist $r_n < b$, so gilt

$$a = n \cdot b + r_n$$

und wir haben die gewünschte Darstellung gefunden.

Dieser Algorithmus bricht ab, denn für hinreichend großes $n \in \mathbb{N}$ gilt

$$r_n = a - n \cdot b < b.$$

Wegen $r_{n-1} \geq b$ ist r_n im übrigen nicht negativ.

Zur Eindeutigkeit: Für $q_i, r_i \in \mathbb{N}_0$ ($i = 1, 2$) mit $0 \leq r_i < b$ gelte

$$a = q_1 \cdot b + r_1, \quad a = q_2 \cdot b + r_2.$$

O.B.d.A. sei $q_1 \geq q_2$. Wir bilden die Differenz und erhalten so

$$0 = (q_1 - q_2) \cdot b + (r_1 - r_2) \text{ und } r_2 = (q_1 - q_2) \cdot b + r_1.$$

Angenommen, es gilt $q_1 > q_2$. Dann folgt aus der letzten Identität wegen $q_1 - q_2 \geq 1$ und $r_1 \geq 0$, daß $r_2 \geq b$ ist, im Widerspruch zur Voraussetzung $r_2 < b$. Also muß $q_1 = q_2$ sein, woraus sofort auch $r_1 = r_2$ folgt. ■

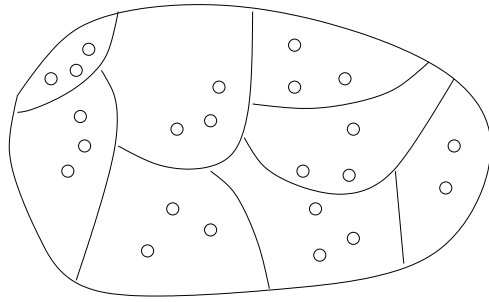
Die Bestimmung von q und r ist verbunden mit der Vorstellung einer Menge, die a Elemente enthält. Es werden jeweils (in jedem Schritt) b Elemente zu einem Bündel zusammengefaßt, bis das nicht mehr geht, also keine b Elemente mehr übrig sind. Die Anzahl der Bündel aus b Elementen ergibt q und $0 \leq r < b$ Elemente bleiben übrig.

Wir wenden den Satz 10.1 nun an, um einen ersten Darstellungssatz für natürliche Zahlen bezüglich der Basiszahl $b = 10$ zu beweisen.

Satz 10.2 Jede natürliche Zahl $a \in \mathbb{N}$ läßt sich eindeutig in der Form

$$a = z_n \cdot 10^n + z_{n-1} \cdot 10^{n-1} + \dots + z_1 \cdot 10^1 + z_0 \cdot 10^0$$

mit $z_i \in \{0, 1, 2, \dots, 9\}$ für $i = 0, 1, 2, \dots, n$ und $z_n \neq 0$ darstellen.



$a=23, b=3, q=7, r=2$

Beweis. Wir gehen wieder algorithmisch vor um die Existenz einer solchen Darstellung zu beweisen.

0. Schritt: Bestimme $n \in \mathbb{N}_0$ so, daß gilt

$$10^{n+1} > a \geq 10^n.$$

1. Schritt: Division durch 10^n mit Rest führt dann auf

$$a = z_n \cdot 10^n + r_{n-1} \quad \text{mit } z_n \in \{1, 2, \dots, 9\} \text{ und } 0 \leq r_{n-1} < 10^n.$$

2. Schritt: Division durch 10^{n-1} mit Rest führt auf

$$r_{n-1} = z_{n-1} \cdot 10^{n-1} + r_{n-2} \quad \text{mit } z_{n-1} \in \{0, 1, 2, \dots, 9\} \text{ und } 0 \leq r_{n-2} < 10^{n-1}.$$

⋮

n. Schritt: Division durch $10 = 10^1$ mit Rest führt auf

$$r_1 = z_1 \cdot 10 + z_0 \quad \text{mit } z_0, z_1 \in \{0, 1, 2, \dots, 9\}.$$

Zusammenfassend ergibt sich

$$\begin{aligned} a &= z_n \cdot 10^n + r_{n-1} \\ &= z_n \cdot 10^n + z_{n-1} \cdot 10^{n-1} + r_{n-2} \\ &\quad \vdots \\ &= z_n \cdot 10^n + z_{n-1} \cdot 10^{n-1} + \dots + z_1 \cdot 10^1 + z_0 \cdot 10^0. \end{aligned}$$

Zur Eindeutigkeit: Es gelte für $z_i, y_i \in \{0, 1, 2, \dots, 9\}$ mit $z_n \neq 0, y_m \neq 0$

$$a = \sum_{i=0}^n z_i \cdot 10^i = \sum_{i=0}^m y_i \cdot 10^i.$$

O.B.d.A. sei $n \leq m$. Angenommen es ist $n < m$. Wegen

$$\sum_{i=0}^n z_i \cdot 10^i \leq \sum_{i=0}^n 9 \cdot 10^i < 10^{n+1}$$

und

$$\sum_{i=0}^m y_i \cdot 10^i \geq 10^m \geq 10^{n+1}$$

gilt dann

$$a = \sum_{i=0}^n z_i \cdot 10^i < \sum_{i=0}^m y_i \cdot 10^i = a.$$

Widerspruch. Also ist $n = m$.

O.B.d.A. gelte nun $z_n \geq y_n$. Angenommen es ist $z_n > y_n$. Dann folgt aus

$$\sum_{i=0}^{n-1} y_i \cdot 10^i = (z_n - y_n) \cdot 10^n + \sum_{i=0}^{n-1} z_i \cdot 10^i$$

zum einen

$$\sum_{i=0}^{n-1} y_i \cdot 10^i > 10^n$$

und zum anderen ist aber

$$\sum_{i=0}^{n-1} y_i \cdot 10^i < 10^n.$$

Widerspruch. Also muss $z_n = y_n$ sein und ferner

$$(z_{n-1} - y_{n-1}) \cdot 10^{n-1} + \sum_{i=0}^{n-2} (z_i - y_i) \cdot 10^i = 0$$

gelten. Sukzessive Wiederholung dieses Arguments liefert $z_i = y_i$ für $i = 0, 1, 2, \dots, n$. ■

Bemerkung. Auf den ersten Blick mag Satz 10.2 überflüssig erscheinen. Schließlich wissen wir ja, daß sich z.B. die natürliche Zahl 5342 eindeutig in der Form $5 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 2 \cdot 10^0$ schreiben läßt. Der Satz ist aber in anderer Weise zu interpretieren: 5342 ist nichts anderes als eine verkürzte Schreibweise der Zehnerdarstellung, und der Satz weist nach, daß sich tatsächlich jede natürliche Zahl (z.B. eingeführt als Kardinalzahl) tatsächlich so schreiben läßt. Man muß hier also klar zwischen Zahlen und ihrer Darstellung unterscheiden.

Bemerkung. Der Algorithmus im Beweis des Satzes 10.2 entspricht dem Vorgehen *von links nach rechts*. Äquivalent dazu hätte man auch einem Vorgehen *von rechts nach links* folgen können. Die von letzterem Vorgehen nahegelegte Darstellung besitzt die Gestalt

$$a = (\dots((z_n \cdot 10 + z_{n-1}) \cdot 10 + \dots + z_1) \cdot 10 + z_0 \tag{10.4}$$

und kann unmittelbar aus der anderen Darstellung durch geschicktes *Klammern* gewonnen werden. Für die *Praxis* besitzt (10.4) den Vorteil, daß man nicht erst n bestimmen muß sondern gleich mit der Division durch 10 und Restbestimmung z_0 beginnen kann. Dieser Unterschied spielt für Zahlen, die im Dezimalsystem gegeben sind und deren Zehnerdarstellung gesucht ist, natürlich keine große Rolle, da wir in diesem Fall das n direkt ablesen können. Dies ist aber anders, wenn man eine Zahl aus dem Dezimalsystem in ein Stellenwertsystem bezüglich einer anderen Basiszahl b umrechnen möchte.

Von zentraler Bedeutung ist ferner, daß in einem Stellenwertsystem jedes Zeichen (jede Ziffer) zwei Informationen überliefert:

1. Zahlenwert (also im Dezimalsystem $z_i \in \{0, 1, 2, \dots, 9\}$) und
2. Stellenwert oder Position (d.h. das i in z_i bzw. in 10^i).

Beispiel. Die 1 in 100 zeigt an 1×100 . Die 1 in 2010 zeigt an 1×10 .

Bemerkung Eine sehr anschauliche Beschreibung von Stellenwertsystemen findet sich in dem Buch von Enzensberger: Der Zahlenteufel (speziell die zweite Nacht). Die heutigen Zahlzeichen, die allgemein als arabische Ziffern bezeichnet werden, stammen ursprünglich aus Indien. (vergl. Ch. Seife, Zwilling der Unendlichkeit, p. 79)

10.3 Stellenwertsysteme zur Basis $b \in \mathbb{N}$ mit $b \neq 1$

Beispiel. Sechzersystem: Wir unterscheiden wieder von rechts nach links:

$$\begin{aligned} 112 &= 18 \cdot 6 + 4 \\ 18 &= 3 \cdot 6 + 0 \\ 3 &= 0 \cdot 6 + 3, \end{aligned}$$

und

von links nach rechts:

$$\begin{aligned} 112 &= 3 \cdot 6^2 + 4 \\ 4 &= 0 \cdot 6^1 + 4 \\ 4 &= 4 \cdot 6^0. \end{aligned}$$

Beide Vorgehensweisen liefern $112 = 3 \cdot 6^2 + 0 \cdot 6^1 + 4 \cdot 6^0$. Das Vorgehen *von rechts nach links* hat den Vorteil, daß man nicht vorab $n = 2$ bestimmen muß. Abkürzend schreibt man statt $3 \cdot 6^2 + 0 \cdot 6^1 + 4 \cdot 6^0$ auch $(304)_6$.

Allgemein gilt nun folgender Satz.

Satz 10.3 Zu gegebenen $a, b \in \mathbb{N}$ ($b \neq 1$) existieren eindeutige Zahlen $n \in \mathbb{N}$ und $z_i \in \{0, 1, 2, \dots, b-1\}$, $i = 0, 1, 2, \dots, n$, $z_n \neq 0$ mit

$$a = z_n \cdot b^n + z_{n-1} \cdot b^{n-1} + \dots + z_1 \cdot b^1 + z_0 \cdot b^0.$$

Beweis. Analog zum entsprechenden Resultat für $b = 10$ mittels Division bezüglich b mit Rest. ■

Definition 10.4 Gegeben seien $a, b \in \mathbb{N}$ mit $b \neq 1$. Für die Darstellung $a = z_n \cdot b^n + z_{n-1} \cdot b^{n-1} + \dots + z_1 \cdot b^1 + z_0$ (entsprechend Satz 10.3) schreibt man

$$a = (z_n z_{n-1} \dots z_1 z_0)_b$$

und nennt das die Darstellung von a im b -adischen System (oder im Stellenwertsystem zur Basis b) mit den Ziffern $z_n, z_{n-1}, \dots, z_1, z_0$.

Beispiele.

i) $350 = (1342)_6$:

$$350 = 58 \cdot 6 + 2$$

$$58 = 9 \cdot 6 + 4$$

$$9 = 1 \cdot 6 + 3$$

$$1 = 0 \cdot 6 + 1.$$

ii) $25 = (11001)_2 = (121)_4 = (31)_8 = (21)_{12}$:

$$25 = 12 \cdot 2 + 1$$

$$12 = 6 \cdot 2 + 0$$

$$6 = 3 \cdot 2 + 0$$

$$3 = 2 \cdot 1 + 1$$

$$1 = 0 \cdot 2 + 1$$

$$25 = 6 \cdot 4 + 1$$

$$6 = 1 \cdot 4 + 2$$

$$1 = 0 \cdot 4 + 1$$

$$25 = 3 \cdot 8 + 1$$

$$3 = 0 \cdot 8 + 3$$

$$25 = 2 \cdot 12 + 1$$

$$2 = 0 \cdot 12 + 2$$

iii) $(1342)_6 = 350$:

$$1 \cdot 6^3 + 3 \cdot 6^2 + 3 \cdot 6 + 2 = 350.$$

Geschickter ist es so zu rechnen:

$$(((1 \cdot 6) + 3) \cdot 6 + 4) \cdot 6 + 2 = 350,$$

bzw. in Tabellenform

0	1·6	9·6=54	58·6=348
1	3	4	2
1	6+3=9	54+4=58	348+2=350.

Das geht für einen allgemeinen Ausdruck der Gestalt (10.4) völlig analog und heißt Horner-Schema. Der Vorteil dieses Schemas ist, daß dabei wesentlich weniger Multiplikationen auszuführen sind. Dies ist vor allem für *große* Stellenzahlen von Bedeutung. In unserem Beispiel fallen bei der ersten Berechnungsart $3 + 2 + 1 = 6$ Multiplikationen an und bei der zweiten Art lediglich 3.

10.4 Dezimalbrüche

Bevor wir im nächsten Abschnitt auf das Rechnen in Stellenwertsystemen (und damit auf das schriftliche Rechnen) eingehen, soll noch gezeigt werden, wie Brüche im Dezimalsystem dargestellt werden können.

Beispiel. Gegeben sei die Zahl 0.1734. Die einzelnen Stellen nach dem Komma erhalten wir durch folgendes Vorgehen:

$$\begin{aligned}0.1734 \cdot 10 &= \mathbf{1} + 0.734 \\0.734 \cdot 10 &= \mathbf{7} + 0.34 \\0.34 \cdot 10 &= \mathbf{3} + 0.4 \\0.4 \cdot 10 &= \mathbf{4} + 0.\end{aligned}$$

Jede Multiplikation mit 10 verschiebt sozusagen das Komma um eine Stelle nach rechts und liefert einen ganzzahligen Anteil, der auch 0 sein kann, und eventuell einen Rest, der wieder zwischen 0 und 1 liegt.

Im allgemeinen Fall, also für beliebiges aber fest gewähltes $0 < \alpha < 1$, läßt sich dieser Algorithmus folgendermaßen formulieren:

$$\begin{aligned}\alpha \cdot 10 &= y_1 + \alpha_1 \text{ mit } y_1 \in \{0, 1, \dots, 9\} \text{ und } 0 \leq \alpha_1 < 1 \\ \alpha_1 \cdot 10 &= y_2 + \alpha_2 \text{ mit } y_2 \in \{0, 1, \dots, 9\} \text{ und } 0 \leq \alpha_2 < 1 \\ &\vdots \\ \alpha_n \cdot 10 &= y_{n+1} + \alpha_{n+1} \text{ mit } y_{n+1} \in \{0, 1, \dots, 9\} \text{ und } 0 \leq \alpha_{n+1} < 1. \\ &\vdots\end{aligned}$$

Der Algorithmus bricht ab, wenn $\alpha_n = 0$ ist. Dies muss aber im allgemeinen nicht passieren, d.h. der Algorithmus liefert im allgemeinen eine nicht abbrechende Folge von Ziffern y_i , das ist ein entscheidender Unterschied zu ganzen Zahlen! Dieses Verfahren von oben kann man beliebig lange fortführen, und es gilt für alle Zahlen $\alpha \in (0, 1)$ der folgende Satz:

Satz 10.5 *Jede Zahl $0 < \alpha < 1$ besitzt eine Darstellung als Dezimalbruch (eine Dezimalbruchentwicklung)*

$$\alpha = y_1 \cdot 10^{-1} + y_2 \cdot 10^{-2} + y_3 \cdot 10^{-3} + \dots$$

mit $y_i \in \{0, 1, 2, \dots, 9\}$ für $i \in \mathbb{N}$.

Bemerkung. Meist schreiben wir $\alpha = 0, y_1 y_2 y_3 \dots$.

Ist jetzt α ein Bruch, d.h. $\alpha = \frac{p}{q}$ mit $p, q \in \mathbb{N}$, dann können diese y_i nicht beliebig variieren, sondern es gilt der folgende Satz:

Satz 10.6 Für $0 < \alpha < 1$, $\alpha \in \mathbb{Q}$, ist die Dezimalbruchentwicklung entweder endlich oder periodisch, d.h. für $\alpha = 0.y_1y_2y_3 \cdots y_i \cdots$ gilt: ab einem geeigneten Index k ist $y_i = y_{i+m}$ mit einem geeigneten m . Wir schreiben dann:

$$\alpha = 0.y_1y_2 \cdots y_k \overline{y_{k+1} \cdots y_{k+m}}$$

Sowohl k (Anzahl der Ziffern nach dem Komma, aber vor der Periode) als auch m (die Länge der Ziffernfolge in der Periode) müssen $\leq q - 1$ sein.

Beweis. Hierzu wenden wir den obigen Algorithmus in leicht veränderter Form an, wir multiplizieren alle auftretenden Gleichungen mit dem Nenner des Bruches, dadurch müssen wir nur in den natürlichen Zahlen denken:

1. Schritt $\frac{p}{q} \cdot 10 = y_1 + \alpha_1$ mit $y_1 \in \{0, 1, \dots, 9\}$, $0 \leq \alpha_1 < 1$. Wegen $p \cdot 10 = y_1 \cdot q + \alpha_1 \cdot q$ muß gelten $p_1 := \alpha_1 \cdot q \in \mathbb{N}_0$.

2. Schritt $p_1 \cdot 10 = y_2 \cdot q + p_2$ mit $y_2 \in \{0, 1, \dots, 9\}$ und $p_2 = \alpha_2 \cdot q \in \mathbb{N}_0$.

⋮

n. Schritt $p_{n-1} \cdot 10 = y_n \cdot q + p_n$ mit $y_n \in \{0, 1, \dots, 9\}$ und $p_n = \alpha_n \cdot q \in \mathbb{N}_0$,

Wir können nun zwei Fälle unterscheiden:

i) Entweder gilt: Irgendwann ist $p_n = 0$. Dann haben wir

$$\frac{p}{q} = y_1 \cdot 10^{-1} + y_2 \cdot 10^{-2} + \cdots + y_n \cdot 10^{-n} = 0.y_1y_2 \cdots y_n.$$

Es liegt also eine endliche Dezimalbruchentwicklung vor.

ii) Oder wir haben ein j mit $p_j = p_k (\neq 0)$ für ein k mit $1 \leq k < j$. Da wegen $0 \leq \alpha_j \leq 1$ auch $0 \leq p_j < q$ gilt, muss dies (wenn keine Null auftritt) spätestens im q -ten Schritt der Fall sein, da es nur $q - 1$ von Null verschiedene positive ganze Zahlen kleiner als q gibt. Damit gilt $k \leq q - 1$ und $m = j - k \leq q - 1$. Danach wiederholt sich dann der Algorithmus und damit die sich ergebende Ziffernfolge.

Beispiele.

i) $\frac{1}{8} = 0.125$.

ii) $\frac{1}{7} = 0.142857142857 \cdots = 0.\overline{142857}$

iii) $\frac{5}{19} = 0.\overline{263157894736842105}$.

iv) $\frac{5}{14} = 0.3\overline{571428}$

Bemerkung. $y_n = y_j$ für ein $j < n$, also gleiche Ziffern, ist nicht hinreichend dafür, daß sich die jeweils nachfolgenden Ziffern ebenfalls wiederholen, das sieht man schon an den Beispielen oben. Ausserdem gibt es Brüche mit beliebig langen (endlichen) periodischen Dezimalbruchentwicklungen, dies sieht man insbesondere auch aus den folgenden Überlegungen.

Die naheliegende Frage ist natürlich: Wie kommt man zurück? Hierzu überlegen wir uns: Jeder periodische Dezimalbruch läßt sich in der Form $\frac{p}{q}$, $p, q \in \mathbb{N}$, schreiben.

Dazu zunächst einige **Beispiele**:

i) $0.173 = \frac{173}{1000}$. So geht das natürlich für jede Zahl mit endlicher Dezimalbruchentwicklung.

$$0.y_1y_2 \cdots y_n = \frac{y_1y_2 \cdots y_n}{10^n}$$

ii) $0.\overline{173}$:

$$999 \cdot 0.\overline{173} = 1000 \cdot 0.\overline{173} - 0.\overline{173} = 173.\overline{173} - 0.\overline{173} = 173,$$

also

$$0.\overline{173} = \frac{173}{999}.$$

$0.1\overline{73}$:

$$990 \cdot 0.1\overline{73} = 1000 \cdot 0.1\overline{73} - 10 \cdot 0.1\overline{73} = 173.\overline{73} - 1.\overline{73} = 172,$$

also

$$0.1\overline{73} = \frac{172}{990}.$$

Auch hier kann man das für jeden anderen periodischen Dezimalbruch systematisch ausdrücken.

Satz 10.7 *Haben wir eine Zahl $\alpha \in (0, 1)$ mit periodischer Dezimalbruchentwicklung, so gilt für $\alpha = 0.y_1y_2 \cdots y_k\overline{y_{k+1} \cdots y_{k+m}}$:*

$$\alpha = \frac{y_1y_2 \cdots y_k y_{k+1} \cdots y_{k+m} - y_1y_2 \cdots y_k}{10^k(10^m - 1)}$$

Beweis: Sei $\alpha = 0.y_1 \cdots y_k \overline{y_{k+1} \cdots y_{k+m}}$, multiplizieren mit 10^{k+m} (verschiebe das Komma hinter die erste Periode) liefert:

$$10^{k+m}\alpha = y_1 \cdots y_k y_{k+1} \cdots y_{k+m}, \overline{y_{k+1} \cdots y_{k+m}}.$$

Multiplizieren mit 10^k (verschiebe das Komma vor die erste Periode) liefert:

$$10^m\alpha = y_1 \cdots y_k \cdot \overline{y_{k+1} \cdots y_{k+m}}.$$

Subtrahieren:

$$\begin{aligned} 10^{k+m}\alpha - 10^m\alpha &= y_1 \cdots y_k y_{k+1} \cdots y_{k+m}, \overline{y_{k+1} \cdots y_{k+m}} - y_1 \cdots y_k, \overline{y_{k+1} \cdots y_{k+m}} \\ &= y_1 \cdots y_k y_{k+1} \cdots y_{k+m} - y_1 \cdots y_k, \quad \Rightarrow \\ \alpha &= \frac{y_1 \cdots y_k y_{k+1} \cdots y_{k+m} - y_1 \cdots y_k}{10^k(10^m - 1)}. \end{aligned}$$

■

Man sich also Dezimalbrüche mit beliebig langer Periode vorgeben, und dann zurückrechnen. Aus dem Beweis der vorigen Satzes weiss man sogar, wie groß der Nenner mindestens ist, selbst nach Kürzen.

Eine besondere Situation liegt für Dezimalbrüche mit Neunerende vor:

$0.\bar{9}$:

$$9 \cdot 0.\bar{9} = 10 \cdot 0.\bar{9} - 0.\bar{9} = 9.\bar{9} - 0.\bar{9} = 9,$$

also

$$0.\bar{9} = \frac{9}{9} = 1.$$

$0.8\bar{9}$:

$$90 \cdot 0.8\bar{9} = 100 \cdot 0.8\bar{9} - 10 \cdot 0.8\bar{9} = 89.\bar{9} - 8.\bar{9} = 81,$$

also

$$0.8\bar{9} = \frac{81}{90} = \frac{9}{10} = 0.9.$$

Dies geht offenbar immer so. Interessant ist davon wiederum die Umkehrung: Starten wir mit einem Bruch natürlicher Zahlen, so wird durch unseren obigen Algorithmus offenbar kein Neunerende produziert. Z.B. liefert $\frac{9}{10}$ den Dezimalbruch 0.9 und nicht $0.8\bar{9}$.

10.5 Darstellungen von Rechnungen in Stellenwertsystemen

Die zu Beginn dieses Abschnittes beschriebenen additiven Zahlendarstellungen der alten Kulturen eigneten sich nicht sehr gut zum „Kopfrechnen“. Daher wurden mechanische Hilfsmittel benutzt, z. B. Rechenbretter oder der von den Babyloniern erfundene Abakus. Die indische Mathematik stand zunächst unter dem Einfluss griechischer, ägyptischer und babylonischer Mathematik, die durch Alexander dem Großen bei seinen Feldzügen mit nach Indien gebracht worden waren. Es ist nicht genau bekannt, wann sie zu einem Positionssystem mit Basis 10, also dem heutigen Dezimalsystem übergingen, die ältesten Quellen darüber sind aus dem 7. Jahrhundert, und sie entwickelten die bis heute gelehrt Techniken des schriftlichen Rechnens (bei den vier Grundrechenarten), sie begannen auch die 0 als Zahl zu benutzen, nicht nur als Platzhalter für nicht vorhandene Potenzen der Zahl 10 oder 60, wie es die Babylonier taten. Dies hat vor allem philosophische Gründe: Die stark von den Philosophen der Griechen, insbesondere Aristoteles, beeinflussten christlichen Weltanschauung war vor der Angst vor dem Nichts – und vor dem Unendlichen – beherrscht. Diese Angst war den Hindus fremd, im Gegenteil: das Nichts wieder zu erlangen, aus dem die Welt erschaffen worden war, war das höchste Ziel. Die Araber, die allen neuen Kenntnissen in den Wissenschaften sehr aufgeschlossen waren, übernahmen die Zahlendarstellung und Rechentechniken der Inder und brachten sie nach Europa mit. Besonders populär wurden die Abhandlungen des berühmten Al-Hwarizmi (ca 800 - 850), aus dessen Namen sich unser Wort Algorithmus ableitet.

Wir beschreiben das Rechnen in Stellenwertsystemen am Beispiel des Fünfersystems. In anderen Stellenwertsystemen geht man im wesentlichen analog vor. Kurze Bemerkungen zu allgemeinen Stellenwertsystemen ergänzen die Darstellung.

10.5.1 Addition

Was ergibt $(424)_5 + (111)_5$? $(424)_5$ ist nichts anderes als $4 \cdot 5^2 + 2 \cdot 5^1 + 4 \cdot 5^0$, $(111)_5$ bedeutet $1 \cdot 5^2 + 1 \cdot 5^1 + 1 \cdot 5^0$. Wir beschreiben das (systematische) Vorgehen bei der

Addition zunächst mit Hilfe sogenannter Plättchenmengen. Dabei werden Plättchen für die jeweiligen Ziffern in verschiedene Spalten entsprechend der Wertigkeit der Ziffern gelegt. Plättchen der gleichen Wertigkeit werden dann zusammengefaßt. Abschließend

5^3	5^2	5^1	5^0
	<div style="border: 1px solid black; padding: 2px; display: inline-block;"> ● ● ● ● ○ </div>	● ● ○ ○	<div style="border: 1px solid black; padding: 2px; display: inline-block;"> ● ● ● ● ○ </div>
○		○	
●		● ● ● ●	

wird darauf geachtet, daß sich in keiner Spalte mehr als 4 Plättchen befinden. Ergeben sich beim Zusammenfassen mehr als 4 Plättchen, werden 5 Plättchen *gebündelt* und durch ein Plättchen in der nächsten Spalte (der Spalte der nächst höheren Wertigkeit) ersetzt.

Für das (formalere) schriftliche Rechnen erweist sich eine (vorab erstellte) 1 + 1-Tafel als hilfreich:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	10
2	2	3	4	10	11
3	3	4	10	11	12
4	4	10	11	12	13

Diese berücksichtigend erhalten wir analog zu unserem Vorgehen mit den Plättchen

$$\begin{array}{r}
 4 \ 2 \ 4 \\
 + \quad 1 \ 1 \ 1 \\
 \hline
 1 \quad 1 \\
 \hline
 1 \ 0 \ 4 \ 0
 \end{array}$$

Dabei rechnen wir (stellenweise von rechts nach links) folgendermaßen:

- i) $4 + 1 = 10$; 0 wird als Ergebnis notiert und die 1 in der nächsten Spalte festgehalten.
- ii) $2 + 1 + 1 = 4$.
- iii) $4 + 1 = 10$, nun weiter wie bei i).
- iv) $0 + 1 = 1$.

Formal könnte man das Vorgehen in der i -ten Spalten so beschreiben:

- i) $z_i \cdot b^i + y_i \cdot b^i = (z_i + y_i) \cdot b^i$
- ii) Falls $z_i + y_i < b$ ist, so lautet das Ergebnis $e_i = z_i + y_i$.
- iii) Falls $z_i + y_i > b$ ist, so lautet das Ergebnis für die i -te Spalte $e_i = z_i + y_i - b$. Zusätzlich ist in der Rechnung der $i + 1$ -ten Spalte $+1 \cdot b^{i+1}$ zu berücksichtigen.

10.5.2 Subtraktion

Zunächst eine Erinnerung an einige Fachbegriffe bei der Subtraktion: In der Gleichung $a - b = c$ heißt a der **Minuend** (lat.: das zu verkleinernde), die Zahl b ist der **Subtrahend** (lat.: das abzuziehende), das Ergebnis c ist die **Differenz**. Die Differenz $(12)_5 - (4)_5$ können wir auf zwei verschiedene Weisen interpretieren

- als *Wegnehmen*, bzw. *Abziehen*: $(12)_5 - (4)_5 = (3)_5$;
- als *Ergänzen*: $(4)_5 + \square = (12)_5$.

Bei beiden Interpretationen ist ein Blick auf die 1 + 1-Tafel hilfreich. Welche der beiden Interpretationen *günstiger* ist, hängt dabei unter anderem von den vorgegebenen Zahlen ab.

- Bei $(1010)_5 - (43)_5 = (412)_5$ liegt die Interpretation *Ergänzen* näher.
- Bei $(433)_5 - (122)_5 = (311)_5$ liegt die Interpretation *Abziehen* näher.

Seit 1958 war durch KMK-Beschluß das Ergänzungsverfahren als Normalverfahren in der Schule vorgeschrieben, dieser Beschluss ist seit kurzem aufgehoben. Beim Ergänzungsverfahren lassen sich drei verschiedene Übertragungstechniken unterscheiden.

i) **Borgetechnik**: Wir beschreiben diese Technik am Beispiel der Aufgabe $(132)_5 - (14)_5$. Bei der Borgetechnik wird im Minuend eine Einheit des nächsthöheren Stellenwertes

5^3	5^2	5^1	5^0
	●	● ● □	● ● ● ● ● ● ● ●
		○	○ ○ ○ ○
	●	●	● ● ●

entbündelt. Steht an dieser Stelle des Minuenden jedoch eine Null, muss man den davor stehenden Stellenwert entbündeln etc. Beim schriftlichen Rechnen notiert man z.B. folgendes

$$\begin{array}{r}
 1 \ 3' \ 2 \\
 - \quad 1 \ 4 \\
 \hline
 1 \ 1 \ 3
 \end{array}$$

Statt $3'$ wird manchmal auch 3^1 geschrieben.

ii) **Erweiterungstechnik:** Wir beschreiben diese Technik wieder am Beispiel der Aufgabe $(132)_5 - (14)_5$:

5^3	5^2	5^1	5^0
	●	● ● ●	● ● ● ● ● ● ●
		○ □	○ ○ ○ ○
	●	●	● ● ●

Die Erweiterungstechnik darauf, daß die Differenz konstant bleibt, wenn zum Minuenden und Subtrahenden dieselbe Zahl addiert bzw. subtrahiert wird:

$$x - y = x - a + a - y = (x + a) - (y + a).$$

Schriftlich ergibt sich folgendes Bild:

$$\begin{array}{r} 1 \ 3 \ 2 \\ - \quad 1_1 \ 4 \\ \hline 1 \ 1 \ 3 \end{array}$$

iii) **Auffülltechnik:** Auch diese Technik beschreiben wir am Beispiel der Aufgabe $(132)_5 - (14)_5$: Bei dieser Technik wird der Minuend überhaupt nicht verändert. Ist in einer Spalte ein Übertrag erforderlich, so wird der Subtrahend zunächst auf die nächsthöhere Einheit aufgefüllt (im Beispiel um 1 auf 5) und diese Einheit in der nächsthöheren Stellenwertspalte notiert. Dann füllen wir das Zwischenergebnis bis zur Anzahl der Einheiten des Minuenden auf. Die Grundlage dieser Technik besteht darin, $(132)_5 - (14)_5$ in $(132)_5 = (14)_5 + \square$ umzudrehen. Schriftlich ergibt sich das gleiche Bild wie bei der Erweiterungstechnik.

5^3	5^2	5^1	5^0
	●	● ● ●	● ●
		○ ○ ←	○ ○ ○ ○
	●	●	● ●

Formal könnte man das Vorgehen bei der Subtraktion im b-adischen System bezüglich der i-ten Spalte, also $z_i \cdot b^i + \square = y_i \cdot b^i$, so beschreiben:

- i) Falls $z_i \geq b_i$ ist, so lautet das Ergebnis $e_i = z_i - y_i$.
- ii) Falls $z_i < y_i$ ist, so lautet das Ergebnis für die i-te Spalte $e_i = z_i + b - y_i$. Zusätzlich ist in der Rechnung der $i + 1$ -ten Spalte $-1 \cdot b^{i+1}$ zu berücksichtigen.

10.5.3 Multiplikation

Die Multiplikation beruht im wesentlichen auf einer Anwendung des Distributivgesetzes und einer Rückführung auf *einstellige* Multiplikationen. Diese kann man in einer 1×1 -Tafel zusammenfassen:

\times	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	11	13
3	0	3	11	14	22
4	0	4	13	22	31

Was ergibt nun z.B. $(431)_5 \cdot (23)_5$?

$$\begin{aligned}
& (431)_5 \cdot (23)_5 \\
&= (4 \cdot 5^2 + 3 \cdot 5 + 1) \cdot (2 \cdot 5 + 3) \\
&= (4 \cdot 2) \cdot 5^3 + (3 \cdot 2) \cdot 5^2 + (1 \cdot 2) \cdot 5 + (4 \cdot 3) \cdot 5^2 + (3 \cdot 3) \cdot 5 + 1 \cdot 3 \\
&= (1 \cdot 5 + 3) \cdot 5^3 + (1 \cdot 5 + 1) \cdot 5^2 + 2 \cdot 5 + (2 \cdot 5 + 2) \cdot 5^2 + (1 \cdot 5 + 4) \cdot 5 + 3 \\
&= 1 \cdot 5^4 + (3 + 1 + 2) \cdot 5^3 + (1 + 2 + 1) \cdot 5^2 + (2 + 4) \cdot 5 + 3 \\
&= 1 \cdot 5^4 + (1 \cdot 5 + 1) \cdot 5^3 + 4 \cdot 5^2 + (1 \cdot 5 + 1) \cdot 5 + 3 \\
&= 2 \cdot 5^4 + 1 \cdot 5^3 + (4 + 1) \cdot 5^2 + 1 \cdot 5 + 3 \\
&= 2 \cdot 5^4 + 2 \cdot 5^3 + 0 \cdot 5^2 + 1 \cdot 5 + 3 \\
&= (22013)_5.
\end{aligned}$$

An dieser ausführlichen Rechnung wird deutlich, daß es sich bei der Multiplikation um eine im Vergleich zur Addition wesentlich komplexere Operation handelt. Es ist deshalb nicht erstaunlich, daß es zum eben beschriebenen Verfahren im Dezimalsystem alternative Vorgehensweisen gibt wie z.B. das Verdopplungsverfahren (man erinnere sich an die Ägypter). Mit diesem läßt sich im übrigen (mit einiger Übung) genauso schnell rechnen wie mit dem (in unserer Kultur) üblichen Verfahren.

Bei der schriftlichen Rechnung (also der Kurzschreibweise des obigen Vorgehens) ist eine sorgfältige und stellengerechte Notation wichtig:

$$\begin{array}{r}
 4 \ 3 \ 1 \cdot 2 \ 3 \\
 \hline
 1 \ 4 \ 1 \ 2 \\
 2 \ 3 \ 4 \ 3 \\
 \hline
 2 \ 2 \ 0 \ 1 \ 3
 \end{array}$$

10.5.4 Division

Die Division ist noch komplexer als die Multiplikation. Man vergleiche dazu etwa das in F. Padberg, *Didaktik der Arithmetik*, auf Seite 232 abgedruckte Flußdiagramm für das systematische Vorgehen bei der Division.

Wir beschränken uns hier zum einen darauf zu bemerken, daß eine (vorab erstellte) 1×1 -Tafel wieder sehr hilfreich ist und zum anderen mit einem Beispiel im Fünfersystem: Was ergibt $(4242)_5 : (23)_5$?

$$\begin{array}{r}
 4242 : 23 = 134 \\
 23 \\
 \overline{144} \\
 124 \\
 \overline{202} \\
 \underline{202} \\
 0
 \end{array}$$

Die Rechnung ergibt also $(4242)_5 : (23)_5 = (134)_5$. Dabei ergibt sich die 1 als erste Ziffer, da $(23)_5 \cdot (2)_5 = (101)_5 > (42)_5$ und $(42)_5 - (23)_5 \cdot 0 = (42)_5 > (23)_5$ ist. Wegen $(23)_5 \cdot (4)_5 = (202)_5 > (144)_5$ und $(144)_5 - (23)_5 \cdot 2 = (43)_5 > (23)_5$, ist die zweite Ziffer eine 3. Schließlich ist $(23)_5 \cdot (4)_5 = (202)_5$.

11 Teilbarkeitsregeln

Wir erinnern an die Definition der Teiler: Für $a, b \in \mathbb{Z}$ sagen wir: a teilt b (oder auch: b ist durch a teilbar), in Zeichen

$$a|b \quad :\iff \quad \text{Es existiert ein } n \in \mathbb{Z} \text{ mit } na = b.$$

Wenn wir die Definition so festlegen, gilt: alle ganzen Zahlen sind Teiler der 0, auch 0 teilt 0 (denn die Definition ist zweifelsfrei erfüllt), *aber man darf trotzdem nicht durch 0 dividieren!* Die Begründung dafür, und warum man es manchmal trotzdem tut und was dann passiert, werden wir uns später noch einmal klar machen.

Auf dem Hintergrund von Satz 10.3 läßt sich formulieren: Eine natürliche Zahl b ist durch eine natürliche Zahl $a \neq 0$ teilbar, wenn sich bei der Division von b durch a der Rest $r = 0$ ergibt. Erinnerung sei daran, daß wir beim Beweis von Satz 10.3 lediglich solche Eigenschaften der natürlichen Zahlen verwendet haben, die nichts mit ihrer Darstellungsweise zu tun haben. Die in diesem Abschnitt behandelten Teilbarkeitsregeln formulieren dagegen Zusammenhänge zwischen der Teilbarkeit als Eigenschaft einer Zahl und Eigenschaften der Darstellung dieser Zahl in einem jeweils festgelegten Stellenwertsystem.

Daß Teilbarkeit eine Eigenschaft bezeichnet, die natürlichen Zahlen unabhängig von ihrer Darstellung zukommt, schließt nicht aus, daß sich z.B. die Eigenschaft *teilbar durch 2* in verschiedenen Stellenwertsystemen auf verschiedene Weise *erkennen* läßt. Z.B. ist es bekanntermaßen so, daß natürliche Zahlen im Dezimalsystem durch 2 teilbar sind, wenn ihre letzte Ziffer durch 2 teilbar ist, es sich also um eine gerade Zahl handelt. Dies gilt für Zahlen im Dreiersystem nicht. Man betrachte z.B. $(12)_3 = 5$. Deshalb erhält man in verschiedenen Stellenwertsystemen in der Regel unterschiedliche Teilbarkeitsregeln.

Wir werden im folgenden Teilbarkeitsregeln zunächst im Dezimalsystem und dann in allgemeinen Stellenwertsystemen behandeln. Zunächst aber zu einigen Eigenschaften der Teilbarkeitsrelation und einer spezifischen Veranschaulichung derselben. In Abschnitt 9 hatten wir schon gesehen, daß teilbar reflexiv und transitiv ist:

$a|a$ für alle $a \in \mathbb{Z}$, denn $a = 1 \cdot a$, also ist $n = 1$ in der Definition oben.

$a|b$ heißt: $na = b$, $b|c$ heißt $mb = c$ mit $n, m \in \mathbb{Z}$ geeignet, damit ist auch $nm \cdot a = c$, also $a|c$.

Satz 11.1 Für $a, b, c, d \in \mathbb{Z}$ gilt

$$a|b \text{ und } c|d \implies ac|bd.$$

Beweis. Nach Voraussetzung existieren $n, m \in \mathbb{Z}$ mit $na = b$ und $mc = d$. Daraus folgt

$$(nm)(ac) = (na)(mc) = bd$$

mit $nm \in \mathbb{Z}$. ■

Beispiel. $3|9$ und $5|20$ liefert $15|180$.

Satz 11.2 Für $a, b, c, r, s \in \mathbb{Z}$ gilt: $a|b$ und $a|c \implies a|(rb + sc)$.

Beweis. Wegen $1|r$ gilt nach Voraussetzung und wegen Satz 11.1 $a|rb$. Analog gilt $a|sc$. Also existieren $n, m \in \mathbb{Z}$ mit $na = rb$ und $ma = sc$. Damit gilt

$$(n + m)a = na + ma = rb + sc$$

mit $n + m \in \mathbb{Z}$. ■

Aus dem letzten Satz folgt insbesondere für $a, b, c \in \mathbb{N}$:

$$a|b \text{ und } a|c \implies a|(b - c).$$

Beispiele. $3|6$ und $3|15$ liefert z.B. $3|72$, da $72 = 6 \cdot 2 + 15 \cdot 4$ ist. $5|25$ und $5|10$ andererseits ergibt $5|15$ wegen $15 = 25 - 10$.

Definition 11.3 Für jedes $a \in \mathbb{N}$ definieren wir die **Teilmengen** $T(a)$:

$$T(a) := \{x \in \mathbb{N} \mid x|a\}.$$

Satz 11.4 Für $a \in \mathbb{N} \setminus \{1\}$ gilt

$$2 \leq |T(a)| \leq a.$$

Beweis. Aus $\{1, a\} \subset T(a)$ folgt $2 \leq |T(a)|$. Ferner gilt für jeden Teiler b von a zum einen $b \geq 1$ und zum anderen, wegen $nb = a$ für $n \in \mathbb{N}$, also $n \geq 1$, $b \leq a$. Da es nur a verschiedene natürliche Zahlen zwischen 1 und a gibt, folgt daraus die Ungleichung $|T(a)| \leq a$. ■

Satz 11.5 Für $a, b \in \mathbb{N}$ gilt:

$$a|b \iff T(a) \subset T(b).$$

Beweis. „ \implies “ folgt unmittelbar aus der Transitivität der Teilerrelation. „ \impliedby “ folgt sofort aus $a \in T(a)$. ■

Wir schauen uns dieses Ergebnis noch einmal sozusagen von außen an:

Einschub: Ordnung, mehr Ordnung, und das Erhalten von Ordnung

1. Wir erinnern an die Potenzmenge von \mathbb{N} : $\mathcal{P}(\mathbb{N})$ ist die Menge aller Teilmengen von \mathbb{N} , also eine Menge von Mengen. Sei nun

$$\mathbf{T} := \{T(a) \mid a \in \mathbb{N}\} \subset \mathcal{P}(\mathbb{N})$$

\mathbf{T} ist ebenfalls eine Menge von Mengen. Auf \mathbf{T} können wir eine uns schon wohlbekannte Relation, die Teilmengenbeziehung, betrachten, also in Formeln:

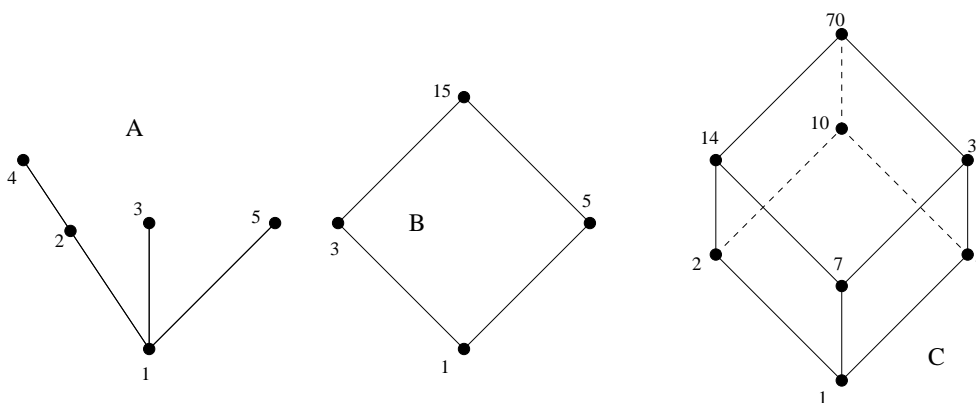
$$\forall T(a), T(b) \in \mathbf{T} \text{ gelte } : T(a) R T(b) \iff T(a) \subset T(b).$$

Wie wir schon wissen, handelt es sich hierbei um eine Ordnungsrelation, die Menge \mathbf{T} erhält durch diese Relation eine Struktur, eine „Ordnung“. Allgemein heißt eine Menge, auf der eine Ordnungsrelation definiert ist, eine **geordnete Menge**.

2. Ein anderes Beispiel für eine geordnete Menge ist \mathbb{N} selbst mit der \leq Relation. Hier haben wir aber noch zusätzlich, dass zwei Elemente *immer* vergleichbar sind, entweder gilt $a \leq b$ oder $b \leq a$. So etwas nennt man eine **total geordnete Menge**. Offensichtlich gilt diese Eigenschaft in $(\mathcal{P}(\mathbb{N}), \subset)$ und auch in (\mathbf{T}, \subset) nicht: Für $T(6) = \{1, 2, 3, 6\}$ und $T(8) = \{1, 2, 4, 8\}$ gilt weder $T(6) \subset T(8)$ noch $T(8) \subset T(6)$.
3. Die Teilerrelation auf \mathbb{N} ist ebenfalls reflexiv, transitiv und antisymmetrisch. Zur Antisymmetrie: Hat man $a, b \in \mathbb{N}$ mit $a|b$ und $b|a$, so gilt $a = nb$ und $b = ma$ mit $n, m \in \mathbb{N}$ (Warum können n, m hier nicht negativ sein?). Also: $b = mn b$, und da $b \neq 0$, muss $1 = mn$ sein, das geht aber nur, wenn $m = 1$ und $n = 1$. Sozusagen schafft die Teilerrelation auf \mathbb{N} „weniger Ordnung“ als „ \leq “. Ordnungen auf endlichen Mengen können auch durch Diagramme veranschaulicht werden, wir betrachten das hier speziell für die Teilerrelation. Relationen veranschaulichten wir in Abschnitt 9 unter anderem mittels sogenannter Pfeildiagramme, bei denen wir Elementen einer Menge Punkte zuordneten und die Punkte, die in Relation zueinander standen, durch Pfeile verbanden. Gegeben sei nun eine beliebige endliche Teilmenge von \mathbb{N} . Wegen der Reflexivität der Teilerrelation besitzt jeder (einem Element der gegebenen Menge) zugeordnete Punkt einen *Ringpfeil*. Wegen der Transitivität existieren auch alle möglichen *Überbrückungspfeile*. Wir können daher auf das Zeichnen der *Ringpfeile* und *Überbrückungspfeile* verzichten, ohne den Informationsgehalt des gezeichneten Pfeildiagramms zu vermindern. Legt man zusätzlich das Diagramm noch so an, daß sämtliche Pfeile nach oben zeigen, so kann zusätzlich auf das Zeichnen der Pfeilspitzen verzichtet werden. Derart vereinfachte Pfeildiagramme nennt man *Hasse-Diagramme*.

Beispiele. $A = \{1, 2, 3, 4, 5\}$, $B = T(15) = \{1, 3, 5, 15\}$,

$C = T(70) = \{1, 2, 5, 7, 10, 14, 35, 70\}$.



4. Wir definieren nun eine Abbildung Φ durch

$$\Phi : \mathbb{N} \rightarrow \mathbf{T}, a \mapsto T(a),$$

jedem $a \in \mathbb{N}$ wird also die Menge seiner Teiler zugeordnet. Nach Definition ist Φ surjektiv. Die Abbildung Φ ist auch injektiv: Seien $a, b \in \mathbb{N}$ mit $a \neq b$ gegeben.

O.B.d.A. gelte $a > b$. Dann ist $a \notin T(b)$, daher $\Phi(a) = T(a) \neq T(b) = \Phi(b)$. (Wir erinnern uns: Zwei Mengen A, B sind schon verschieden, wenn es $a \in A$ gibt, mit $a \notin B$.)

Die Abbildung Φ ist also bijektiv. Wir betrachten nun \mathbb{N} als Menge versehen mit der Relation „|“ und \mathbf{T} als Menge versehen mit der Relation „ \subset “. Dann gilt nach dem bisher gesehenen:

$$a|b \iff \Phi(a) \subset \Phi(b),$$

Die Abbildung Φ erhält also die Ordnung, ist **strukturverträglich**.

5. Allgemein nennt man eine strukturhaltende Abbildung einen **Morphismus**, das ist allerdings ein sehr allgemeiner Begriff, je nach konkreter mathematischer Umgebung erhält das Wort noch Zusätze. Da hier $\Phi : (\mathbb{N}, |) \rightarrow (\mathbf{T}, \subset)$ zusätzlich noch bijektiv ist, kann man Φ z.B. auch einen **Isomorphismus** nennen. (Die Silbe „Iso“ impliziert immer eine bijektive Abbildung, wir werden später noch andere Beispiele kennenlernen.)

Nun zu einigen (elementaren) Teilbarkeitsregeln.

Satz 11.6 (Endstellenregeln) Sei $a \in \mathbb{N}$ im Dezimalsystem gegeben durch

$$a = (y_n y_{n-1} y_{n-2} \dots y_2 y_1 y_0)_{10}.$$

Dann gilt

- i) $2|a \iff 2|y_0$,
- ii) $5|a \iff 5|y_0$,
- iii) $4|a \iff 4|y_1 y_0$,
- iv) $25|a \iff 25|y_1 y_0$,
- v) $8|a \iff 8|y_2 y_1 y_0$,
- vi) $10|a \iff y_0 = 0$.

Beweis.

Zu i) „ \implies “: Aus $2|a$ und $2|10$ folgt $2|(a - 10 \cdot y_n y_{n-1} y_{n-2} \dots y_2 y_1)$, also $2|y_0$.

„ \impliedby “: Aus $2|y_0$ und $2|10$ folgt $2|(y_0 + 10 \cdot y_n y_{n-1} y_{n-2} \dots y_2 y_1)$, also $2|a$.

Zu ii) Völlig analog zu i).

Zu iii) „ \implies “: Aus $4|a$ und $4|100$ folgt $4|(a - 100 \cdot y_n y_{n-1} y_{n-2} \dots y_2)$, also $4|y_1 y_0$.

„ \impliedby “: Aus $4|y_1 y_0$ und $4|100$ folgt $4|(y_1 y_0 + 100 \cdot y_n y_{n-1} y_{n-2} \dots y_2)$, also $4|a$.

Zu iv) Völlig analog zu iii).

Zu v) „ \implies “: Aus $8|a$ und $8|1000$ folgt $8|(a - 1000 \cdot y_n y_{n-1} y_{n-2} \dots y_3)$, also $8|y_2 y_1 y_0$.

„ \impliedby “: Aus $8|y_2 y_1 y_0$ und $8|1000$ folgt $8|(y_2 y_1 y_0 + 1000 \cdot y_n y_{n-1} y_{n-2} \dots y_3)$, also $8|a$.

Zu vi) Klar. ■

Nach diesem Muster können viele weitere Teilungsregeln hergeleitet und bewiesen werden. Ferner läßt sich unser Vorgehen leicht auf andere Zahldarstellungen übertragen.

Satz 11.7 Sei $a = (y_n y_{n-1} y_{n-2} \dots y_2 y_1 y_0)_b$ für $b \in \mathbb{N}$, $b > 1$.

i) Für $d \in T(b)$ gilt

$$d|a \iff d|y_0.$$

ii) Für $d \in T(b^2)$ gilt

$$d|a \iff d|(y_1 \cdot b + y_0).$$

Beweis.

Zu i) „ \implies “: Aus $d|a$ und $d|b$ folgt

$$d|(a - b \cdot (y_n \cdot b^{n-1} + y_{n-1} b^{n-2} + y_{n-2} b^{n-3} + \dots + y_2 b^1 + y_1)),$$

also $d|y_0$.

„ \impliedby “: Aus $d|y_0$ und $d|b$ folgt

$$d|(y_0 + b \cdot (y_n \cdot b^{n-1} + y_{n-1} b^{n-2} + y_{n-2} b^{n-3} + \dots + y_2 b^1 + y_1)),$$

also $d|a$.

Zu ii) „ \implies “: Aus $d|a$ und $d|b^2$ folgt

$$d|(a - b^2 \cdot (y_n \cdot b^{n-2} + y_{n-1} b^{n-3} + y_{n-2} b^{n-4} + \dots + y_2)),$$

also $d|(y_1 \cdot b + y_0)$.

„ \impliedby “: Aus $d|(y_1 \cdot b + y_0)$ und $d|b^2$ folgt

$$d|(y_1 \cdot b + y_0 + b^2 \cdot (y_n \cdot b^{n-2} + y_{n-1} b^{n-3} + y_{n-2} b^{n-4} + \dots + y_2)),$$

also $d|a$. ■

Beispiele. i) Für $b = 12$ gilt $T(12) = \{1, 2, 3, 4, 6, 12\}$ und

$T(12^2) = \{1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 36, 48, 72, 144\}$.

ii) Für $b = 5$ ist $T(5) = \{1, 5\}$ und $T(5^2) = \{1, 5, 25\}$.

Wir kommen nun zum nächsten Typ von Teilbarkeitsregeln.

Satz 11.8 (Quersummenregeln) Sei $a \in \mathbb{N}$ im Dezimalsystem gegeben durch

$$a = (y_n y_{n-1} y_{n-2} \dots y_2 y_1 y_0)_{10}.$$

Dann gilt

i) $3|a \iff 3|(y_n + y_{n-1} + y_{n-2} + \dots + y_2 + y_1 + y_0)$,

ii) $9|a \iff 9|(y_n + y_{n-1} + y_{n-2} + \dots + y_2 + y_1 + y_0)$.

Beweis. Zunächst beobachten wir, daß für jedes $n \in \mathbb{N}$, wegen

$$10^n - 1 = 9 \cdot 10^{n-1} + 9 \cdot 10^{n-2} + \dots + 9 \cdot 10 + 9,$$

gilt

$$9 | (10^n - 1).$$

Daraus folgt insbesondere $3 | (10^n - 1)$ für $n \in \mathbb{N}$.

Zu **i)** „ \implies “: Aus $3 | a$ und $3 | (10^n - 1)$ für $n \in \mathbb{N}$ folgt

$$3 | \left(a - \sum_{i=1}^n (10^i - 1) \cdot y_i \right),$$

also, wegen

$$a - \sum_{i=1}^n (10^i - 1) \cdot y_i = \sum_{i=0}^n 10^i \cdot y_i - \sum_{i=1}^n (10^i - 1) \cdot y_i = y_n + y_{n-1} + y_{n-2} + \dots + y_1 + y_0,$$

$$3 | (y_n + y_{n-1} + y_{n-2} + \dots + y_2 + y_1 + y_0).$$

„ \impliedby “: Aus $3 | (y_n + y_{n-1} + y_{n-2} + \dots + y_2 + y_1 + y_0)$ und $3 | (\sum_{i=1}^n (10^i - 1) \cdot y_i)$ folgt

$$3 | \left(\sum_{i=1}^n (10^i - 1) \cdot y_i + \sum_{i=0}^n y_i \right),$$

also, wegen

$$\sum_{i=1}^n (10^i - 1) \cdot y_i + \sum_{i=0}^n y_i = \sum_{i=0}^n 10^i \cdot y_i = a,$$

$$3 | a.$$

Zu **ii)** Völlig analog zu **i)**. ■

Auch dieses Resultat läßt sich problemlos auf Darstellungen in anderen Stellenwertsystemen übertragen.

Satz 11.9 Für $a = (y_n y_{n-1} y_{n-2} \dots y_2 y_1 y_0)_b$ mit $b \in \mathbb{N}$, $b > 1$, und $d \in T(b-1)$ gilt

$$d | a \iff d | (y_n + y_{n-1} + y_{n-2} + \dots + y_2 + y_1 + y_0).$$

Beweis. Analog zum vorhergehenden Satz. ■

Dieses Resultat läßt sich weiter verallgemeinern auf Teiler von $b^n - 1$ und b -adische Quersummen höherer Ordnung (vgl. z.B. F.Padberg, *Elementare Zahlentheorie*, Abschnitt VII.3). So ergibt sich die b -adische Quersumme 2.Ordnung durch Addition der Zahlen, die durch die 1. und 2. bzw. 3. und 4. Ziffer usw. dargestellt werden: Für $d \in T(b^2 - 1)$ gilt $d | a$ genau dann, wenn d die b -adische Quersumme 2.Ordnung von a teilt.

Beispiele.

i) $b = 12$ führt auf $T(12 - 1) = T(11) = \{1, 11\}$, d.h. $a = (y_n y_{n-1} y_{n-2} \dots y_2 y_1 y_0)_{12}$ ist

durch 11 teilbar, wenn $11 \mid \sum_{i=0}^n y_i$ gilt.

ii) $b = 5$ ergibt $T(4) = \{1, 2, 4\}$, d.h. $a = (y_n y_{n-1} y_{n-2} \dots y_2 y_1 y_0)_5$ ist z.B. durch 2 teilbar, wenn $2 \mid \sum_{i=0}^n y_i$ gilt.

iii) $b = 7$ liefert $T(6) = \{1, 2, 3, 6\}$, d.h. $a = (y_n y_{n-1} y_{n-2} \dots y_2 y_1 y_0)_7$ ist z.B. durch 6 teilbar, wenn $6 \mid \sum_{i=0}^n y_i$ gilt.

iv) 165 ist durch 33 teilbar, da $33 \mid 99$ und $1 + 65 = 66$ durch 33 teilbar ist.

ii) $(253)_7$ ist durch 4 teilbar, da $4 \mid 48$ und $2 + (53)_7 = 2 + 38 = 40$ durch 4 teilbar ist.

Wir kommen nun zum letzten Typ von Teilbarkeitsregeln.

Satz 11.10 (Alternierende Quersummenregel) Sei $a \in \mathbb{N}$ im Dezimalsystem gegeben durch

$$a = (y_n y_{n-1} y_{n-2} \dots y_2 y_1 y_0)_{10}.$$

Dann gilt

$$11 \mid a \iff 11 \mid ((-1)^n y_n + (-1)^{n-1} y_{n-1} + (-1)^{n-2} y_{n-2} + \dots + y_2 - y_1 + y_0).$$

Beweis. Wir zeigen zunächst, daß für $n \in \mathbb{N}$ gilt

$$11 \mid (10^n - (-1)^n) :$$

Ist $n \in \mathbb{N}$ gerade, so ist

$$(10 + 1) \sum_{i=0}^{n-1} (-1)^{i+1} 10^i = \sum_{i=0}^{n-1} (-1)^{i+1} 10^{i+1} + \sum_{i=0}^{n-1} (-1)^{i+1} 10^i = 10^n - 1.$$

Ist $n \in \mathbb{N}$ ungerade, so gilt

$$(10 + 1) \sum_{i=0}^{n-1} (-1)^i 10^i = \sum_{i=0}^{n-1} (-1)^i 10^{i+1} + \sum_{i=0}^{n-1} (-1)^i 10^i = 10^n + 1.$$

„ \implies “: Aus $11 \mid a$ und $11 \mid (10^i - (-1)^i)$ für $i \in \mathbb{N}$ folgt

$$11 \mid (a - \sum_{i=1}^n (10^i - (-1)^i) y_i),$$

also, wegen

$$a - \sum_{i=1}^n (10^i - (-1)^i) y_i = \sum_{i=0}^n 10^i \cdot y_i - \sum_{i=1}^n (10^i - (-1)^i) y_i = \sum_{i=0}^n (-1)^i y_i,$$

$$11 \mid \sum_{i=0}^n (-1)^i y_i.$$

„ \impliedby “: Aus $11 \mid \sum_{i=0}^n (-1)^i y_i$ und $11 \mid (10^i - (-1)^i)$ für $i \in \mathbb{N}$ folgt

$$11 \mid (\sum_{i=0}^n (-1)^i y_i + \sum_{i=1}^n (10^i - (-1)^i) y_i),$$

also, wegen

$$\sum_{i=0}^n (-1)^i y_i + \sum_{i=1}^n (10^i - (-1)^i) y_i = \sum_{i=0}^n 10^i y_i = a,$$

$$11|a.$$

■

Völlig analog dazu gilt im b -adischen System:

Satz 11.11 Für $a = (y_n y_{n-1} y_{n-2} \dots y_2 y_1 y_0)_b$ mit $b \in \mathbb{N}$, $b > 1$, und $d \in T(b+1)$ gilt

$$d|a \iff d|((-1)^n y_n + (-1)^{n-1} y_{n-1} + (-1)^{n-2} y_{n-2} + \dots + y_2 - y_1 + y_0).$$

Dieses Resultat läßt sich weiter verallgemeinern auf Teiler von $b^n + 1$ und alternierende b -adische Quersummen höherer Ordnung (vgl. z.B. wieder F. Padberg, *Elementare Zahlentheorie*, Abschnitt VII.3).

Beispiele.

- i) $b = 12$ ergibt $T(13) = \{1, 13\}$, d.h. $a = (y_n y_{n-1} y_{n-2} \dots y_2 y_1 y_0)_{12}$ ist durch 13 teilbar, wenn $13 | \sum_{i=0}^n (-1)^i y_i$ gilt.
- ii) $b = 5$ führt auf $T(6) = \{1, 2, 3, 6\}$, d.h. (z.B.) $a = (y_n y_{n-1} y_{n-2} \dots y_2 y_1 y_0)_5$ ist durch 3 teilbar, wenn $3 | \sum_{i=0}^n (-1)^i y_i$ gilt.
- iii) $b = 7$ liefert $T(8) = \{1, 2, 4, 8\}$, d.h. (z.B.) $a = (y_n y_{n-1} y_{n-2} \dots y_2 y_1 y_0)_7$ ist durch 4 teilbar, wenn $4 | \sum_{i=0}^n (-1)^i y_i$ gilt.

12 Hauptsatz der elementaren Zahlentheorie

Eine Sonderstellung nehmen diejenigen natürlichen Zahlen a ein, für die $|T(a)| = 2$ ist.

Definition 12.1 Eine Zahl $a \in \mathbb{N} \setminus \{1\}$ heißt **Primzahl**, wenn $T(a) = \{1, a\}$ gilt.

Die Bruchrechnung und dabei insbesondere die Addition von Brüchen (das sog. *gleichnamig machen*) beruht ganz wesentlich auf der Tatsache, dass man jede natürliche Zahl $a > 1$ als Produkt von Primzahlen schreiben kann. Existenz und Eindeutigkeit der Primfaktorzerlegung für jede natürliche Zahl $a > 1$ behandelt der Hauptsatz der elementaren Zahlentheorie.

Satz 12.2 Für $a \in \mathbb{N} \setminus \{1\}$ ist der kleinste von 1 verschiedene Teiler eine Primzahl.

Beweis. Sei $a \in \mathbb{N} \setminus \{1\}$ beliebig aber fest gewählt. Sei t der kleinste Teiler von a mit $t \neq 1$. Angenommen, t ist keine Primzahl, d.h. es existiert ein $n \in \mathbb{N}$ mit $1 < n < t$ und $n|t$. Wegen $t|a$ gilt auch $n|a$. Widerspruch zur Minimalität von t . Also ist t eine Primzahl.

■

Definition 12.3 Für $a \in \mathbb{N} \setminus \{1\}$ heißt jedes Produkt $a = p_1 p_2 \dots p_r$ mit Primzahlen p_1, p_2, \dots, p_r Primfaktorzerlegung von a .

Satz 12.4 Jedes $a \in \mathbb{N} \setminus \{1\}$ besitzt (mindestens) eine Primfaktorzerlegung.

Beweis. Sei $p_1 \neq 1$ der kleinste (von 1 verschiedene) Teiler von $a > 1$. Dieser ist nach Satz 12.2 eine Primzahl. Gilt $p_1 = a$, so sind wir fertig. Anderenfalls ist $1 < p_1 < a$ und es existiert ein $n_1 \in \mathbb{N}$ mit $1 < n_1 < a$ und

$$a = n_1 \cdot p_1.$$

Ist n_1 eine Primzahl, so ist $n_1 \cdot p_1$ eine Primfaktorzerlegung von a und wir sind fertig. Anderenfalls bestimmen wir den kleinsten Teiler $p_2 \neq 1$ von n_1 , der wieder eine Primzahl sein muß und für den $1 < p_2 < n_1$ gilt. Insbesondere existiert wieder ein $n_2 \in \mathbb{N}$ mit $1 < n_2 < n_1$ und $p_2 \cdot n_2 = n_1$, so daß gilt

$$a = p_1 p_2 n_2.$$

Nur fahren wir mit n_2 fort. Auf diese Weise erhalten wir eine Folge natürlicher Zahlen $n_1 > n_2 > n_2 > \dots > 1$, die nach endlich vielen Schritten mit einer Primzahl $n_s = p_s \geq 2$ abbrechen muß. Es gilt dann

$$a = p_1 p_2 \dots p_s.$$

■

Nun zur Eindeutigkeit.

Satz 12.5 (Hauptsatz) *Jede natürliche Zahl $a \in \mathbb{N} \setminus \{1\}$ besitzt bis auf die Reihenfolge der Faktoren genau eine Primfaktorzerlegung.*

Beweis. Angenommen, es gebe eine natürliche Zahl mit zwei verschiedenen Primfaktorzerlegungen. Sei a die kleinste solche Zahl und es gelte

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot \dots \cdot q_s$$

mit Primzahlen $1 < p_1 \leq p_2 \leq \dots \leq p_r \leq a$ und $1 < q_1 \leq q_2 \leq \dots \leq q_s \leq a$. Wäre $p_1 = q_1$, so gäbe es eine natürliche Zahl mit verschiedenen Primfaktorzerlegungen, die kleiner als a ist. Also muß $p_1 \neq q_1$ sein. Analog müssen alle p_i und q_j paarweise voneinander verschieden sein.

O.B.d.A. sei $p_1 > q_1$. Wir definieren

$$n := (p_1 - q_1) \cdot p_2 \cdot p_3 \cdot \dots \cdot p_r.$$

Wegen $n < a$ besitzt n eine eindeutige Primfaktorzerlegung. Andererseits ist q_1 ein Teiler von n , da

$$\begin{aligned} n &= (p_1 - q_1) \cdot p_2 \cdot \dots \cdot p_r \\ &= p_1 \cdot p_2 \cdot \dots \cdot p_r - q_1 \cdot p_2 \cdot \dots \cdot p_r \\ &= q_1 \cdot q_2 \cdot \dots \cdot q_r - q_1 \cdot p_2 \cdot \dots \cdot p_r \\ &= q_1(q_2 \cdot \dots \cdot q_r - p_2 \cdot \dots \cdot p_r). \end{aligned}$$

Da q_1 verschieden von p_2, \dots, p_r ist gilt

$$q_1 | (p_1 - q_1),$$

also $q_1 | p_1$. p_1 ist aber Primzahl, d.h. es muß $p_1 = q_1$ sein. Widerspruch! ■

Mit Hilfe des Hauptsatzes können wir nun zeigen, daß es unendlich viele Primzahlen gibt.

Satz 12.6 *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen, es gäbe nur endlich viele Primzahlen p_1, p_2, \dots, p_r . Wir definieren

$$n := p_1 \cdot p_2 \cdot \dots \cdot p_r + 1.$$

Sei $t \neq 1$ der kleinste Teiler von n . Dieser ist eine Primzahl. Also gilt für ein $i \in \{1, 2, \dots, r\}$ $t = p_i$ und somit

$$p_i | (p_1 \cdot p_2 \cdot \dots \cdot p_r + 1).$$

Daraus folgt

$$p_i | 1.$$

Widerspruch! ■

Nun zu einigen Folgerungen aus dem Hauptsatz. Wir erinnern zunächst an eine Bezeichnung. Analog zum Summenzeichen \sum gibt es das Produktzeichen \prod . Für beliebige Zahlen a_1, \dots, a_m ist

$$a_1 \cdot a_2 \cdot \dots \cdot a_m =: \prod_{i=1}^m a_i.$$

Wir definieren nun

$$\mathbb{P} = \{p \in \mathbb{N} \mid p \text{ Primzahl}\} = \{p_1, p_2, p_3, \dots\}.$$

wobei wir die Primzahlen der Einfachheit halber der Größe nach sortieren, also $\mathbb{P} = \{2, 3, 5, 7, 11, \dots\}$. Da immer $p_i^0 = 1$ gilt, können wir z.B. schreiben:

$$140 = 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^1 \cdot 11^0 \cdot 13^0 \cdot \dots = \prod_{i=1}^{\infty} p_i^{n_i},$$

wobei alle $n_i = 0$ außer (hier) für $i = 1, 3, 4$. Formal heißt das, dass wir 140 auffassen als Grenzwert der Folge $a_k = \prod_{i=1}^k p_i^{n_i}$, natürlich gilt hier $a_k = 140$ für alle $k \geq 4$. In dieser Art und Weise können wir die eindeutige Primzahlzerlegung einer natürlichen Zahl $a \in \mathbb{N}$ immer schreiben als

$$a = \prod_{i=1}^{\infty} p_i^{n_i},$$

wobei alle $n_i = 0$ sind bis auf endlich viele wohlbestimmte Ausnahmen. Dies erleichtert uns die mathematisch korrekte Formulierung des folgenden Satzes.

Satz 12.7 (Teilbarkeitskriterium) *Es sei $a = \prod_{i=1}^{\infty} p_i^{n_i}$, $b = \prod_{i=1}^{\infty} p_i^{m_i}$ mit $p_i \in \mathbb{P}$, $n_i, m_i \in \mathbb{N}_0$. Dann gilt*

$$a|b \iff n_i \leq m_i \text{ für alle } i \in \mathbb{N}.$$

Beweis. “ \implies ”: Wegen $a|b$ existiert ein $c = \prod_{i=1}^{\infty} p_i^{k_i} \in \mathbb{N}$ ($k_i \in \mathbb{N}_0$) mit $c \cdot a = b$, also

$$\prod_{i=1}^{\infty} p_i^{m_i} = b = c \cdot a = \prod_{i=1}^{\infty} p_i^{k_i} \cdot \prod_{i=1}^{\infty} p_i^{n_i} = \prod_{i=1}^{\infty} p_i^{k_i+n_i}.$$

Aus der Eindeutigkeit der Primfaktorzerlegung folgt $k_i+n_i = m_i$ und aus $k_i \geq 0$ schließlich $n_i \leq m_i$.

“ \impliedby ”: Wegen $n_i \leq m_i$ für $i \in \mathbb{N}$ existieren $k_i \in \mathbb{N}_0$ mit $k_i+n_i = m_i$. Für $c = \prod_{i=1}^{\infty} p_i^{k_i} \in \mathbb{N}$ gilt dann $c \cdot a = b$, also $a|b$. ■

Als Folgerung aus diesem Satz ergibt sich die folgenden Aussage über Teilmengen.

Satz 12.8 *Die Teilermenge $T(a)$ von $a = p_1^{n_1} \cdot p_2^{n_2} \cdot \dots \cdot p_r^{n_r}$, $p_i \in \mathbb{P}$, $n_i \in \mathbb{N}$, besteht genau aus den Zahlen $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}$ mit $0 \leq \alpha_i \leq n_i$ für $i = 1, 2, \dots, r$. $T(a)$ enthält demnach genau $(n_1 + 1) \cdot (n_2 + 1) \cdot \dots \cdot (n_r + 1)$ Elemente.*

Bemerkung Folgerungen zur Gestalt von Hasse-Diagrammen (in den Übungen).

Satz 12.9 (Primzahlkriterium) Für $p \in \mathbb{N} \setminus \{1\}$ gilt

$$p \text{ Primzahl} \iff (\text{Für alle } a, b \in \mathbb{N} \text{ gilt: } p|a \cdot b \implies p|a \text{ oder } p|b.)$$

Beweis. “ \implies ”: Wegen $p|a \cdot b$ kommt $p \in \mathbb{P}$ in der Primfaktorzerlegung von $a \cdot b$ und somit, wegen der Eindeutigkeit, ebenfalls in der Primfaktorzerlegung von a oder b vor. Also gilt $p|a$ oder $p|b$. (Das *oder* ist hier natürlich *nicht ausschließend* gemeint.)

“ \impliedby ”: Angenommen es gilt $p \notin \mathbb{P}$. Dann existieren $a, b \in \mathbb{N}$ mit $1 < a < p$, $1 < b < p$ und $p = a \cdot b$. Damit gilt $p|a \cdot b$ sowie $p \nmid a$ und $p \nmid b$. Widerspruch! ■

13 GgT und kgV

Dieses Thema wird in der Schule in der 5. bzw. 6. Klasse im Rahmen der Teilbarkeitslehre behandelt und spielt insbesondere eine Rolle bei der Bruchrechnung.

Definition 13.1 Seien $a, b \in \mathbb{N}$.

- i) Jedes Element von $T(a) \cap T(b)$ heißt gemeinsamer Teiler von a und b .
- ii) Gilt $T(a) \cap T(b) = \{1\}$, so heißen a und b teilerfremd oder prim zueinander.
- iii) Das größte Element von $T(a) \cap T(b)$ heißt größter gemeinsamer Teiler von a und b , kurz $\text{ggT}(a, b)$.

Beispiele. $T(24) \cap T(36) = \{1, 2, 3, 4, 6, 12\}$, also $\text{ggT}(24, 36) = 12$.

Auf naheliegende Weise können diese Definitionen auf mehr als zwei natürliche Zahlen verallgemeinert werden: Für $a, b, c \in \mathbb{N}$ heißen die Elemente von $T(a) \cap T(b) \cap T(c)$ z.B. die gemeinsamen Teiler von a, b und c .

Aus der Definition 13.1 folgt unmittelbar:

- i) $\text{ggT}(1, a) = 1$ für $a \in \mathbb{N}$.
- ii) $a|b \implies \text{ggT}(a, b) = a$.

Mit Hilfe von Primfaktorzerlegungen kann der größte gemeinsame Teiler bestimmt werden ohne vorher die Teilmengen explizit anzugeben.

Satz 13.2 Für $a = \prod_{i=1}^{\infty} p_i^{m_i}$, $b = \prod_{i=1}^{\infty} p_i^{n_i}$ mit $p_i \in \mathbb{P}$, $m_i, n_i \in \mathbb{N}_0$, gilt

$$\text{ggT}(a, b) = \prod_{i=1}^{\infty} p_i^{\min(m_i, n_i)}.$$

Beweis. Wir definieren $d := \prod_{i=1}^{\infty} p_i^{\min(m_i, n_i)}$. Aus den Voraussetzungen folgt unmittelbar $d \in T(a) \cap T(b)$. Sei $c = \prod_{i=1}^{\infty} p_i^{k_i} \in T(a) \cap T(b)$ mit $k_i \in \mathbb{N}_0$. Dann gilt $k_i \leq m_i$ und $k_i \leq n_i$, also $k_i \leq \min(m_i, n_i)$, und somit $c|d$ und $c \leq d$. Damit ist $d = \text{ggT}(a, b)$ gezeigt.

■

Folgerung. Für $a, b, n \in \mathbb{N}$ gilt $\text{ggT}(na, nb) = n \cdot \text{ggT}(a, b)$.

Beispiel. $\text{ggT}(520, 910) = 130 \cdot \text{ggT}(4, 7) = 130$.

Insbesondere für größere Zahlen ist die Bestimmung einer Primfaktorzerlegung in der Regel recht mühsam, da hierfür kein schnelles systematisches Rechenverfahren existiert. Das

erklärt die Bedeutung des im folgenden behandelten sogenannten „Euklidischen Algorithmus“: Dieser erlaubt es, den ggT systematisch zu berechnen, ohne Primfaktorzerlegungen zu bestimmen.

Erinnert sei zunächst an die Division mit Rest, d.h. Satz 9.1: Für $a, b \in \mathbb{N}$ gibt es genau ein Paar $q, r \in \mathbb{N}_0$ mit

$$a = q \cdot b + r \quad \text{mit } 0 \leq r < b.$$

Die dem Euklidischen Algorithmus zugrundeliegende Eigenschaft von Teilmengen beschreibt das folgende Beispiel: Gesucht sei $\text{ggT}(564, 80)$. Es ist $564 = 7 \cdot 80 + 4$. Also gilt für $t \in T(564) \cap T(80)$ auch $t|4$, also $t \in T(80) \cap T(4)$. Nun ist $4 = \text{ggT}(80, 4)$ und offensichtlich auch $4 = \text{ggT}(564, 80)$. Allgemein gilt folgender Satz.

Satz 13.3 *Seien $a, b \in \mathbb{N}$ und sei $a = q \cdot b + r$ mit $q, r \in \mathbb{N}_0$ und $0 \leq r < b$. Dann gilt*

$$T(a) \cap T(b) = T(b) \cap T(r)$$

und somit $\text{ggT}(a, b) = \text{ggT}(b, r)$.

Beweis. Sei $t \in T(a) \cap T(b)$, d.h. $t|a$ und $t|b$. Dann gilt auch $t|a - qb$ und somit $t|r$. Damit haben wir gezeigt

$$T(a) \cap T(b) \subset T(b) \cap T(r).$$

Sei $t \in T(b) \cap T(r)$, d.h. $t|b$ und $t|r$. Dann gilt auch $t|qb + r$ und somit $t|a$. Also gilt auch

$$T(b) \cap T(r) \subset T(a) \cap T(b).$$

■

Im allgemeinen führt die einmalige Anwendung des Satzes 13.3 nicht auf eine Menge $T(b) \cap T(r)$ aus der man mühelos $\text{ggT}(a, b)$ ablesen kann. Man wendet den Satz dann mehrfach an. Dieses Vorgehen führt auf den Euklidischen Algorithmus:

$$\begin{aligned} a &= q_1 \cdot b + r_1, & 0 \leq r_1 < b, \\ b &= q_2 \cdot r_1 + r_2, & 0 \leq r_2 < r_1, \\ r_1 &= q_3 \cdot r_2 + r_3, & 0 \leq r_3 < r_2, \\ & \vdots & \vdots \\ r_{n-1} &= q_{n+1} \cdot r_n + r_{n+1}, & 0 \leq r_{n+1} < r_n, \\ & \vdots & \vdots \end{aligned} \tag{13.1}$$

Wegen $b > r_1 > r_2 > r_3 > \dots \geq 0$ muß dieser Algorithmus spätestens nach b Schritten den Rest 0 ergeben, d.h. nach spätestens b Schritten erhält man die Gleichung

$$r_{m-1} = q_{m+1}r_m + 0,$$

d.h. $r_m|r_{m-1}$. Wenden wir Satz ?? (mehrfach) an, so erhalten wir

$$\begin{aligned} T(a) \cap T(b) &= T(b) \cap T(r_1) = T(r_1) \cap T(r_2) \\ &= \dots = T(r_{m-1}) \cap T(r_m) = T(r_m), \end{aligned}$$

also

$$\text{ggT}(a, b) = r_m.$$

Beispiel. $a = 6930$, $b = 1098$ ergibt

$$\begin{aligned} 6930 &= 6 \cdot 1098 + 342 \\ 1098 &= 3 \cdot 342 + 72 \\ 342 &= 4 \cdot 72 + 54 \\ 72 &= 1 \cdot 54 + 18 \\ 54 &= 3 \cdot 18 + 0, \end{aligned}$$

also $\text{ggT}(6930, 1098) = 18$.

Satz 13.4 Für alle $a, b \in \mathbb{N}$ existieren $x, y \in \mathbb{Z}$ mit

$$\text{ggT}(a, b) = x \cdot a + y \cdot b.$$

Anmerkung Eine solche Darstellung mit beliebigen Zahlen x, y heißt *Linearkombination* von a und b , hier ist eine *ganzzahlige Linearkombination* gesucht.

Beweis. Die erste Gleichung in (13.1) ergibt $r_1 = a - q_1b$. Dies in die zweite Gleichung eingesetzt und nach r_2 aufgelöst ergibt

$$r_2 = b - q_2(a - q_1b) = -q_2a + (1 + q_1q_2)b.$$

Dieses Vorgehen fortgesetzt (bis zur vorletzten Gleichung $r_{m-2} = q_m r_{m-1} + r_m$) liefert $x, y \in \mathbb{Z}$ mit

$$\text{ggT}(a, b) = r_m = x \cdot a + y \cdot b.$$

■

Beispiel. Gegeben seien wieder $a = 6930$ und $b = 1098$. Die Koeffizienten $x, y \in \mathbb{Z}$ mit $18 = x \cdot 6930 + y \cdot 1098$ ergeben sich wie folgt:

$$\begin{aligned} 342 &= 6930 - 6 \cdot 1098 \\ 72 &= 1098 - 3 \cdot 342 = 19 \cdot 1098 - 3 \cdot 6930 \\ 54 &= 342 - 4 \cdot 72 = 13 \cdot 6930 - 82 \cdot 1098 \\ 18 &= 72 - 54 = 101 \cdot 1098 - 16 \cdot 6930, \end{aligned}$$

also $18 = (-16) \cdot 6930 + 101 \cdot 1098$ ($x = -16$, $y = 101$).

Folgerungen

i) Jedes Vielfache von $\text{ggT}(a, b)$ läßt sich als Linearkombination in der Form $\tilde{x}a + \tilde{y}b$ mit $\tilde{x}, \tilde{y} \in \mathbb{Z}$ darstellen.

(Klar, wegen $k \cdot \text{ggT}(a, b) = (k \cdot x)a + (k \cdot y)b$ für $k \in \mathbb{Z}$.)

- ii) Es gilt auch die Umkehrung: Jede Zahl der Form $xa + yb$ ($x, y \in \mathbb{Z}$) ist ein Vielfaches von $\text{ggT}(a, b)$.
(Klar, da aus $\text{ggT}(a, b)|a$ und $\text{ggT}(a, b)|b$ folgt $\text{ggT}(a, b)|xa + yb$ für alle $x, y \in \mathbb{Z}$.)
- iii) Aus ii) folgt sofort: $\text{ggT}(a, b)$ ist die kleinste natürliche Zahl, die sich als Linearkombination von a und b darstellen läßt.
- iv) Ebenfalls: $c \in \mathbb{Z}$ läßt sich genau dann als ganzzahlige Linearkombination von a und b darstellen, wenn c ein Vielfaches von $\text{ggT}(a, b)$ ist.
Oder auch: $ax + yb = c$ besitzt ganzzahlige Lösungen genau dann wenn $\text{ggT}(a, b)|c$.
- v) Aus iv) folgt: $\text{ggT}(a, b) = 1 \implies$ Jede ganze Zahl läßt sich als ganzzahlige Linearkombination von a und b darstellen.

Anwendung. (Aus F. Padberg, Elementare Zahlentheorie) Eine Firma will für genau 1000 Euro zwei Arten von Werbegeschenken kaufen. Die eine Sorte kostet je Stück 13 Euro, die andere 19 Euro. Wieviele Werbegeschenke kann sie von den einzelnen Sorten einkaufen?

Bezeichnet man die Anzahl der Werbegeschenke für 13 Euro mit x , die Anzahl der Werbegeschenke für 19 Euro mit y , so entsprechen die gesuchten Anzahlen den ganzzahligen (hier sogar nichtnegativen) Lösungen der Gleichung

$$13x + 19y = 1000.$$

Wegen $\text{ggT}(13, 19) = 1$ und $1|1000$ besitzt diese Gleichung ganzzahlige Lösungen. Allerdings ergibt sich (z.B. mit dem Euklidischen Algorithmus)

$$1 = 3 \cdot 13 - 2 \cdot 19,$$

also durch Multiplikation mit 1000

$$1000 = 3000 \cdot 13 - 2000 \cdot 19.$$

Dies stellt für die vorgestellte Anwendung offensichtlich keine sinnvolle Lösung dar. Für beliebiges $x \in \mathbb{Z}$ gilt jedoch auch

$$\begin{aligned} 1000 &= 3000 \cdot 13 - 2000 \cdot 19 - x \cdot 19 \cdot 13 + x \cdot 13 \cdot 19 \\ &= (3000 - x \cdot 19)13 + (x \cdot 13 - 2000) \cdot 19. \end{aligned}$$

Für $x = 154$ gilt nun $154 \cdot 13 = 2002$ und $154 \cdot 19 = 2926$. Daraus ergibt sich

$$1000 = 74 \cdot 13 + 2 \cdot 19.$$

$x = 74, y = 2$ ist nicht die einzig mögliche Lösungen. Es gilt auch

$$\begin{aligned} 1000 &= 55 \cdot 13 + 15 \cdot 19 \\ &= 36 \cdot 13 + 28 \cdot 19 \\ &= 17 \cdot 13 + 41 \cdot 19. \end{aligned}$$

Andererseits besitzt z.B. die Gleichung $5x + 10y = 997$ wegen $\text{ggT}(5, 10) = 5$ und $5 \nmid 997$ keine ganzzahlige Lösung.

Nun zum kgV.

Definition 13.5 i) Für $a \in \mathbb{N}$ heißt

$$V(a) := \{x \in \mathbb{N} \mid a|x\} = \{n \cdot a \mid n \in \mathbb{N}\}.$$

Vielfachenmenge von a .

ii) Für $a, b \in \mathbb{N}$ heißen die Elemente von $V(a) \cap V(b)$ gemeinsame Vielfache von a und b .

iii) Das kleinste Element der Menge $V(a) \cap V(b)$ heißt kleinstes gemeinsames Vielfache von a und b , kurz $\text{kgV}(a, b)$.

Beispiele. $\text{kgV}(4, 3) = \text{kgV}(4, 6) = 12$, $\text{kgV}(6, 8) = 24$.

Auch diese Definitionen lassen sich auf naheliegende Weise auf mehr als zwei Elemente von \mathbb{N} verallgemeinern.

Die kgV Bestimmung mittels Vielfachenmenge ist oft recht mühsam. Primfaktorzerlegungen führen häufig weiter.

Satz 13.6 Für $a = \prod_{i=1}^{\infty} p_i^{m_i}$, $b = \prod_{i=1}^{\infty} p_i^{n_i}$ mit $p_i \in \mathbb{P}$, $m_i, n_i \in \mathbb{N}_0$, gilt

$$\text{kgV}(a, b) = \prod_{i=1}^{\infty} p_i^{\max(m_i, n_i)}.$$

Beweis. Sei $d := \prod_{i=1}^{\infty} p_i^{\max(m_i, n_i)}$. Wegen $m_i \leq \max(m_i, n_i)$ und $n_i \leq \max(m_i, n_i)$ gilt $a|d$ und $b|d$, d.h. $d \in V(a) \cap V(b)$. Sei $v = \prod_{i=1}^{\infty} p_i^{k_i} \in V(a) \cap V(b)$, $k_i \in \mathbb{N}_0$. Dann gilt $k_i \geq m_i$ und $k_i \geq n_i$, also $k_i \geq \max(m_i, n_i)$ und somit $d|v$. ■

Offensichtlich gilt

i) $\text{kgV}(na, nb) = n \cdot \text{kgV}(a, b)$.

ii) $a, b \in \mathbb{N}$ teilerfremd $\implies \text{kgV}(a, b) = a \cdot b$.

Satz 13.7 (Zusammenhang von ggT und kgV) Für alle $a, b \in \mathbb{N}$ gilt

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

Beweis. Wegen der Sätze 12.2 und 12.7 gilt für $a = \prod_{i=1}^{\infty} p_i^{m_i}$ und $b = \prod_{i=1}^{\infty} p_i^{n_i}$ mit $p_i \in \mathbb{P}$, $m_i, n_i \in \mathbb{N}_0$,

$$\begin{aligned}
 \text{ggT}(a, b) \cdot \text{kgV}(a, b) &= \prod_{i=1}^{\infty} p_i^{\min(m_i, n_i)} \cdot \prod_{i=1}^{\infty} p_i^{\max(m_i, n_i)} \\
 &= \prod_{i=1}^{\infty} p_i^{\min(m_i, n_i) + \max(m_i, n_i)} \\
 &= \prod_{i=1}^{\infty} p_i^{m_i + n_i} \\
 &= \prod_{i=1}^{\infty} p_i^{m_i} \cdot \prod_{i=1}^{\infty} p_i^{n_i} \\
 &= a \cdot b.
 \end{aligned}$$

■

Aus Satz 12.7 folgt insbesondere

$$\text{kgV}(a, b) = \frac{a \cdot b}{\text{ggT}(a, b)},$$

d.h. man kann den kgV bestimmen, indem man zunächst mit dem Euklidischen Algorithmus den ggT bestimmt und anschließend $a \cdot b$ durch ggT dividiert.

Beispiel. $a = 6930$, $b = 1098$. Wegen $\text{ggT}(a, b) = 18$ gilt

$$\text{kgV}(a, b) = \frac{a \cdot b}{18} = 422730.$$

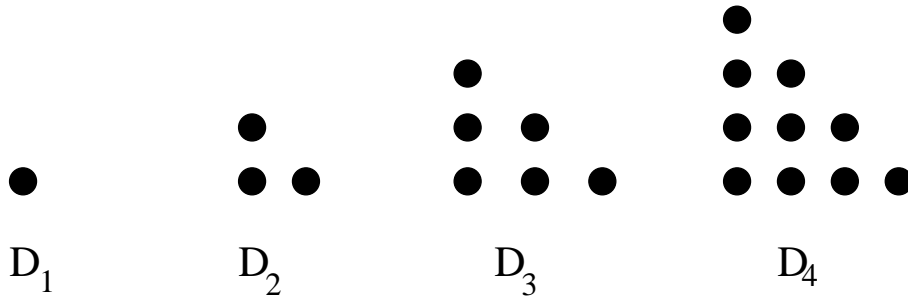
Weitere Eigenschaft: Für $a, b \in \mathbb{N}$ gilt (wegen $x \in V(a) \cap V(b) \iff \text{kgV}(a, b) | x$)

$$V(a) \cap V(b) = V(\text{kgV}(a, b)).$$

14 Zahlen und Muster, Polynomialzahlen

14.1 Dreieckszahlen

In diesem Abschnitt wollen wir uns mit weiteren Beziehungen zwischen den natürlichen Zahlen beschäftigen. Als Dreieckszahlen D_1, D_2, D_3, \dots bezeichnet man die Anzahlen von Punkten in den folgenden dreiecksförmigen Anordnungen:



Für $n \in \mathbb{N}$ ist $D_n = D_{n-1} + n = 1 + 2 + 3 + 4 + \dots + n$.

also für $n \in \mathbb{N}$

$$2 \cdot D_n = n(n+1),$$

d.h.

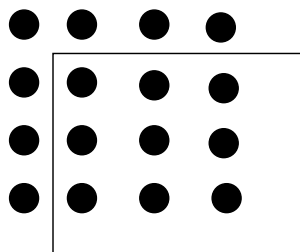
$$D_n = \frac{n(n+1)}{2}.$$

14.2 Quadratzahlen

Naheliegenderweise bezeichnet man die Zahlen $Q_n := n^2$ ($n \in \mathbb{N}$) als Quadratzahlen. Aus obiger Veranschaulichung für die Dreieckszahlen folgt sofort (‘\’ auf die linke Seite bringen) für die Quadratzahlen die Beziehung

$$Q_n = n^2 = D_n + D_n - n = D_n + D_{n-1}.$$

Das Bild



legt ferner folgende Zusammenhänge nahe:

i) $Q_{n+1} = Q_n + 2 \cdot n + 1$, d.h. (Binomische Formel)

$$Q_{n+1} = (n+1)^2 = n^2 + 2n + 1.$$

ii)

$$Q_{n+1} = (n+1)^2 = 1 + 3 + 5 + 7 + \dots + (2n+1).$$

Wir wollen uns noch ein wenig damit beschäftigen, wie man Quadratzahlen erkennt. Welche Ziffern können bei Quadratzahlen als letzte Ziffer auftauchen?

In diesem Zusammenhang erinnern wir noch einmal an die Schreibweise aus Abschnitt 9: $a = c \pmod b$, falls bei der Division von a und c durch b derselbe Rest auftaucht, also falls gilt: $b|(a-c)$. Um auszudrücken, dass es sich hier um eine Restklasse handelt, und nicht um Gleichheit von Zahlen im üblichen Sinn, benutzt man auch häufig das Zeichen \equiv , also $a \equiv c \pmod b$, z.B. $5 \equiv 2 \pmod 3$.

Ist $a \in \mathbb{N}$ eine Quadratzahl, also $a = n^2$, so können wir n darstellen als $n = 10s + t$, daher

$$a = n^2 = (10s + t)^2 = (100s^2 + 20st + t^2) \equiv t^2 \pmod{10},$$

da ja die beiden ersten Summanden auf jeden Fall durch 10 teilbar sind. M.a. W.: Wir müssen nur für $t \in \{0, 1, \dots, 9\}$ die möglichen Endziffern anschauen, und erhalten

Satz 14.1 *Ist $a \in \mathbb{N}$ eine Quadratzahl, so gilt: die letzte Ziffer von a ist ein Element der Menge $\{0, 1, 4, 5, 6, 9\}$.*

Aus diesem Grund können z.B. die Zahlen 99, 37, 1593, 223462 keine Quadratzahlen sein. Zieht man die beiden letzten Ziffern in Betracht, so kann man ähnlich argumentieren: Gilt $a = n^2$, $n = 100s + t$, $t = (y_1 y_0)_{10}$, so gilt mit der analogen Rechnung wie oben: $n^2 \equiv t^2 \pmod{100}$. Ist jetzt $t = (y_1 y_0)_{10} = 10y_1 + y_0$, so gilt:

$$t^2 = y_0^2 + 20 \cdot y_1 \cdot y_0 + 100y_1^2 \equiv (y_0^2 + 20 \cdot y_1 \cdot y_0) \pmod{100}, \quad (14.1)$$

Da wir ja schon wissen, dass $y_0^2 \pmod{10} \in \{0, 1, 4, 5, 6, 9\}$, müssen wir nur diese Fälle als Endziffer für a betrachten. Eine weitere Beobachtung: Sind a und b zwei Quadratzahlen mit gleicher Endziffer, so gilt: $20|(a-b)$. Das kann man für Q_0, \dots, Q_{10} direkt sehen, man kann es aber auch allgemein beweisen (wie?) Hieraus und aus (14.1) folgt: Die vorletzte Endziffer einer Quadratzahl Q_n kann nur in „2-er Schritten“ weiterlaufen. Ausserdem sieht man: Ist $y_0 = 5$, so gilt $20 \cdot y_1 \cdot y_0 = 0 \pmod{100}$, also ist hier nur 25 für die beiden letzten Ziffern möglich. Natürlich tauchen alle Zahlen aus Satz 14.1 als mögliche Endziffern auf!

Daher erhalten wir folgendes Ergebnis:

Satz 14.2 *Ist $a = n^2 \geq 10$ eine Quadratzahl, so sind die beiden letzten Ziffern in folgender Tabelle wiederzufinden:*

Endziffer					
0	00				
1	01	21	41	61	81
4	04	24	44	64	84
5	25	0	0	0	0
6	16	36	56	76	96
9	09	29	49	69	89

Beispiel Ist 2354 eine Quadratzahl? Nein, denn 54 taucht nicht in der Tabelle auf.

Diese Tests liefern immer nur hinreichende Bedingungen dafür, dass eine Zahl **keine** Quadratzahl ist! Bei einer zufällig herausgegriffenen Zahl ist die Wahrscheinlichkeit, dass man keine Quadratzahl hat, allerdings viel größer als die, eine Quadratzahl zu erwischen. Insofern sind diese Kriterien auch das, was man „mehr“ braucht.

Weitere Test sind z.B. solche auf mögliche Reste nach Teilen durch 9 oder 11. Die prinzipielle Überlegung ist immer ähnlich: Ist $a = n^2$, und $b \in \mathbb{N}$ eine gegebene Zahl, so erhalten wir nach Division durch b mit Rest $n = bs + t$, also

$$n^2 = b^2s^2 + 2bs + t^2 \Rightarrow n^2 \bmod b = t^2 \bmod b,$$

weil die beiden ersten Summanden auf der rechten Seite durch b teilbar sind. Durchprobieren der Zahlen $0, 1, 2, \dots, b - 1$ liefert dann die möglichen Reste nach Teilen durch b . Für $b = 9$ oder $b = 11$ erhalten wir:

Satz 14.3 *Eine Zahl a ist genau dann eine Quadratzahl,*
 - *wenn sich beim Teilen durch 9 der Rest 0, 1, 4 oder 7 ergibt,*
 - *wenn sich beim Teilen durch 11 der Rest 0, 1, 3, 4, 5 oder 9 ergibt.*

Diese beiden Regeln sind deshalb praktisch, weil sich bei a durch 9 (11) der gleiche Rest wie beim Teilen der Quersumme (der alternierenden Quersumme) durch 9 (11) ergibt.

Beispiel $a = 122176$: 76 taucht in der Tabelle in Satz 14.2 auf, $a \bmod 9 = 19 \bmod 9$, und $19 : 9 = 2 \text{ Rest } 1$, ist auch kein Widerspruch, allerdings ist die alternierende Quersumme von $a = -6 + 7 - 1 + 2 - 2 + 1 = -1$, und $-1 : 11 = -1 \text{ Rest } 10$, (da $-1 = -1 \cdot 11 + 10$) daher ist a keine Quadratzahl.

Weitere Eigenschaften von Quadratzahlen

Ist n ungerade, so gibt es ein k mit $n = 2k + 1$ ($n = 5$: $k = 2$; $n = 27$: $k = ?$) \Rightarrow

$$2k + 1 = (k + 1)^2 - k^2 \text{ (binomische Formel oder Punktmenge anschauen)}. \quad (14.2)$$

Fazit: *Ungerade Zahlen lassen sich immer als Differenz zweier Quadratzahlen darstellen.*

Ebenfalls durch Betrachten der Punktfolgen gelangt man zu der Einsicht:

Die Quadratzahl Q_n ist die Summe der ersten n ungeraden Zahlen. Also

$$n^2 = 1 + 2 + 5 + \dots + (2n - 1).$$

Das kann man auch mit (14.2) machen:

$$\begin{array}{llll} k = 0 : & 1 & = & 1^2 - 0 & (1. \text{ Gleichung}) \\ k = 1 : & 3 & = & 2^2 - 1^2 & (2. \text{ Gleichung}) \\ k = 2 : & 5 & = & 3^2 - 2^2 & (3. \text{ Gleichung}) \\ k = 3 : & 7 & = & 4^2 - 3^2 & (4. \text{ Gleichung}) \\ & & & \vdots & \\ k = n - 2 : & 2n - 3 & = & (n - 1)^2 - (n - 2)^2 & ((n-1)\text{te Gleichung}) \\ k = n - 1 : & 2n - 1 & = & n^2 - (n - 1)^2 & (n\text{-te Gleichung}) \end{array}$$

Jetzt addiert man alles und erhält die Behauptung.

Somit ist auch klar, wie man Tabellen von Quadratzahlen ohne Multiplikation erhält. Die Darstellung ungerader Zahlen durch zwei Quadrate ist nicht unbedingt eindeutig, denn es gilt immer: Ist $a \cdot b$ ungerade, so ist

$$a \cdot b = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2. \quad (14.3)$$

(Diese Formel gilt eigentlich immer, wozu braucht man $a \cdot b$ ungerade?) Diese Formel wurde schon von den Babyloniern zum Multiplizieren benutzt, für Quadratzahlen benutzten sie Tabellen. Auf diese Art erhält man z.B.

$$99 = 50^2 - 49^2 = 2500 - 2401 = 10^2 - 1^2.$$

Ist allerdings $p > 2$ eine Primzahl, so gibt es nur eine Darstellung $p = x^2 - y^2$, mit $x = (p+1)/2$, $y = (p-1)/2$. und umgekehrt.

Zwei weitere Fragestellungen im Zusammenhang mit Quadratzahlen:

1. Wieviele Quadratzahlen braucht man, um jede natürliche Zahl als deren Summe darzustellen?

M.a.W.: Wann gilt $n = a_1^2 + \dots + a_k^2$ mit *festem* k und für *jedes* n ?

$k \geq 4$: Denn $7 = 2^2 + 1^2 + 1^2 + 1^2$.

Man kommt mit 4 Quadratzahlen aus, das sagt der Vier-Quadrate Satz von Lagrange. (Joseph Louis Lagrange 1736 - 1813)

Schon in der Antike interessierte man sich besonders für die Frage:

2. Für welche $a, b, c \in \mathbb{N}$ gilt $a^2 + b^2 = c^2$?

Definition und Bemerkung

1. Ein Tripel (a, b, c) mit $a, b, c \in \mathbb{N}$ und $a^2 + b^2 = c^2$ heißt *Pytharoräisches Zahlentripel*.
2. Es gibt unendlich viele solche Tripel (das wusste schon Pythagoras (ca 570-480 v. Ch.)), nämlich $(2n+1, 2n^2+2n, 2n^2+2n+1)$. Beispiele hierfür: $(3, 4, 5)$, $(5, 12, 13)$, ... Man erhält aber nicht alle Pytharoräischen Zahlentripel auf diese Art: Beispiel: $8^2 + 15^2 = 17^2$.
3. Man kann solche Tripel auch mit Hilfe von Quadratzahlen erzeugen: Für beliebiges $n > m$ ist $(n^2 - m^2, 2mn, n^2 + m^2)$ (was passiert bei $n = m$?) ein Pytharoräisches Zahlentripel. Diese Formeln zur Erzeugung von Pytharoräischen Zahlentripel nennt man *indische Formeln*, da sie von dem indischen Mathematiker und Astronom Brahmagupta (um 600 n. Ch.) in einem Lehrbuch angegeben wurden. Diese Formel erhält man aber auch aus (14.3), wenn man $a = m^2$ und $b = n^2$ einsetzt. Beispiel: $m = 1$, $n = 4$ liefert $(15, 8, 17)$.

Die indischen Formeln geben die Antwort auf die zweite Frage:

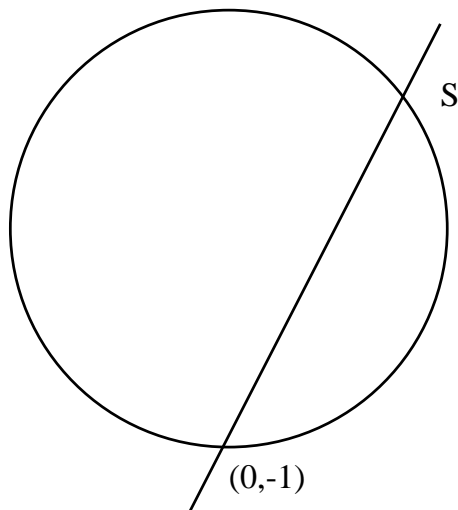
Satz 14.4 *Die indischen Formeln liefern alle Pytharoräischen Zahlentripel.*

BEWEIS

Ist (a, b, c) ein Pythagoräisches Tripel, so ist der Punkt mit den Koordinaten $x = a/c$, $y = b/c$ ein Punkt auf dem Einheitskreis mit rationalen Koordinaten.

(Umgekehrt: Wie bekommt man aus Punkten mit rationalen Koordinaten Pythagoräische Zahlentripel?)

Jeden Punkt (x, y) auf dem Einheitskreis ohne $(0, 1)$ erhält man als Schnittpunkt S mit der Geraden $y = \lambda x - 1$ mit geeignetem λ . Setzt man die Geradengleichung in die Kreis-



gleichung $x^2 + y^2 = 1$ ein, so erhält man die beiden Schnittpunkte $(-1, 0)$ (liefert natürlich immer ein Pythagoräisches Tripel, ist aber nicht so spannend), und

$$S = \left(\frac{2\lambda}{\lambda^2 + 1}, \frac{\lambda^2 - 1}{\lambda^2 + 1} \right).$$

S hat rationale Koordinaten, genau dann wenn λ rational ist, also $\lambda = \frac{m}{n}$. \Rightarrow

$$S = \left(\frac{2mn}{m^2 + n^2}, \frac{m^2 - n^2}{m^2 + n^2} \right).$$

Weil man ja zusätzlich noch weiss, dass S auf dem Einheitskreis liegt:

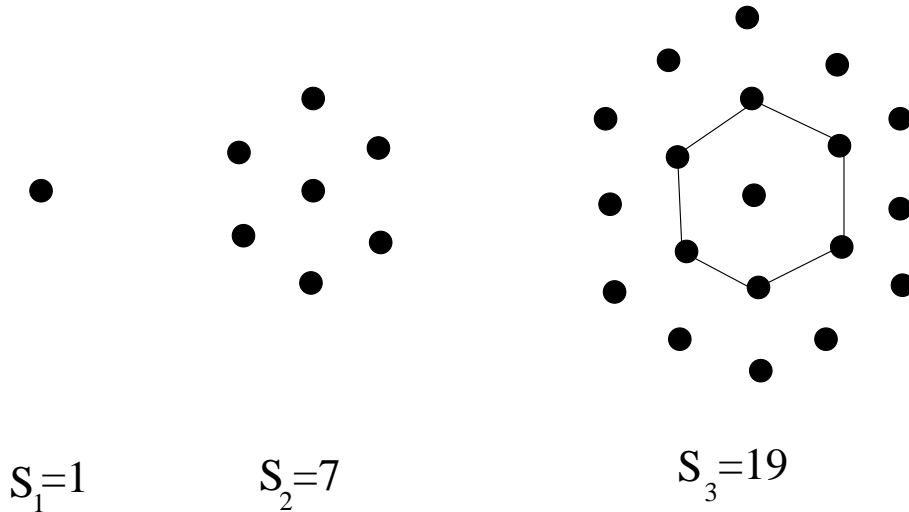
$$(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2.$$

Fermats letzter Satz

Man kann die obige Fragestellungen verallgemeinern, indem man statt 2 einen beliebigen Exponenten zulässt: Wieviele Zahlentripel (a, b, c) mit $a, b, c \in \mathbb{N}$ gibt es, so dass die Gleichung $a^k + b^k = c^k$ erfüllt ist bei gegebenem $k \in \mathbb{N}$, $k \geq 3$. Zwei gibt es immer $(1, 0, 1)$, $(0, 1, 1)$. Fermat (Pierre de Fermat, 1601-1665, eigentlich Jurist und „Hobymathematiker“) notierte am Rand einer Übersetzung der „Arithmetica“ von Diophant die Vermutung, dass es keine weiteren Lösungen dieser Gleichungen für $k \geq 3$ gibt. Er behauptete auch, einen Beweis dafür zu haben. Diese *Fermatsche Vermutung* war über 300 Jahre lang eines der berühmtesten offenen Probleme der Mathematik, und wurde erst 1993 von Andrew Wiles endgültig bewiesen.

14.3 Sechseckzahlen

Als Sechseckzahlen S_1, S_2, S_3, \dots bezeichnet man die Anzahlen von Punkten in den folgenden Sechsecken



Hierbei legt man um jedes bereits entstandene Sechseck ein weiteres mit einer um 1 erhöhten Seitenlänge. Für $n \in \mathbb{N}$ gilt also

$$\begin{aligned}
 S_{n+1} &= S_n + 6 \cdot n \\
 &= S_{n-1} + 6 \cdot (n-1) + 6 \cdot n \\
 &\vdots \\
 &= 1 + 6 + 6 \cdot 2 + \dots + 6 \cdot (n-1) + 6 \cdot n \\
 &= 1 + 6 \cdot \sum_{i=1}^n i \\
 &= 1 + 6 \frac{n(n+1)}{2} \\
 &= 1 + 3n^2 + 3n.
 \end{aligned}$$

Diese Rechnung “enthält” auch eine Beziehung zwischen den Sechseck- und den Dreieckzahlen:

$$S_{n+1} = 1 + 6D_n \quad \text{für } n \in \mathbb{N}.$$

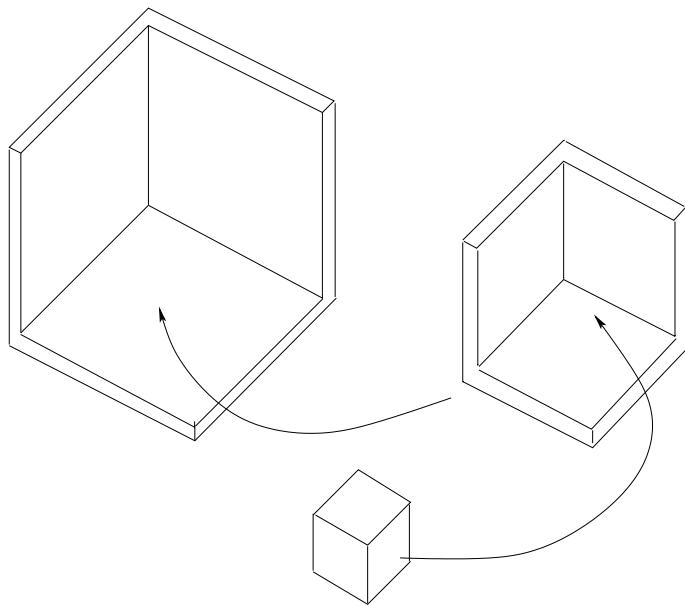
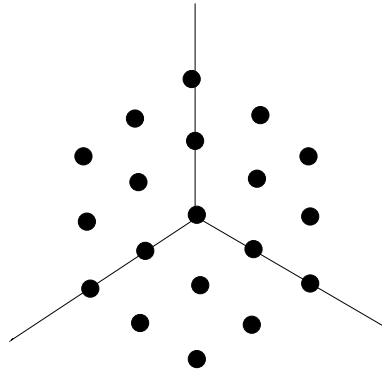
Wir wollen noch sehen wie sich die Endformel (für $n \in \mathbb{N}$)

$$S_n = 1 + 3(n-1)^2 + 3(n-1) = 3n^2 - 3n + 1 \tag{14.4}$$

geometrisch interpretieren läßt:

Diese Interpretation erlaubt (14.4) direkt (ohne Rechnung) “abzulesen”.

Ferner sieht man durch “Aneinanderreihen von Schichten” zu einem Würfel, d.h.



die Identität

$$n^3 = S_1 + S_2 + S_3 + \dots + S_n$$

ein. Daraus folgt unmittelbar für $n \in \mathbb{N}$

$$\begin{aligned}(n+1)^3 &= n^3 + S_{n+1} \\ &= n^3 + 3 \cdot n^2 - 3 \cdot n + 1 \\ &= n^3 + 3n^2 + 3n + 1.\end{aligned}\tag{14.5}$$

Natürlich könnten wir (14.5) auch leicht durch “Ausmultiplizieren” verifizieren.

15 Vollständige Induktion

Wir beschäftigen uns noch einmal mit der Identität

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2} \quad \text{für } n \in \mathbb{N} \quad (15.1)$$

und geben für diese im folgenden einen alternativen Beweis.

Zunächst könnten wir (15.1) für einige n “durchprobieren” und würden dabei feststellen, daß beide Seiten gleiche Ergebnisse liefern. Das wäre natürlich kein Beweis dafür, daß (15.1) für alle $n \in \mathbb{N}$ richtig ist: Betrachten Sie (zur Warnung!) z.B. die Behauptung:

$$n^2 + n + 41 \text{ ist eine Primzahl.}$$

Dies ist für $n = 1, 2, \dots, 39$ wahr und erst für $n = 40$ (wegen $40^2 + 40 + 41 = 41 \cdot 41$) falsch.

Wir überlegen uns nun folgendes: Wir bezeichnen die Aussage (15.1) für ein bestimmtes $n \in \mathbb{N}$ als $A(n)$. Daß die Aussage $A(1)$ wahr ist, können wir einfach durch einsetzen verifizieren. Angenommen wir hätten, daß für (beliebiges) $n \in \mathbb{N}$ gilt

$$A(n) \text{ wahr} \implies A(n+1) \text{ wahr}, \quad (15.2)$$

so könnten wir folgern

$$A(1) \implies A(2) \implies A(3) \implies \dots \quad (15.3)$$

Bevor wir nun diese Aussagenkette weiter “interpretieren”, prüfen wir, ob in unserem Beispiel (15.2) gilt: Wir nehmen also an, daß

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$$

für (irgendein) $n \in \mathbb{N}$ wahr ist. Dann gilt für $n+1$

$$\begin{aligned} 1 + 2 + 3 + \dots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Damit haben wir für unser Beispielproblem (15.2) gezeigt, und können damit (15.3) folgern.

“Erwischen” wir aber in (15.3) alle $n \in \mathbb{N}$, bzw., haben wir damit tatsächlich bewiesen, daß $A(n)$ für alle $n \in \mathbb{N}$ wahr ist?

Angenommen, daß wäre nicht der Fall, d.h., angenommen, es gäbe ein $m \in \mathbb{N}$ für das $A(m)$ falsch ist. Dann gäbe es (und so haben wir schon öfter argumentiert!) ein kleinstes $m \in \mathbb{N}$ für das $A(m)$ falsch ist. Da $A(1)$ wahr ist, muß $m > 1$ sein, also $m-1 \geq 1$ gelten.

Nun ist aber (wegen der Minimalität von m) $A(m - 1)$ wahr und daraus folgt wegen (15.2), daß auch $A(m)$ wahr sein muß. Widerspruch! Also: $A(m)$ ist für alle $m \in \mathbb{N}$ wahr.

Damit können wir aus unserer obigen Argumentation tatsächlich die Summenformel für alle $n \in \mathbb{N}$ folgern!!!

Zusammenfassend: Unter der Voraussetzung, daß **jede nichtleere Teilmenge der natürlichen Zahlen ein kleinstes Element besitzt** (Dies nennt man übrigens das *Wohlordnungsprinzip*. Wer wollte dies in Frage stellen?), haben wir für die Menge von Aussagen $A(n)$, $n \in \mathbb{N}$, gezeigt: Ist

- i) $A(1)$ wahr, und gilt
- ii) für $n \in \mathbb{N}$: $A(n)$ wahr $\implies A(n + 1)$ wahr,

so ist

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

Schritt i) nennt man den *Induktionsanfang*, Schritt ii) den *Induktionsschritt* und darin “ $A(n)$ wahr” die *Induktionsvoraussetzung* und “ $A(n + 1)$ wahr” die *Induktionsbehauptung*.

Hat man eine Menge von Aussagen $A(n)$ für $n \in \mathbb{N}$ mit $n \geq k \in \mathbb{N}$, $k \in \mathbb{N}$, gegeben, so ist natürlich der Induktionsanfang “ $A(1)$ wahr” durch “ $A(k)$ wahr” zu ersetzen und der Induktionsschritt für $n \in \mathbb{N}$ mit $n \geq k$ zu beweisen.

Unabhängig davon bezeichnet man dieses Vorgehen als *vollständige Induktion*. Daß durch dieses Vorgehen die Wahrheit von $A(n)$ für alle $n \in \mathbb{N}$ bewiesen ist, nennt man das *Prinzip der vollständigen Induktion*.

Bemerkung. Es wurde oben bewiesen, daß aus dem Wohlordnungsprinzip das Prinzip der vollständigen Induktion folgt. Äquivalent hätten wir dieses auch aus dem Dirichlet’schen Schubfachprinzip folgern können. Dieses besagt: Wenn ich $m \in \mathbb{N}$ Gegenstände auf $n \in \mathbb{N}$ Schubfächer mit $n < m$ verteile, dann liegt in wenigstens einem Schubfach mehr als ein Element. Dieses erscheint genauso evident wie das Wohlordnungsprinzip, wogegen gegen das Prinzip der vollständigen Induktion eher Vorbehalte formuliert werden könnten. Erwähnt sei (und das ist nicht schwierig zu beweisen, siehe z.B. F.Padberg, R.Danckwert, M.Stein, *Zahlbereiche*), daß diese drei Prinzipien tatsächlich äquivalent sind. Ausserdem: Will man die Menge \mathbb{N} der natürlichen Zahlen charakterisieren führt letztlich um die Induktionseigenschaft kein Weg herum. Die für die Kardinalzahlen hergeleiteten Rechenregeln z.B. reichen nicht aus. Andererseits ist es nicht notwendig alle von uns für Kardinalzahlen hergeleiteten Rechenregeln in einer Charakterisierung zu berücksichtigen. Das bekannteste (die Induktionseigenschaft als ein Axiom enthaltende) Axiomensystem stammt von Peano. Vgl. dazu auch die Bemerkungen und Hinweise in dem oben erwähnten Buch von F.Padberg et al. oder auch in A.Kirsch, *Mathematik wirklich verstehen*.

Nun aber zu weiteren Beispielen für die Anwendung der vollständigen Induktion.

a) Für $n \in \mathbb{N}$ gilt

$$\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}. \quad (15.4)$$

Beweis. Die Aussage $A(n)$ ist hier $\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}$.

Induktionsanfang: $A(1)$ ist richtig, es gilt nämlich: Für $n = 1$ ergibt die linke Seite von (15.4) 1 und die rechte Seite $\frac{1(1+1)(2 \cdot 1+1)}{6} = 1$.

Induktionsschritt: Für ein $n \in \mathbb{N}$ gelte (15.4), d.h. $A(n)$ sei wahr. Zu zeigen ist, daß daraus die Richtigkeit von $A(n+1)$ folgt. Es ergibt sich

$$\begin{aligned} \sum_{i=1}^{n+1} i^2 &= \sum_{i=1}^n i^2 + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= (n+1) \frac{n(2n+1) + 6(n+1)}{6} \\ &= \frac{n+1}{6} (2n^2 + 7n + 6). \end{aligned}$$

Andererseits ist

$$\begin{aligned} \frac{(n+1)(n+2)(2(n+1)+1)}{6} &= \frac{n+1}{6} (n+2)(2n+3) \\ &= \frac{n+1}{6} (2n^2 + 7n + 6). \end{aligned}$$

Also folgt aus der Richtigkeit von $A(n)$ stets die Richtigkeit von $A(n+1)$. Der Satz ist damit bewiesen. ■

b) Für $n \in \mathbb{N}$ gilt

$$n^2 + n \text{ ist eine gerade Zahl.} \quad (15.5)$$

Beweis.

Induktionsanfang: Für $n = 1$ ist $1^2 + 1 = 2$ eine gerade Zahl.

Induktionsschritt: Für $n \in \mathbb{N}$ sei $n^2 + n$ eine gerade Zahl. Dann gilt

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

$n^2 + n$ ist nach Induktionsvoraussetzung eine gerade Zahl und $2(n+1)$ ist offenbar auch eine gerade Zahl. Da eine Summe gerader Zahlen gerade ist, muß $(n+1)^2 + (n+1)$ ebenfalls gerade sein. ■

(Beweis ohne vollständige Induktion: Für $n \in \mathbb{N}$ ist $n^2 + n = n(n+1)$. Da entweder n oder $n+1$ eine gerade Zahl ist, muß $n^2 + n$ gerade sein.)

c) Für $x \in \mathbb{R}$ mit $x \geq -1$ und $n \in \mathbb{N}$ gilt

$$(1+x)^n \geq 1 + nx. \quad (15.6)$$

Beweis.

Induktionsanfang: Für $n = 1$ gilt

$$(1 + x)^1 \geq 1 + 1 \cdot x$$

für $x \geq -1$.

Induktionsschritt: Für $n \in \mathbb{N}$ und $x \geq -1$ gelte (15.6). Dann gilt

$$\begin{aligned}(1 + x)^{n+1} &= (1 + x)^n(1 + x) \\ &\geq (1 + nx)(1 + x) \\ &= 1 + (n + 1)x + nx^2 \\ &\geq 1 + (n + 1)x,\end{aligned}$$

da $(1 + x) \geq 0$ für $x \geq -1$ und $nx^2 \geq 0$. ■

d) Für $n \in \mathbb{N}$ mit $n > 4$ gilt

$$2^n > n^2. \tag{15.7}$$

Beweis.

Induktionsanfang: Für $n = 5$ ist $2^5 = 32$ und $5^2 = 25$, also $2^5 > 5^2$.

Induktionsschritt: Für $n \in \mathbb{N}$ mit $n > 4$ gelte

$$2^n > n^2.$$

Dann ergibt sich

$$\begin{aligned}2^{n+1} &= 2 \cdot 2^n \\ &> 2 \cdot n^2 = n^2 + n \cdot n \\ &> n^2 + 4 \cdot n = n^2 + 2n + 2n \\ &> n^2 + 2n + 1 \\ &= (n + 1)^2.\end{aligned}$$
■

e) Für $n \in \mathbb{N}$ gilt

$$\sum_{i=1}^n \frac{1}{i(i+1)} = 1 - \frac{1}{n+1}. \tag{15.8}$$

Beweis.

Induktionsanfang: Für $n = 1$ ist $\frac{1}{1(1+1)} = 1/2$ und $1 - \frac{1}{1+1} = 1/2$.

Induktionsschritt: Für $n \in \mathbb{N}$ gelte

$$\sum_{i=1}^n \frac{1}{i(i+1)} = 1 - \frac{1}{n+1}.$$

Daraus folgt

$$\begin{aligned}\sum_{i=1}^{n+1} \frac{1}{i(i+1)} &= \sum_{i=1}^n \frac{1}{i(i+1)} + \frac{1}{(n+1)(n+2)} \\ &= 1 - \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} \\ &= 1 - \frac{n+2-1}{(n+1)(n+2)} \\ &= 1 - \frac{1}{n+2}.\end{aligned}$$

■

Wir werden in den folgenden Abschnitten und insbesondere im nächsten Semester (z.B. in der “Elementaren Kombinatorik”) wiederholt feststellen, daß die vollständige Induktion ein äußerst nützliches Werkzeug ist.

Bemerkungen

a) Auf den Induktionsanfang kann nicht verzichtet werden, oder mit anderen Worten: Aus “ $A(n)$ wahr $\implies A(n+1)$ wahr” für $n \in \mathbb{N}$ folgt noch lange nicht “ $A(n)$ wahr für $n \in \mathbb{N}$ ”.

Behauptung: Für alle $n \in \mathbb{N}$ gilt $3 + 3^2 + 3^3 + \dots + 3^n = \frac{3}{2}3^n$.

Induktionsschritt: Für $n \in \mathbb{N}$ gelte $3 + 3^2 + 3^3 + \dots + 3^n = \frac{3}{2}3^n$. Daraus folgt für $n+1$

$$3 + 3^2 + 3^3 + \dots + 3^n + 3^{n+1} = \frac{3}{2}3^n + 3^{n+1} = \frac{3}{2}3^{n+1}.$$

Damit ist allerdings die Behauptung noch nicht für alle $n \in \mathbb{N}$ bewiesen. Tatsächlich ist diese sogar für alle $n \in \mathbb{N}$ offensichtlich falsch, da $3 + 3^2 + 3^3 + \dots + 3^n \in \mathbb{N}$ und $\frac{3}{2}3^n \notin \mathbb{N}$ für alle $n \in \mathbb{N}$ gilt. $n=1$ liefert z.B. $3 \neq \frac{9}{2}$.

b) Ein weiteres Beispiel für eine Induktion, die nicht bei $n=1$ anfängt, liefert die

Behauptung: In jedem n -Eck ($n \geq 3$) beträgt die Summe der Innenwinkel $(n-2) \cdot 180^\circ$.

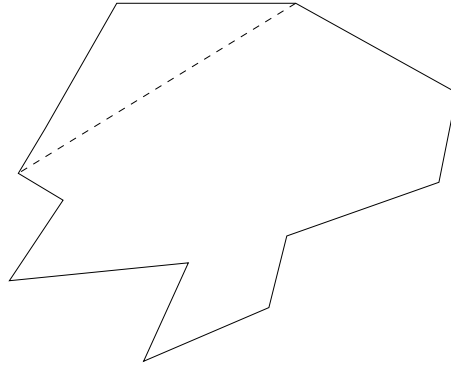
Induktionsanfang: Für $n=3$ ist die Aussage klar, da die Summe der Winkel in jedem Dreieck bekanntermaßen 180° beträgt.

Induktionsschritt: Die Summe der Innenwinkel in einem n -Eck betrage $(n-2) \cdot 180^\circ$. Daraus folgt für ein $n+1$ -Eck durch Ergänzen einer Verbindungslinie

für die Summe der Innenwinkel $(n-2) \cdot 180^\circ + 180^\circ = ((n+1)-2) \cdot 180^\circ$.

Abschließend eine etwas weniger triviale Variante der vollständigen Induktion anhand eines Beispiels von Cauchy: Für $n \in \mathbb{N}$ mit $n \geq 2$ gilt für beliebige positive Zahlen a_1, \dots, a_n

$$\sqrt[n]{a_1 \cdot a_2 \cdot \dots \cdot a_n} \leq \frac{a_1 + a_2 + \dots + a_n}{n}. \quad (15.9)$$



Den Term auf der linken Seite nennt man das *geometrische Mittel*, den Term auf der rechten Seite das *arithmetisches Mittel*.

Bezeichnet man die vorliegende Behauptung (15.9) für $n \in \mathbb{N}$ mit $A(n)$, so werden wir zeigen:

- i) $A(2)$ ist wahr.
- ii) Für $n \in \mathbb{N}, n \geq 2$: $A(n)$ wahr $\implies A(2n)$ wahr.
- iii) Für $n \in \mathbb{N}, n \geq 2$: $A(n+1)$ wahr $\implies A(n)$ richtig.

i) – iii) erlaubt dann offenbar zu folgern: $A(n)$ ist richtig für alle $n \in \mathbb{N}$ mit $n \geq 2$.

Zu i) Wegen $0 \leq (a_1 - a_2)^2 = a_1^2 - 2a_1a_2 + a_2^2$ gilt

$$4a_1a_2 \leq a_1^2 + 2a_1a_2 + a_2^2 = (a_1 + a_2)^2,$$

also

$$\sqrt{a_1a_2} \leq \frac{a_1 + a_2}{2}.$$

Zu ii) Es gelte $\sqrt[n]{a_1 \cdot a_2 \cdot \dots \cdot a_n} \leq \frac{a_1 + a_2 + \dots + a_n}{n}$. Daraus folgt

$$\begin{aligned} \sqrt[2n]{a_1 \cdot \dots \cdot a_n a_{n+1} \cdot \dots \cdot a_{2n}} &= \sqrt[n]{\sqrt{a_1 \cdot a_{n+1}} \cdot \dots \cdot \sqrt{a_n \cdot a_{2n}}} \\ &\leq \frac{\sqrt{a_1 \cdot a_{n+1}} + \dots + \sqrt{a_n \cdot a_{2n}}}{n} \\ &\leq \frac{\frac{a_1 + a_{n+1}}{2} + \dots + \frac{a_n + a_{2n}}{2}}{n} \\ &= \frac{a_1 + \dots + a_n + a_{n+1} + \dots + a_{2n}}{2n}. \end{aligned}$$

Zu iii) Es gelte $\sqrt[n+1]{a_1 \cdot a_2 \cdot \dots \cdot a_n a_{n+1}} \leq \frac{a_1 + a_2 + \dots + a_n + a_{n+1}}{n+1}$. Daraus folgt für $a_{n+1} = \frac{a_1 + a_2 + \dots + a_n}{n}$

$$\begin{aligned} \sqrt[n+1]{a_1 \cdot a_2 \cdot \dots \cdot a_n \frac{a_1 + a_2 + \dots + a_n}{n}} &\leq \frac{a_1 + a_2 + \dots + a_n + \frac{a_1 + a_2 + \dots + a_n}{n}}{n+1} \\ &= \frac{a_1 + a_2 + \dots + a_n}{n}, \end{aligned}$$

also

$$a_1 \cdot a_2 \cdot \dots \cdot a_n \frac{a_1 + a_2 + \dots + a_n}{n} \leq \left(\frac{a_1 + a_2 + \dots + a_n}{n} \right)^{n+1}$$

und somit

$$a_1 \cdot a_2 \cdot \dots \cdot a_n \leq \left(\frac{a_1 + a_2 + \dots + a_n}{n} \right)^n$$

und

$$\sqrt[n]{a_1 \cdot a_2 \cdot \dots \cdot a_n} \leq \frac{a_1 + a_2 + \dots + a_n}{n}.$$