Einleitung

Zunächst wiederholen wir einige Bezeichnungen, die Sie hoffentlich schon aus der Schule kennen. Insbesondere benutzen wir die Abkürzungen $\mathbb{N} := \{1, 2, 3, 4, \dots\}$ *Menge der natürlichen Zahlen* und $\mathbb{Z} := \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$ *Menge der ganzen Zahlen.*

Bemerkung. Bitte beachten Sie, dass wir 0 nicht als natürliche Zahl auffassen. Das ist eine Frage der Konvention, also letztlich willkürlich, und hat keinen tieferen mathemtischen Hintergrund. Die um 0 erweiterte Menge der natürlichen Zahlen wird mit $\mathbb{N}_0$ bezeichnet.

Weitere wichtige Mengen, die Sie in den Schule kennengelernt haben sollten, sind

$\mathbb{Q}$, die Menge der rationalen Zahlen

$\mathbb{R}$, die Menge der reellen Zahlen.

Schließlich haben Sie die Punkte in der Ebene mit Koordinaten beschrieben:

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} := \big\{(x, y)\,;\ x, y \in \mathbb{R}\big\}$$

Analog kann man auch $\mathbb{N}^2$ usw. erklären.

Keine dieser Beschreibungen ist eine Definition im mathematischen Sinne. Eines der Ziele dieser Vorlesung wird es sein, eine präzise Definition aller beschriebenen Mengen zu geben.

Dazu werden wir *axiomatisch* vorgehen. Das bedeutet, dass wir aus wenigen (unbewiesenen) Grundaussagen, den **Axiomen**, alle anderen Aussagen mit Hilfe logischer Schlüsse beweisen.

So werden wir die Menge $\mathbb{N}$ der natürlichen Zahlen mit Hilfe der *Peano Axiome* konstruieren und alle wichtigen Eigenschaften beweisen können.

Diese Vorgehensweise erfordert eine hohe sprachliche Präzision, die Sie im Rahmen dieser Vorlesung erlernen sollen. Grundlage dafür wiederum ist die Mengenlehre. Tatsächlich lassen sich alle Begriffe der modernen Mathematik auf Mengen zurückführen.

Ein axiomatischer Zugang zur Mengenlehre würde den Rahmen dieser Veranstaltung sprengen. Übrigens trifft das auch für die Anfängervorlesungen der anderen Mathemtikstudiengänge zu. Wir starten also mit einem „naiven“ Zugang zur Mengenlehre. Wer sich dennoch mit axiomatischer Mengenlehre befassen möchte, kann in [Ebb03] oder [SS09] nachlesen.

Noch bevor wir die oben beschriebenen Mengen (wie $\mathbb{N}$ usw.) präzise definiert haben, werden wir diese Mengen benutzen, um anschauliche und (hoffentlich) leicht verständliche Beispiele für einige der abstrakten Konstrukte zu bekommen, die in den folgenden Kapiteln auftreten werden.

Obwohl diese Vorgehensweise scheinbar widersprüchlich ist und Puristen sie ablehnen würden, erscheint sie doch aus didaktischen Gründen sinnvoll.

1 Mengenlehre und Aussagenlogik

Wir beschäftigen uns also mit Mengen und ihren Beziehungen zueinander. Zeitgleich werden wir in den Übungen *Aussagen* behandeln. Mehr dazu finden Sie im Abschnitt „Ausagenlogik“ ab Seite 7. Dabei werden wir eine tiefliegende und wichtige Analogie zwischen den beiden Gebieten erkennen.

Mengen

Die folgende „Definition“ (Festlegung) geht auf den großen deutschen Mathematiker Georg Cantor[1] (1845–1918) zurück:

(1.1) Definition. Eine **Menge** ist eine Zusammenfassung von wohlbestimmten und wohlunterschiedenen Objekten unseres Denkens oder unserer Anschauung zu einem Ganzen.

(1.2) Bemerkung. 1. Hierbei bedeutet

wohlbestimmt, dass es eindeutig feststellbar ist, ob ein Objekt x zu einer Menge M gehört oder nicht, in Zeichen $x \in M$ oder $x \notin M$, in Worten: „x ist (nicht) Element von M“.

wohlunterschieden, dass jedes Objekt maximal einmal zu einer Menge gehört.

2. Statt von *Objekten* spricht man heute von **Elementen** einer Menge.

3. (1.1) ist keine „richtige“ Definition, da der neue Begriff „Menge“ nicht auf schon bekannte Begriffe zurückgeführt wird. Daher spricht man von „naiver“ Mengenlehre.

4. Eine strenge Fundierung der Mengenlehre im Sinne einer Axiomatik ist keineswegs einfach.

5. Links zum Thema:

   - Einführung in Mengen[2] (Mathe online Wien).
   - Überblick zur Mengenlehre[3] in der Enzyklopädie *Wikipedia*.

(1.3) Beispiele. 1. Die Menge aller Personen im Hörsaal.

2. Die Menge aller Primzahlen zwischen 10 und 30.

3. $\mathbb{N}$, $\mathbb{Z}$ usw.

4. Die Menge aller guten Mathematikstudenten. (?)

[1] `https://de.wikipedia.org/wiki/Georg_Cantor`
[2] `http://www.mathe-online.at/mathint/mengen/i.html`
[3] `https://de.wikipedia.org/wiki/Mengenlehre`

5. Die Menge der Buchstaben $\mathcal{B}$, aus denen das Wort SEMESTER gebildet wird.
6. $\{z \in \mathbb{Z};\ z^2 - z = 6\} = \{-2, 3\}$ und $\{z \in \mathbb{N};\ z^2 - z = 6\} = \{3\}$.
7. Jede Gerade der Anschauungsebene ist eine Menge von Punkten.
8. Die Menge $\mathfrak{G}$ aller Geraden hat als Elemente selbst Mengen.

Mengen können angegeben werden durch

- eine (evt. unvollständige) Auflistung aller Elemente (vgl. Bsp'e. 3.,6.)
- durch Angabe von Eigenschaften (vgl. Bsp'e. 1.,2.,5.,6.).

Stets werden sie eingerahmt durch die **Mengenklammern** { und }. Die Menge aus dem Beispiel 5. kann auch durch Auflistung beschrieben werden, etwa $\mathcal{B} = \{S, E, M, T, R\}$, aber auch $\mathcal{B} = \{E, M, R, S, T\}$. Es kommt nicht auf die Reihenfolge der Elemente an.

Bemerkung. Bei der Beschreibung der Mengen aus Bsp. 5 steht hinter dem ; eine Aussage (im Bsp. $z^2 - z = 6$), die von einer Variablen (im Bsp. z) abhängt. Diese Art der Beschreibung einer Menge ist die bei weitem Wichtigste. Mehr dazu in den Übungen.

(1.4) Definition. Seien A, B beliebige Mengen.

1. A heißt **Teilmenge** von B, geschrieben $A \subseteq B$, wenn jedes Element von A auch Element von B ist.
2. $A = B \ :\Longleftrightarrow\ A \subseteq B$ und $B \subseteq A$.
3. A heißt **echte Teilmenge** von B, geschrieben $A \subsetneqq B$, wenn jedes Element von A auch Element von B, aber $A \neq B$ ist.

Bemerkung. 1. Auf Grund der Definition ist jede Menge Teilmenge von sich selbst.

2. Das Zeichen $\subset$ wird in der Fachliteratur leider nicht einheitlich benutzt (echte/unechte Teilmenge). Durch unsere Schreibweise vermeiden wir Missverständnisse.
3. Die Bedeutung von $A \supseteq B$ liegt auf der Hand, wenn man diese Aussage von rechts nach links betrachtet: B ist Teilmenge von A oder A ist **Obermenge** von B. Ebenfalls selbsterklärend ist $A \not\subseteq B$: A ist keine Teilmenge von B.

(1.5) Beispiele. 1.) $\{1, 2, 3\} \subseteq \{1, \ldots, 10\} \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} (\subseteq \mathbb{C})$.

2.) $\{0, 1\} \not\subseteq \mathbb{N}$, da $0 \notin \mathbb{N}$.

3.) Menge der ungeraden natürlichen Zahlen $\{n \in \mathbb{N};\ \exists m \in \mathbb{N} : n = 2m - 1\} \subseteq \mathbb{N}$.

Enthält eine Menge kein einziges Element, so liegt die **leere Menge** vor, geschrieben $\varnothing$ oder manchmal auch $\{\,\}$. Es gibt nur *eine* leere Menge; so ist die Menge aller Primzahlen zwischen 24 und 28 gleich der Menge aller singenden Kugelfische. Die leere Menge ist Teilmenge jeder Menge.

Wir erklären die wichtigsten Rechenoperationen für Mengen.

(1.6) Definition. Es seien M eine Menge, und $A, B \subseteq M$.

1.) $A \cup B := \{x \in M\,;\, x \in A \text{ oder } x \in B\}$ heißt die **Vereinigung** von A und B.

2.) $A \cap B := \{x \in M\,;\, x \in A \text{ und } x \in B\}$ heißt der **Durchschnitt** von A und B.

3.) $A \backslash B := \{x \in M\,;\, x \in A \text{ und } x \notin B\}$ heißt die **Differenzmenge** von A und B (Reihenfolge von A und B wichtig!).

4.) $\overline{A} := \{x \in M\,;\, x \notin A\}$ heißt das **Komplement** von A (in M).

Bemerkung. Statt $\overline{A}$ wird auch oft A^c geschrieben, oder, wenn man die „Grundmenge“ (hier M) betonen will A^{c_M}.

Komplementbildung ist nur sinnvoll, wenn eine Grundmenge festgelegt ist.

Mengenoperationen können im **Venndiagramm** (Einzelheiten in der Vorlesung) veranschaulicht werden.

Wir formulieren einige Folgerungen, die man sich alle leicht mit Hilfe von Venndiagrammen klar machen kann.

(1.7) *Es seien M eine Menge und $A, B, C \subseteq M$. Dann gelten*

(1) $A \cap B = B \cap A, \qquad A \cup B = B \cup A$ *(**Kommutativgesetze**)*

(2) $A \cap (B \cap C) = (A \cap B) \cap C, \qquad A \cup (B \cup C) = (A \cup B) \cup C$ *(**Assoziativgesetze**)*

(3) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(**Distributivgesetze**)*

(4) $A \cap M = A, \quad A \cup M = M, \quad A \cap \varnothing = \varnothing, \quad A \cup \varnothing = A$

(5) $A \cap \overline{A} = \varnothing, \quad A \cup \overline{A} = M$

(6) $\overline{\overline{A}} = A$

(7) $\overline{A \cap B} = \overline{A} \cup \overline{B}, \quad \overline{A \cup B} = \overline{A} \cap \overline{B}$ *(Regeln von de Morgan)*

Wir verzichten hier auf die Beweise, zeigen aber wie man (7) $\overline{A \cap B} = \overline{A} \cup \overline{B}$ durch Fallunterscheidung in Tabellenform begründet. Es gibt vier möglich Fälle für ein Element $x \in M$:

$$x \in A \ \wedge \ x \in B, \qquad x \in A \ \wedge \ x \notin B, \qquad x \notin A \ \wedge \ x \in B, \qquad x \notin A \ \wedge \ x \notin B$$

In der Tabelle bedeutet
1: *ist Element von* 0: *ist nicht Element von.*

A	B	$A \cap B$	$\overline{A \cap B}$	$\overline{A}$	$\overline{B}$	$\overline{A} \cup \overline{B}$
1	1	1	**0**	0	0	**0**
1	0	0	**1**	0	1	**1**
0	1	0	**1**	1	0	**1**
0	0	0	**1**	1	1	**1**

Da die Einträge in den fett gekennzeichneten Spalten übereinstimmen, ist die Behauptung bewiesen. Die anderen Regel können analog bewiesen werden.

Bemerkung. In der Schule haben Sie eine anderes Distributivgesetz kennengelernt: $a \cdot (b + c) = a \cdot b + a \cdot c$ für alle reellen Zahlen a, b, c. Hier kann man die Rollen von $+$ und $\cdot$ nicht vertauschen.

(1.8) Definition. Seien A, B beliebige Mengen. Dann heißt

$$A \times B := \big\{(a, b)\,;\ a \in A, b \in B\big\} \quad \textbf{kartesisches Produkt} \text{ der Mengen } A \text{ und } B.$$

Bemerkung. Das Wort *kartesische* leitet sich vom Namen des bedeutenden Philosophen und Mathematikers René Descartes[4] (1596–1650) ab.

Ein Beispiel für das kartesische Produkt zweier Mengen ist Ihnen vielleicht bekannt: Beim Spiel *Schiffe versenken* wird die Lage einer jeden Schiffseinheit durch ein Paar (Buchstabe, Zahl) angegeben (kartesisches Produkt!).

Analog definiert man $A \times B \times C := \big\{(a, b, c)\,;\ a \in A, b \in B, c \in C\big\}$, usw.

(1.9) Beispiele. 1. $\{1, 2\} \times \{x, y\} = \{(1, x), (1, y), (2, x), (2, y)\}$.

2. $\{1, 2\}^3 := \{1, 2\} \times \{1, 2\} \times \{1, 2\} = \{(1, 1, 1), (1, 1, 2), \ldots, (2, 2, 2)\}$ (insgesamt acht Elemente)

3. $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$ als Punkte der Anschauungsebene.

4. $\mathbb{Z}^2 := \mathbb{Z} \times \mathbb{Z}$ als Gitterpunkte der Anschauungsebene.

[4] `https://de.wikipedia.org/wiki/Rene_Descartes`

5. Jedes Datum ist Element der Menge $\{1,\dots,31\}\times\{1,\dots,12\}\times\mathbb{Z}$

6. Studierende in einer Datenbank werden in einem kartesischen Produkt geführt. Ein Element hat etwa die Form $(\text{Matrikelnummer}, \text{Name}, \text{Vorname}, \dots)$

(1.10) Bemerkung. Besteht ein kartesisches Produkt aus endlichen Mengen, ist die Anzahl der Elemente gerade das Produkt der Anzahl der Elemente der beteiligten Mengen. Im Beispiel 2. ergeben sich $2\cdot 2\cdot 2 = 8$ Elemente.

(1.11) *Seien A, B, S, T beliebige Mengen. Dann gelten*

(1) $(A\cap B)\times(S\cap T) = (A\times S)\cap(B\times T)$

(2) $A\times(S\cup T) = (A\times S)\cup(A\times T)$

Beweis. (1) Sei $(x,y)\in(A\cap B)\times(S\cap T) \iff x\in(A\cap B)\wedge y\in(S\cap T)$
$\iff (x,y)\in(A\times S)\cap(B\times T)$.

(2) Sei $(a,x)\in A\times(S\cup T)$, dann gilt $a\in A\wedge x\in S\cup T$.

1. Fall: $x\in S \implies (a,x)\in A\times S \implies (a,x)\in(A\times S)\cup(A\times T)$

2. Fall: $x\notin S \implies x\in T \implies (a,x)\in A\times T \implies (a,x)\in(A\times S)\cup(A\times T)$

Insgesamt also $A\times(S\cup T)\subseteq(A\times S)\cup(A\times T)$.

Sei nun $(a,x)\in(A\times S)\cup(A\times T)$, dann gibt es wieder zwei Fälle:

1. Fall: $(a,x)\in(A\times S) \implies a\in A\wedge x\in S \implies a\in A\wedge x\in S\cup T$
$\implies (a,x)\in A\times(S\cup T)$

2. Fall: $(a,x)\notin(A\times S) \implies (a,x)\in(A\times T) \implies a\in A\wedge x\in T$
$\implies a\in A\wedge x\in S\cup T \implies (a,x)\in A\times(S\cup T)$

Also $A\times(S\cup T)\supseteq(A\times S)\cup(A\times T)$. ∎

An dieser Stelle sei noch einmal explizit auf den Unterschied zwischen dem *Tupel* (a,b) und der *Menge* $\{a,b\}$ hingewiesen!

Aussagenlogik

Eine **Aussage** ist eine sinnvolle Zusammenstellung von Zeichen (Buchstaben, Zahlen, Sonderzeichen), die entweder **wahr** oder **falsch** ist. (Eindeutig entscheidbar, eine andere Möglichkeit gibt es nicht.)

(1.12) Beispiele. 1.) 2 ist eine Primzahl.

2.) 4 ist eine Primzahl.

3.) Es regnet.

4.) Die Straße ist nass.

5.) Es regnet nicht und die Straße ist nass.

6.) Haltet den Dieb! (?)

7.) $1 + 3 = 5$

8.) $2^{109} - 1$ ist eine Primzahl.

9.) Für alle natürlichen Zahlen n gilt: n prim und $n > 10$, dann ist n ungerade.

10.) Für alle Primzahlen n gilt: $n > 5$ und n gerade, dann ist n ungerade.

11.) Wenn $x \leq 5$, dann $x \leq 10$.

Die letzten drei der obigen Aussagen (und 5.)) sind durch Verknüpfung von Einzelaussagen entstanden. Mit derartigen Verknüpfungen wollen wir uns jetzt befassen. Dabei werden wir uns nur für die Eigenschaft wahr oder falsch, nicht aber für den jeweiligen Inhalt einer Aussage interessieren. Aussagen wollen wir im Folgenden mit großen lateinischen Buchstaben $A, B, \ldots$ bezeichnen. Außerdem legen wir fest

„falsch“ wird ausgedrückt durch „0“ — „wahr“ wird ausgedrückt durch „1“.

(1.13) Definition. Gegeben seine zwei Aussagen A und B.

Alle Verknüpfungen werden mit einer **Wahrheitstafel** erklärt.

1.) Einstellige Verknüpfung: **Negation** einer Aussage A, geschrieben $\neg A$, gesprochen „nicht A“ oder „non A“. Die Aussage $\neg A$ ist genau dann wahr, wenn die Aussage A falsch ist.

A	$\neg A$
0	1
1	0

2.) Zweistellige Verknüpfungen $A \wedge B$, $A \vee B$, $A \implies B$, $A \iff B$.

A	B	$A \wedge B$	$A \vee B$	$A \implies B$	$A \iff B$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Dabei werden folgende Bezeichnungen und Abkürzungen benutzt:

Name	Symbol	Umgangssprachliche Bezeichnung
Konjunktion	$\wedge$	„und“
Disjunktion	$\vee$	„oder“ (nicht ausschließend)
Implikation	$\Longrightarrow$	„wenn, dann“
Äquivalenz	$\Longleftrightarrow$	„genau dann, wenn“ oder „dann und nur dann“

(1.14) Bemerkung. 1.) Formulieren Sie die Definitionen auch umgangssprachlich! Z. B. „Die durch die Verknüpfung $\vee$ aus A, B gebildete Aussage $A \vee B$ ist genau dann falsch, wenn beide Aussagen A, B falsch sind.“

2.) **Vorsicht:** Die Implikation ist immer wahr, wenn A falsch ist! Das scheint auf den ersten Blick unserer Intuition zu widersprechen. Das Beispiel 10.) oben und die folgenden Beispiele (1.15.5 u. 6) zeigen, warum man es dennoch so macht (und so machen sollte!).

Diese Verknüpfungen können beliebig kombiniert werden.

(1.15) Beispiele. 1.) $\neg(\neg A) = A$ (doppelte Verneinung)

2.) $(A \vee \neg B) \implies (\neg A \wedge C)$ mit der zugehörigen Wahrheitstafel:

A	B	C	$\neg A$	$\neg B$	$A \vee \neg B$	$\neg A \wedge C$	$(A \vee \neg B) \implies (\neg A \wedge C)$
0	0	0	1	1	1	0	0
0	0	1	1	1	1	1	1
0	1	0	1	0	0	0	1
0	1	1	1	0	0	1	1
1	0	0	0	1	1	0	0
1	0	1	0	1	1	0	0
1	1	0	0	0	1	0	0
1	1	1	0	0	1	0	0

3.) $(A \wedge B) \implies (A \iff B)$ Die zugehörige Wahrheitstafel zeigt, dass diese Aussage stets wahr ist.

4.) $(A \wedge (B \implies A)) \iff B$ ergibt eine andere Wahrheitstafel als das Beispiel 3.!

5.) Die Aussage $((A \implies B) \wedge (B \implies A)) \iff (A \iff B)$ ist immer wahr. Verifizieren Sie das mit einer Wahrheitstafel!

6.) Die Aussage „für alle $z \in \mathbb{Z}$ gilt $z < 3 \implies z < 5$“ ist wahr (auch wenn $z \geq 3$).

7.) Es gilt $(A \implies B) \iff (\neg B \implies \neg A)$ (Übung).

(1.16) Bemerkung. 1.) Ein Aussage, die immer wahr ist, nennt man auch eine **Tautologie**. Die Beispiele 3.), 5.) und 7.) sind Tautologien.

2.) Die Beispiele 5.) und 7.) aus (1.15) haben wichtige beweistechnische Bedeutung:

- Man zeigt die Äquivalenz von Aussagen A, B oft dadurch, dass man $A \implies B$ und $B \implies A$ zeigt.
- In 7.) versteckt sich der *indirekte Beweis*. Wir werden noch viele Beispiele sehen.

3.) Man kann für Aussagen Rechenregeln beweisen, wie sie in (1.7) für Mengen formuliert sind.

Eine **Aussageform** ist eine sinnvolle Zusammenstellung von Zeichen (Buchstaben, Zahlen, Sonderzeichen), die von einer oder mehreren Variablen abhängt, die aus vorgegebenen *Grundmengen* stammen müssen. Weist man den Variablen Werte zu, dann entsteht eine Aussage.

Neben den Beispielen aus den Übungen betrachten wir noch einige weitere

(1.17) Beispiele. 1.) $A(x) := (x \leq 5)$ und $B(x) := (x \leq 10)$, $x \in \mathbb{R}$, sind Aussageformen, wie auch $A(x) \implies B(x)$ (vgl. (1.12.10)).

2.) $A(4)$ ist wahr, $A(7)$ nicht.

3.) Wir skizzieren die Menge $\big\{(x, y) \in \mathbb{R}^2 ;\ A(x) \vee B(y)\big\}$ in der Vorlesung.

4.) Wir stellen fest, dass $A(x) \implies B(x)$ für alle $x \in \mathbb{R}$ wahr ist.

Den Sachverhalt aus dem letzten Beispiel schreibt man auch

$$\forall x \in \mathbb{R} : x \leq 5 \implies x \leq 10 \quad \text{oder abstrakter} \quad \forall x \in \mathbb{R} : A(x) \implies B(x).$$

Man nennt $\forall$ (spricht: „für alle“) einen **Quantor**. Die oben formulierte Aussage ist also genau dann wahr, wenn sie für jede reelle Zahl richtig ist.

Ein zweiter wichtiger Quantor ist $\exists$ (sprich: „es existiert“). Es ist also $\exists x \in G : A(x)$ wahr genau dann, wenn es auch nur ein $x_0 \in G$ gibt, sodass $A(x_0)$ wahr ist (es darf aber auch mehr geben).

Beispiel. Wir nutzen die Bezeichnungen aus (1.17). Es gilt

$\exists x \in \mathbb{R} : A(x) \wedge B(x)$ ist wahr, denn z.B. $x = 0$.

$\forall x \in \mathbb{R} : A(x) \vee B(x)$ ist falsch, denn z.B. $x = 11$.

(1.18) Bemerkung. Um eine Existenzaussage zu beweisen, genügt ein Beispiel; um eine Allaussage zu *widerlegen*, genügt ein Gegenbeispiel.

Der Beweis von Allaussagen ist meist aufwendiger!

Für viele Argumente ist es wichtig, mit der Negation von Aussagen mit Quantoren umzugehen. Wir halten fest (vgl. die vorige Bemerkung)

(1.19) *Sei $A(x)$ eine Aussageform über der Grundmenge G. Dann gilt („ist wahr")*

$$\begin{aligned} \neg(\forall x \in G : A(x)) &\iff \exists x \in G : \neg A(x) \\ \neg(\exists x \in G : A(x)) &\iff \forall x \in G : \neg A(x) \end{aligned}$$

Bemerkung. Die beiden Aussagen sind Tautologien, die ihrerseits zueinander äquivalent sind, wie man mit (1.15.1) sofort sieht.

Weil man Mengen durch Aussageformen definieren kann, gibt es viele Parallelen zwischen Mengenlehre und Aussagenlogik. Wir halten in einer Tabelle fest:

Menge M	$x \in M$ / $x \notin M$	Komplement	$\cap$	$\cup$	$\subseteq$	$=$
Aussageform $A(x)$	$A(x)$ ist wahr / falsch	Negation	$\wedge$	$\vee$	$\Longrightarrow$	$\Longleftrightarrow$

Bemerkung. Die Logik ist ein wichtiger Bestandteil der Philosophie. Sie ist auch ein Grundlagengebiet der Mathematik. In den Anwendungen spielt sie im Rahmen der Booleschen Algebra eine wichtige Rolle in der Elektrotechnik („logische Schaltungen") und in der Informatik.

Die Potenzmenge

Elemente einer Menge können auch selbst Mengen sein.

(1.20) Definition. Sei M eine Menge. Die **Potenzmenge** von M, geschrieben $\operatorname{Pot} M$, ist die Menge aller Teilmengen von M.

(1.21) Beispiele. 1.) Sei $M = \{1, 2\} \implies \operatorname{Pot} M = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$.

2.) $\operatorname{Pot}(\operatorname{Pot} M) = \Big\{\varnothing, \{\varnothing\}, \{\{1\}\}, \{\{2\}\}, \{M\}, \{\varnothing, \{1\}\}, \{\varnothing, \{2\}\}, \{\varnothing, M\}, \{\{1\}, \{2\}\},$

$\{\{1\}, M\}, \{\{2\}, M\}, \{\varnothing, \{1\}, \{2\}\}, \{\varnothing, \{1\}, M\}, \{\varnothing, \{2\}, M\}, \{\{1\}, \{2\}, M\}, \operatorname{Pot} M\Big\}$

3.) Für $A = \{x\}, B = \{a, b\}$ ist $\operatorname{Pot}(A \times B) = \Big\{\varnothing, \{(x, a)\}, \{(x, b)\}, \{(x, a), (x, b)\}\Big\}$

4.) $\mathrm{Pot}\{\varnothing\} = \Big\{\varnothing, \{\varnothing\}\Big\}$. *Frage*: Wer kann dieses Beispiel richtig deuten?

Wir notieren den Zusammenhang mit Schnitt und Vereinigung.

(1.22) *Seien $A, B \subseteq M$ beliebige Mengen. Dann gelten*

(1) $\mathrm{Pot}\, A \cap \mathrm{Pot}\, B = \mathrm{Pot}(A \cap B)$

(2) $\mathrm{Pot}\, A \cup \mathrm{Pot}\, B \subseteq \mathrm{Pot}(A \cup B)$.

Beweis. (1) Es gilt $X \in (\mathrm{Pot}\, A \cap \mathrm{Pot}\, B) \iff X \in \mathrm{Pot}\, A \ \wedge\ X \in \mathrm{Pot}\, B$

$$\iff X \subseteq A \ \wedge\ X \subseteq B \iff X \subseteq (A \cap B) \iff X \in \mathrm{Pot}(A \cap B).$$

(2) Es gilt $X \in (\mathrm{Pot}\, A \cup \mathrm{Pot}\, B) \iff X \in \mathrm{Pot}\, A \ \vee\ X \in \mathrm{Pot}\, B$

$$\iff X \subseteq A \ \vee\ X \subseteq B \implies X \subseteq (A \cup B) \iff X \in \mathrm{Pot}(A \cup B).$$

■

In der Formel (2) gilt anders als in (1) in der Regel nicht das Gleichheitszeichen (im Beweis kommt man an einer Stelle nicht von rechts nach links, wo?). Wir belegen dies durch folgendes

Beispiel. Sei $A = \{1, 2\}$ und $B = \{2, 3\}$. Dann gehört die Menge $\{1, 3\}$ zwar zur Potenzmenge von $A \cup B$, aber nicht zu $\mathrm{Pot}\, A \cup \mathrm{Pot}\, B$.

Bemerkung. Wir haben eine Behauptung durch ein Gegenbeispiel widerlegt. Man hüte sich vor dem Irrtum, eine Behauptung durch ein Beispiel beweisen zu wollen!

Relationen

... sind spezielle Aussageformen mit zwei Variablen, die (für unsere Zwecke!) aus derselben Menge stammen müssen.

(1.23) Beispiele. 1.) Zwischen Menschen ist „verwandt“ eine Relation.

2.) Sei H die Menge aller Personen in diesem Hörsaal. „sitzen nebeneinander“ definiert eine Relation auf H.

3.) Auf der Menge $\mathbb{N}$ ist „$\leq$“ eine Relation.

Z.B. gilt $1 \leq 4$, aber $3 \not\leq 2$.

4.) Entsprechend liefert $\leq$ auch eine Relation auf $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$. Diese Relationen hängen sehr eng zusammen und werden in der Notation nicht unterschieden.

5.) „liegt parallel zu“ (i.Z.: $\parallel$) und „steht senkrecht auf“ (i.Z.: $\perp$) sind Relationen auf der Menge $\mathfrak{G}$ aller Geraden.

6.) Auf jeder Menge M ist „$=$“ eine Relation, die **Gleichheitsrelation**.

Wir untersuchen zwei weitere wichtige Beispiele etwas genauer.

(1.24) Definition. Gegeben seien Zahlen $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$.

1.) a ist ein **Teiler** von b, wenn es ein $q \in \mathbb{Z}$ gibt mit $b = q \cdot a$. Man schreibt dann $a|b$, sprich: „a teilt b“. Damit ist „$|$“ eine Relation auf $\mathbb{Z}$.

2.) Man sagt a, b seien **kongruent modulo** m, wenn m ein Teiler von $(b-a)$ ist. Wir schreiben für diesen Sachverhalt $\quad a \equiv b \mod m$.

Hält man m fest, so ist auch „$\equiv \mod m$“ eine Relation auf $\mathbb{Z}$.

Bemerkung. Für alle $a \in \mathbb{Z}$ gilt $a|0$, und $\Big(0|a \implies a = 0\Big)$.

(1.25) Beispiele. 1.) $7|21,\ 7\nmid 20,\ -3|12,\ 4|-40$.

2.) Wir prüfen ob

$$3 \equiv 15 \mod 12, \quad 5 \equiv 18 \mod 12, \quad 15 \equiv 181 \mod 7, \quad -2 \equiv 11 \mod 3.$$

3.) Welche Zahlen sind $\equiv 0 \mod 2$, $\equiv 1 \mod 2$, $\equiv 2 \mod 2$, $\equiv -1 \mod 2$, usw.?

Wir notieren einige grundlegende Eigenschaften dieser Relationen.

(1.26) *Seien $a, b, c, d, u, v \in \mathbb{Z}$.*

(1) $a|a$ *(**Reflexivität**)*

(2) *Gilt $a|b$ und $b|c$, dann auch $a|c$.* *(**Transitivität**)*

(3) *Aus $a|b$ und $c|d$ folgt $a \cdot c \,|\, b \cdot d$.*

(4) *Aus $c \cdot a \,|\, c \cdot b$ mit $c \neq 0$ folgt $a|b$.*

(5) *Aus $a|b$ und $a|c$ folgt $a \,|\, u \cdot b + v \cdot c$.*

Beweis. (1) Übung!

(2) Aus $b = ka$ und $c = \ell b$ folgt $c = (k\ell)a$.

(3) Aus $b = ka$ und $d = \ell c$ folgt $bd = (k\ell)ac$.

(4) $cb = kca \implies b = ka$ mit der Kürzregel in $\mathbb{Z}$.

(5) $b = ka$ und $c = \ell a \implies ub + vc = (uk + v\ell)a$. ∎

Um ein Gefühl für Kongruenzen zu bekommen, betrachten wir einige weitere

(1.27) Beispiele. 1.) Gesucht sind alle Zahlen $a \in \mathbb{Z}$ mit $a \equiv 2 \mod 5$. Können Sie diese Menge A anders beschreiben? Vergleichen Sie diese mit der Menge B aller $b \in \mathbb{Z}$ mit $b \equiv 17 \mod 5$; und mit der Menge C aller $c \in \mathbb{Z}$ mit $c \equiv 1 \mod 5$. Was fällt auf?

2.) Dasselbe mit $a \equiv 0 \mod 7$, $b \equiv -14 \mod 7$ und $c \equiv -1 \mod 7$.

3.) Für welche Zahlen ist $a \equiv 0 \mod 1$?

Wir sammeln die wichtigsten Eigenschaften.

(1.28) *Es seien $a, b, c, d \in \mathbb{Z}$ und $m \in \mathbb{N}$. Dann gilt*

(1) $a \equiv a \mod m$ *(**Reflexivität**)*

(2) $a \equiv b \mod m \implies b \equiv a \mod m$ *(**Symmetrie**)*

(3) $a \equiv b \mod m \wedge b \equiv c \mod m \implies a \equiv c \mod m$ *(**Transitivität**)*

(4) *Aus $a \equiv b \mod m$ und $c \equiv d \mod m$ folgt*

$$a + c \equiv b + d \mod m \quad \text{und} \quad a \cdot c \equiv b \cdot d \mod m$$

Beweis. (1) Es gilt $m|0 = a - a$.

(2) $m|b - a \implies m|(-1)(b - a) = a - b$.

(3) Aus $m|b - a$ und $m|c - b$ folgt mit (1.26.4) auch $m|b - a + c - b = c - a$.

(4) Nach Voraussetzung gilt $m|b - a$ und $m|d - c$. Wir betrachten

$$bd - ac = bd - ad + ad - ac = (b - a)d + a(d - c) \implies m|bd - ac \quad \text{nach (1.26.5).}$$

Die Aussage für „+“ ist noch einfacher. Übung! ∎

Die Aussage (4) bedeutet eine Verträglichkeit von Kongruenzen mit „+“ und „·“. Sie wird uns noch häufig beschäftigen.

Wir abstrahieren Beobachtungen aus diesem Abschnitt zu einem neuen Begriff.

Äquivalenzrelationen und Klassenbildung

(1.29) Definition. Eine Relation $\sim$ auf der Menge M heißt **Äquivalenzrelation**, wenn sie für alle $a, b, c \in M$ folgende Eigenschaften besitzt:

(r) **reflexiv**, d.h. $a \sim a$;

(s) **symmetrisch**, d.h. $a \sim b \implies b \sim a$;

(t) **transitiv**, d.h. aus $a \sim b$ und $b \sim c$ folgt $a \sim c$.

Wir untersuchen die obigen Beispiele:

(1.30) Beispiele. 1.) „verwandt“ ist reflexiv, symmetrisch, aber nicht transitiv.

2.) Die Relation „sitzen nebeneinander“ ist symmetrisch, aber weder reflexiv, noch transitiv; also keine Äquivalenzrelation.

3.) „$\leq$“ ist reflexiv und transitiv. Ist sie auch symmetrisch?

4.) „liegt parallel zu“ ist eine Äquivalenzrelation. Warum?

„steht senkrecht auf“ ist nur symmetrisch.

5.) „$=$“ ist offenbar eine Äquivalenzrelation.

6.) „$|$“ ist reflexiv und transitiv, aber nicht symmetrisch.

„$\equiv \mod m$“ ist nach (1.28) für alle $m \in \mathbb{N}$ eine Äquivalenzrelation auf $\mathbb{Z}$.

Das wichtigste Konstrukt im Zusammenhang mit Äquivalenzrelationen ist der Quotientenraum.

Definition. Es sei M eine Menge mit der Äquivalenzrelation $\sim$.

Zu $a \in M$ heißt

$$[a]_\sim = [a] := \{x \in M\,;\ a \sim x\}$$

die zu a gehörige **Äquivalenzklasse**. Wir setzen

$$M/\sim := \big\{[a] \in \operatorname{Pot} M\,;\ a \in M\big\}$$

und sprechen vom **Quotientenraum** der Menge M nach $\sim$ (sprich M **modulo** $\sim$).

Wir untersuchen diese Begriffe am Beispiel der Modulo–3–Relation und allgemeiner der Relation $\equiv \mod m$.

(1.31) Beispiele. 1.) Wir betrachten die Relation $\equiv \mod 3$ auf $\mathbb{Z}$. Es gilt $\overline{0} := \{x \in \mathbb{Z}\,;\, 0 \equiv x \mod 3\}$, und wegen $x \in \overline{0} \iff 3|x-0$ besteht $\overline{0}$ genau aus den Vielfachen von 3. In Formeln:

$$\overline{0} = 3\mathbb{Z} := \{3k\,;\, k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, 9, 12, \ldots\}.$$

Weiter gilt $x \in \overline{1} \iff 3|x-1 \iff \exists k \in \mathbb{Z} : x - 1 = 3k$. Somit gilt

$$\overline{1} = 3\mathbb{Z} + 1 := \{3k+1\,;\, k \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, 10, 13, \ldots\}.$$

In der Vorlesung bestimmen wir $\overline{2}$, $\overline{3}$, usw.

Daraus ergibt sich als Quotientenraum:

$$\mathbb{Z}_3 := \mathbb{Z}/(\equiv \mod 3) = \left\{\overline{0}, \overline{1}, \overline{2}\right\}.$$

2.) Die Modulo–4–Relation auf $\mathbb{Z}$ unterteilt die ganzen Zahlen in die vier Teilmengen

$$\begin{aligned}
\overline{0} &= \{4z\,;\, z \in \mathbb{Z}\} = \{0, \pm 4, \pm 8, \ldots\} \\
\overline{1} &= \{1 + 4z\,;\, z \in \mathbb{Z}\} = \{1, 5, 9, \ldots, -3, -7, \ldots\} \\
\overline{2} &= \{2 + 4z\,;\, z \in \mathbb{Z}\} \\
\overline{3} &= \{3 + 4z\,;\, z \in \mathbb{Z}\}
\end{aligned}$$

3.) Wie sehen die Äquivalenzklassen der Modulo–2–Relation aus?

4.) Was passiert, wenn man statt 3 oder 4 eine andere Zahl $m \in \mathbb{N}$ wählt?

5.) Die Relation $\parallel$ ist eine Äquivalenzrelation auf der Menge aller Geraden. Wie sehen die Äquivalenzklassen aus?

6.) Wie sehen die Äquivalenzklassen der Äquivalenzrelation „$=$“ aus?

Die Beobachtungen, die wir an den Beispielen gewonnen haben, gelten ganz allgemein.

(1.32) Satz. *Es sei M eine Menge mit der Äquivalenzrelation $\sim$, dann gilt*

(1) *Für $a, b \in M$ sind äquivalent*

(I) $a \sim b$

(II) $[a] \cap [b] \neq \varnothing$

(III) $[a] = [b]$.

(2) *Es gilt $\bigcup_{a \in M} [a] = M$, d.h. jedes Element aus M liegt in genau einer Äquivalenzklassen.*

Beweis. (1) (I) $\Longrightarrow$ (II): Es gilt $a \in [a]$ wegen der Reflexivität und $a \in [b]$ nach Definition und Symmetrie.

(II) $\Longrightarrow$ (III): Sei $c \in [a] \cap [b]$ also $a \sim c$ und $b \sim c$. Aus Symmetrie und Transitivität von $\sim$ folgt $a \sim b$ und $b \sim a$. Für ein beliebiges $x \in [a]$ gilt $a \sim x$, also auch (warum?) $b \sim x$ und damit $x \in [b]$. Daher gilt $[a] \subseteq [b]$. Analog zeigt man $[b] \subseteq [a]$.

(III) $\Longrightarrow$ (I): Wegen $b \in [b] = [a]$ gilt auch $b \in [a]$, also $a \sim b$.

(2) Aus der Reflexivität folgt $\forall a \in M : a \in [a]$, also $[a] \neq \varnothing$ und a liegt in einer Klasse. Aus (1) folgt, dass $[a] \cap [b] = \varnothing$ falls $[a] \neq [b]$. Also kann a in höchstens einer Klasse liegen. Insgesamt zeigt das auch $\bigcup_{a \in M} [a] = M$. ∎

Der Satz besagt, dass die Menge M durch die Klassenbildung in disjunkte Teilmengen zerlegt wird. Am Beispiel der Parallelität wird das sehr augenfällig. So eine Zerlegung nennt man auch **Partition**.

Ein einzelnes Element b aus einer Äquivalenzklasse $[a]$ wird auch **Vertreter** oder **Repräsentant** der Klasse genannt.

2 Die reellen Zahlen

Sie werden im gesamten Mathematik-Studium immer wieder mit den reellen Zahlen zu tun haben. Welche wichtigen Eigenschaften besitzen die reellen Zahlen, die sie vor anderen Strukturen auszeichnen? Dies ist die Grundfrage einer axiomatischen Vorgehensweise. Wir werden einige — Ihnen wohlbekannte — Rechenregeln benutzen, die wir als „selbstevidente Tatsachen“ voraussetzen. Solche Aussagen nennt man **Axiome**. Alle anderen Rechenregeln müssen daraus ableitbar sein.

Hier werden Axiome angegeben, durch die die Menge, deren Elemente in der Schule als reelle Zahlen bekannt sind, letztendlich eindeutig bestimmt ist. Dabei versucht man, die Anzahl der Axiome möglichst klein zu halten.

Da die Liste der Axiome eher lang ist, unterteilen wir sie in drei Gruppen; die Axiome der

Verknüpfung, die Regeln für „$+$“ und „$\cdot$“ ;

Anordnung, die Regeln für „$<$“ ;

Vollständigkeit, die Idee der „Lückenlosigkeit“ der Anordnung.

Körperaxiome

Die Axiome für die Verküpfungen sind im Begriff des *Körpers* zusammengefasst. Den Begriff der „Verknüpfung“ werden wir später präzisieren, hier nur so viel: Eine Verknüpfung ordnet je zwei Elementen der unterliegenden Menge eine neues Element zu. Wie z.B. $7 + 5 = 12$, oder $7 \cdot 5 = 35$.

Wir starten mit einem Tripel $(\mathbb{K}, +, \cdot)$, bestehend aus einer Menge $\mathbb{K}$ und zwei Verknüpfungen „$+$“ und „$\cdot$“, bei denen Sie an die bekannte Addition und Multiplikation reeller Zahlen denken dürfen.

Definition (Körperaxiome). $(\mathbb{K}, +, \cdot)$ heißt **Körper**, wenn für alle $a, b, c \in \mathbb{K}$ gilt

(K1) $a + (b + c) = (a + b) + c$, und $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) $\exists\, 0 \in \mathbb{K} : \forall a \in \mathbb{K} : a + 0 = a$ und $\exists\, 1 \in \mathbb{K} : 1 \neq 0 \wedge \forall a \in \mathbb{K} \implies a \cdot 1 = a$

(K3) $\exists - a \in \mathbb{K} \ : \ a + (-a) = 0$ und falls $a \neq 0$, dann $\exists\, a^{-1} \in \mathbb{K} \ : \ a \cdot a^{-1} = 1$

(K4) $a + b = b + a$, und $a \cdot b = b \cdot a$

(Dg) $a \cdot (b + c) = a \cdot b + a \cdot c$

Wenn es klar ist, welche Verknüpfungen zu Grunde liegen, spricht man auch von dem Körper $\mathbb{K}$ an Stelle von $(\mathbb{K}, +, \cdot)$. Die Axiome (K1), (K4), (Dg) heißen **Assoziativ-**, **Kommutativ-** und **Distributivgesetz**.

Die Elemente 0 und 1 werden **neutrale Elemente** bezüglich der jeweiligen Verknüpfung oder auch Null- bzw. Einselement genannt. Analog spricht man in (K3) vom **inversen Element**. Die Inversen bezüglich „+“ nennt man auch **Negative**. Bei einer beliebigen Menge $\mathbb{K}$ handelt es sich bei den neutralen Elementen in der Regel nicht um die Zahlen 0 und 1, obwohl sie eine analoge Rolle spielen!

(2.1) Beispiele. 1.) Neben den rellen Zahlen, erfüllen auch die rationalen Zahlen mit der normalen Addition und Multiplikation diese Axiome, bilden also einen Körper. Wir werden noch einige weitere Körper kennenlernen.

2.) Welche Axiome gelten für $(\mathbb{Z}, +, \cdot)$; welche für $(\mathbb{N}, +, \cdot)$?

3.) Für eine Menge $M \neq \varnothing$ erfüllt $(\operatorname{Pot} M, \cup, \cap)$ alle Axiome außer (K3) — warum?

(2.2) Bemerkung. 1.) Man beachte die völlige Analogie der geforderten Axiome (K1) – (K4) für „+“ und „$\cdot$“ . Daraus werden wir später den Begriff der **abelschen Gruppe** extrahieren.

2.) Die einzige Ausnahme für diese Analogie ist — neben (Dg) — die Rolle des Nullelements 0 in unserer Struktur. Wir begründen, warum 0 bezüglich „$\cdot$“ kein Inverses haben kann: Angenommen es gäbe eine Zahl $j \in \mathbb{K}$ mit $0 \cdot j = 1$, dann folgte

$$1 = 0 \cdot j \overset{\text{(K2)}}{=} (0+0) \cdot j \overset{\text{(K4)}}{=} j \cdot (0+0) \overset{\text{(Dg), (K4)}}{=} 0 \cdot j + 0 \cdot j = 1 + 1 = 2.$$

Das ist ein Widerspruch. Der entscheidende Schritt in der Rechnung ist das Distributivgesetz. Wenn das Distributivgesetz gelten soll, dann kann 0 kein Inverses besitzen.

3.) Die Forderung nach der Kommutativität der Addition ist eigentlich überflüssig, da sie aus den anderen Axiomen gefolgert werden kann.

Wie angekündigt ziehen wir einige Folgerungen aus unseren Axiomen. Für die Menge $\mathbb{K} \setminus \{0\}$ scheibt man oft $\mathbb{K}^*$.

(2.3) *Es sei $(\mathbb{K}, +, \cdot)$ ein Körper. Dann gilt für alle $a, b, c \in \mathbb{K}$, $d \in \mathbb{K}^*$*

(1) $c + a = c + b \implies a = b$ *(**Kürzregel** für die Addition)*

(2) $d \cdot a = d \cdot b \implies a = b$ *(**Kürzregel** für die Multiplikation)*

(3) $-(-a) = a$ *und* $(d^{-1})^{-1} = d$.

(4) $a \cdot 0 = 0 = 0 \cdot a$

(5) $a \cdot (-b) = (-a) \cdot b = -ab$

(6) $(-a)\cdot(-b) = ab$.

Im Beweis und in der Folge schreiben wir häufig ab statt $a\cdot b$, wie Sie das wahrscheinlich aus der Schule schon kennen.

Beweis. (1) Wir addieren auf beiden Seiten $-c$ und wenden (K4) und (K1), dann (K2) und (K3) an an:

$$\begin{aligned} c+a=c+b &\implies (-c)+(c+a)=(-c)+(c+b)\\ &\implies (c+(-c))+a=(c+(-c))+b\\ &\implies 0+a=0+b \implies a=b. \end{aligned}$$

(2) geht völlig analog.

(3) Wegen (K4) gilt $(-a)+a=0=(-a)+(-(-a))$, mit (1) folgt die Behauptung. Die entsprechende Aussage für „$\cdot$“ geht wieder analog.

(4) $a0+0=a0=a(0+0)=a0+a0$, mit (1) folgt $0=a0$.

(5) $ab+a(-b)=a(b+(-b))=a\cdot 0=0 \implies a(-b)=-ab$. Wegen (K4) folgt die andere Gleichung.

(6) $(-a)\cdot(-b)=-(a\cdot(-b))=-(-ab)=ab$. ∎

(2.4) Bemerkung. 1. Die Kürzregel (2) impliziert zusammen mit (4) auch:

Ein Produkt ist Null genau dann, wenn einer der Faktoren Null ist.

Diese Aussage gilt in allen Körpern. Führen Sie den Beweis aus!

2. Aussage (6) ist die bekannte Regel:

Minus mal Minus gibt Plus.

3. Mit (4) kann man erneut folgern, dass 0 wirklich nicht invertierbar ist. Es würde sonst $0=1$ folgen; wie?

4. Etwas pointiert ausgedrückt, kann man sagen:

In Körpern kann man so rechnen, wie man es in der Schule gelernt hat.

Wir benutzen in Zukunft die verkürzte Schreibweise $a-b := a+(-b) \overset{!}{=} a+(-1)\cdot b$.

Anordnung

Wir befassen uns jetzt mit der Tatsache, dass man reelle Zahlen der Größe nach vergleichen kann. Wir werden später sehen, dass das nicht in jedem Körper sinnvoll möglich ist. Anordnung ist eine Relation auf $\mathbb{K}$. Wir wollen hier einen Weg aufzeigen, wie man diese Relation definieren kann. Später werden wir in anderen Kontexten analog vorgehen. Es stellt sich heraus, dass es für beliebige $a \in \mathbb{K}$ genügt, entscheiden zu können, ob a positiv ist oder nicht.

(2.5) Definition (Anordnungsaxiome). Ein Körper $(\mathbb{K}, +, \cdot, <)$ heißt **angeordnet**, wenn es eine Menge **positiver** Elemente $\mathbb{K}^+$ gibt mit

(A1) $\forall a \in \mathbb{K}^*$ gilt $a \in \mathbb{K}^+$ oder $-a \in \mathbb{K}^+$, aber nicht beides; und $0 \notin \mathbb{K}^+$.

(A2) $\forall a, b \in \mathbb{K}^+$ gilt $a + b \in \mathbb{K}^+$ und $a \cdot b \in \mathbb{K}^+$.

Wir schreiben $a < b$, wenn $b - a \in \mathbb{K}^+$, wenn also $b - a$ positiv ist. Somit ist „$<$“ eine Relation auf $\mathbb{K}$.

Wie gewohnt, schreiben wir $a \leq b$ falls $a < b \vee a = b$. An Stelle von $a < b$ bzw. $a \leq b$ werden wir auch $b > a$ bzw. $b \geq a$ mit der üblichen Bedeutung verwenden.

(2.6) Beispiele. 1.) $\mathbb{Q}$ und $\mathbb{R}$ bilden jeweils angeordnete Körper. (Genauer müsste man z. B. $(\mathbb{Q}, +, \cdot, <)$ schreiben.)

2.) Die komplexen Zahlen, die später eingeführt werden, bilden einen Körper, den man nicht so anordnen kann, dass die Axiome (A1) und (A2) erfüllt sind.

Wir halten einige Eigenschaften von $<$ fest.

(2.7) *Es sei $(\mathbb{K}, +, \cdot, <)$ ein angeordneter Körper, dann gilt für alle $a, b, c \in \mathbb{K}$*

(1) *genau eine Aussage $a < b \ \vee \ a = b \ \vee \ b < a$ (**Trichotomie**).*

(2) $a < b \ \wedge \ b < c \implies a < c$ *(**Transitivität**).*

(3) $a \leq b \ \wedge \ b \leq a \implies a = b$ *(**Antisymmetrie**).*

Beweis. (1) Wir betrachten $b - a$ und gehen die Fälle aus (A1) durch.

Im Fall $b - a \in \mathbb{K}^+$ folgt $a < b$; im Fall $0 = b - a$ ergibt sich $a = b$.

Es bleibt der Fall $-(b - a) \in \mathbb{K}^+$. Mit (2.3) (5), (6), (Dg) und (K4) ergibt sich

$$-(b - a) = (-1)(b + (-a)) = (-1)b + (-1)(-a) = -b + a = a - b.$$

Daher folgt $b < a$ in diesem Fall.

(2) Nach Voraussetzung gilt $b - a \in \mathbb{K}^+$ und $c - b \in \mathbb{K}^+$. Nun folgt mit (A2)

$$c - a = b - a + c - b \in \mathbb{K}^+, \quad \text{also} \quad a < c.$$

(3) folgt direkt aus (1). ∎

Wir wollen einige Rechenregeln für Ungleichungen in angeordneten Körpern beweisen. Da die Multiplikation kommutativ ist, schreiben wir statt b^{-1} auch $\frac{1}{b}$. In diesem Sinne ist $ab^{-1} = \frac{a}{b} = b^{-1}a$ (siehe auch die Übungen).

(2.8) *Sei* $(\mathbb{K}, +, \cdot, <)$ *ein angeordneter Körper, und seien* $a, b, c, d \in \mathbb{K}$. *Dann gelten*

(1) $a < b \wedge c \leq d \implies a + c < b + d$;

(2) $a < b \wedge 0 < c \implies ca < cb$;

(3) $a < b \wedge c < 0 \implies ca > cb$;

(4) $a \neq 0 \implies 0 < a \cdot a = a^2$;

(5) $0 < 1$;

(6) $0 < a \leq b \implies 0 < \dfrac{1}{b} \leq \dfrac{1}{a}$.

Beweis. (1) Es gilt $b - a \in \mathbb{K}^+$ nach Definition. Im Fall $c = d$ kann man rechnen

$$b - a = b - a + 0 = b - a + d - c = b + d + (-1)(a + c) = b + d - (a + c)$$

Wegen $b - a \in \mathbb{K}^+$ gilt also $b + d - (a + c) \in \mathbb{K}^+$ und somit $a + c < b + d$.

Im Fall $d - c \in \mathbb{K}^+$ folgt mit (2.3.5) und (A2)

$$b + d - (a + c) = b - a + d - c \in \mathbb{K}^+ \implies a + c < b + d.$$

(2) Wegen $b - a \in \mathbb{K}^+$ und $c \in \mathbb{K}^+$ gilt mit (A2)

$$cb - ca = cb + c(-a) = c(b - a) \in \mathbb{K}^+ \implies ca < cb.$$

(3) Ist $c < 0$, so gilt $-c \in \mathbb{K}^+$. Wenn wir (2) auf $a < b$ anwenden, erhalten wir $(-c)a < (-c)b$. Dies ist nach (2.3.5) gleichbedeutend mit $-ca < -cb$. Nach (1) kann man auf beiden Seiten $ca + cb$ addieren, und erhält die Behauptung mit Hilfe der Körperaxiome.

(4) Ist $a \in \mathbb{K}^+$, so gilt $a \cdot a \in \mathbb{K}^+$ nach (A2); und im Fall $a < 0$ gilt wegen (3) ebenfalls $a \cdot a > a \cdot 0 = 0$. Nach (A1) muss einer der beiden Fälle vorliegen.

(5) folgt wegen $1 = 1 \cdot 1 > 0$ direkt aus (4).

(6) Wäre $a^{-1} < 0$, so folgte $1 = aa^{-1} < a0 = 0$ nach (2) — ein Widerspruch zu (5). Also muss $0 < a^{-1}$ gelten. Dann gilt mit (2) auch

$$\frac{1}{a \cdot b} > 0 \quad \text{und} \quad \frac{1}{b} = \frac{a}{a \cdot b} \leq \frac{b}{a \cdot b} = \frac{1}{a}.$$ ∎

Bemerkung. Die Aussagen (1) – (3) werden auch **Monotoniegesetze** genannt. Sie regeln das Zusammenspiel von Addition, Multiplikation und Anordnung.

Der Betrag

In den folgenden Sätzen und Definitionen sei $(\mathbb{K}, +, \cdot, <)$ ein angeordneter Körper und $a, b, c, d \in \mathbb{K}$. Wir geben einige Regeln für den Betrag an.

Definition. $|a| := \begin{cases} a & \text{falls} \quad a \geq 0 \\ -a & \text{falls} \quad a < 0 \end{cases}$ heißt der **(Absolut-)Betrag** von a.

Beispiel. $|-5| = -(-5) = 5$. Spätestens jetzt sollte klar sein, dass $-x$ nicht automatisch eine negative Zahl ist!

Wir zeigen einige (bekannte?) Rechenregeln für den Betrag.

(2.9) *Es seien* $a, b \in \mathbb{K}$.

(1) *Es gilt stets* $|a| \geq 0$ *und es ist* $|a| = 0 \iff a = 0$

(2) $|a \cdot b| = |a| \cdot |b|$

(3) $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$ *falls* $b \neq 0$

(4) $|a + b| \leq |a| + |b|$ ***(Dreiecksungleichung)***

(5) $|a - b| \geq |a| - |b|$.

Beweis. (1) Für $a > 0$ ist $|a| = a$, für $a < 0$ ist $|a| = -a > 0$ nach (A1).

(2) Wir führen eine Fallunterscheidung durch. Dabei wird mehrfach (A2) und (2.8.3) benutzt.

$$\begin{aligned} a, b \geq 0 &\implies ab \geq 0 \implies |ab| = ab = |a|\,|b| \\ a \geq 0,\ b < 0 &\implies ab \leq 0 \implies |ab| = -ab = a(-b) = |a|\,|b| \\ a < 0,\ b \geq 0 &\implies ab \leq 0 \implies |ab| = -ab = (-a)b = |a|\,|b| \\ a, b < 0 &\implies ab > 0 \implies |ab| = ab = (-a)(-b) = |a|\,|b| \end{aligned}$$

(3) Es ist $a = \frac{a}{b} \cdot b$, also $|a| = \left|\frac{a}{b} \cdot b\right| = \left|\frac{a}{b}\right| |b|$ und es folgt die Behauptung.

(4) Für $x \in \mathbb{K}$ gilt stets $x \leq |x|$ und $-x \leq |x|$. Damit und mit (2.8.1) folgt

$$a + b \leq |a| + |b| \quad \text{und} \quad -(a + b) = (-a) + (-b) \leq |a| + |b|.$$

Es gibt zwei Möglichkeiten:

$a+b \geq 0 \implies |a+b| = a+b \leq |a|+|b|$ oder $a+b < 0 \implies |a+b| = -(a+b) \leq |a|+|b|$.

(5) $|a| = |b + a - b| \leq |b| + |a - b|$ ergibt die Behauptung. ∎

Ordnungstheoretische Grundbegriffe

... werden immer wieder auftauchen; besonders in der Analysis. Im Folgenden sei M stets eine Teilmenge der reellen Zahlen (oder eines anderen angeordneten Körpers).

(2.10) Definition. 1.) $k \in \mathbb{R}$ heißt **obere Schranke** von $M :\iff \forall m \in M : m \leq k$.

M heißt **nach oben beschränkt**, falls M eine obere Schranke besitzt.

2.) $k \in \mathbb{R}$ heißt **untere Schranke** von $M :\iff \forall m \in M : k \leq m$.

M heißt **nach unten beschränkt**, falls M eine untere Schranke besitzt.

3.) M heißt **beschränkt**, falls M nach unten und nach oben beschränkt ist.

(2.11) Beispiele. 1.) $\{1, 2, 3\}$ besitzt — neben unendlich vielen anderen — die unteren Schranken -11, 0 oder 1 und die oberen Schranken 3, π oder 2018.

2.) $\mathbb{Q} \subseteq \mathbb{R}$ und $\mathbb{Z} \subseteq \mathbb{R}$ sind weder nach unten und noch nach oben beschränkt, also **unbeschränkt**.

3.) $\mathbb{R}^+$ besitzt untere (sogar unendlich viele) Schranken, und ist somit nach unten beschränkt. Es gibt aber keine obere Schranke und deshalb ist $\mathbb{R}^+$ nicht beschränkt.

4.) a und b sind Schranken der **Intervalle**

$$]a,b[:= \{r \in \mathbb{R}\,;\ a < r < b\}\,, \quad [a,b] := \{r \in \mathbb{R}\,;\ a \leq r \leq b\}\,, \quad [a,b[\,, \quad \text{und} \quad]a,b].$$

5.) *Frage*: Welche Schranken hat $\left\{q \in \mathbb{Q}\,;\ q^2 < 2\right\}$?

(2.12) Definition. 1.) $k \in \mathbb{R}$ heißt **Maximum** von M, wenn $k \in M$ und k obere Schranke von M ist. Wir schreiben $k = \max M$,

2.) $k \in \mathbb{R}$ heißt **Minimum** von M, geschrieben $k = \min M$, wenn $k \in M$ und k untere Schranke ist.

Wie wir an den Beispielen sehen, besitzt nicht jede Teilmenge von $\mathbb{R}$ ein Maximum oder ein Minimum, selbst wenn sie beschränkt ist. Falls Maximum oder Minimum existieren, sind sie eindeutig festgelegt:

Angenommen, a und b seien beide Maxima von M, dann folgt $a \leq b$ und $b \leq a$, also $a = b$ wegen der Antisymmetrie.

Wenn $\max M$ existiert, so handelt es sich um die **kleinste obere Schranke**, analog ist $\min M$ die **größte untere Schranke**.

Beispiel. Sei $M := \left\{\frac{1}{n}\,;\ n \in \mathbb{N}\right\}$, dann ist M beschränkt mit größter unterer Schranke 0 und kleinster oberer Schranke 1. Während 1 gleichzeitig Maximum ist, also $1 = \max M$, existiert kein Minimum.

Größte untere und kleinste obere Schranken interessieren auch, falls sie *nicht* zu der betreffenden Menge gehören.

(2.13) Definition. 1.) $s \in \mathbb{R}$ heißt **Supremum** von M, geschrieben $s = \sup M :\Longleftrightarrow$ s ist kleinste obere Schranke.

2.) $t \in \mathbb{R}$ heißt **Infimum** von M, geschrieben $t = \inf M :\Longleftrightarrow$ t ist größte untere Schranke.

Beispiel. Für $M := \left\{\frac{1}{n};\ n \in \mathbb{N}\right\}$ ist $1 = \max M = \sup M$ und $0 = \inf M$ (kein Minimum, siehe oben).

Wegen $s = \min\{k \in \mathbb{R};\ k \text{ ist obere Schranke von } M\}$ sind Supremum und analog Infimum — falls existent — eindeutig bestimmt. Wenn Maximum oder Minimum existieren, ist $\max M = \sup M$ bzw. $\min M = \inf M$.

Alle Aussagen und Definitionen in diesem Abschnitt galten bisher gleichermaßen für $\mathbb{R}$ und für $\mathbb{Q}$. Dies wird sich nun ändern!

Vollständigkeit

Definition (Vollständigkeitsaxiom). Ein angeordneter Körper $(\mathbb{K}, +, \cdot, <)$ heißt **vollständig**, wenn gilt:

Jede nicht leere, nach oben beschränkte Teilmenge besitzt ein Supremum.

Aus naheliegenden Gründen spricht man auch vom **Supremumsprinzip**.

Bemerkung. Es gibt ein Reihe äquivalenter Formulierungen des Vollständigkeitsaxioms. Z.B. das *Schnittaxiom* oder die Konvergenz von *Cauchy-Folgen* (zusammen mit (2.15)).

Jetzt haben wir unser Ziel erreicht, die reellen Zahlen $\mathbb{R}$ sind eindeutig durch Axiome festgelegt. Es gilt nämlich der Satz

(2.14) Satz. *Es gibt — bis auf Isomorphie*[5] *— einen einzigen vollständig angeordneten Körper, den Körper der* ***reellen Zahlen****.*

Eine weitere wichtige Eigenschaft der reellen Zahlen ergibt sich leicht aus der Vollständigkeit. Sie erscheint uns fast selbstverständlich.

(2.15) *Sei $r \in \mathbb{R}^{>0}$, dann gilt*

(1) $\exists n \in \mathbb{N} : r < n$.

[5] D.h., bis auf Umbenennung der Elemente; genaueres später.

(2) $\exists n \in \mathbb{N} : 0 < \dfrac{1}{n} < r\,.$

(3) *Die Menge* $\mathbb{N}$ *ist nicht beschränkt.*

Beweis. (3) Angenommen, $\mathbb{N}$ besitzt eine obere Schranke s. Nach dem Vollständigkeitsaxiom dürfen wir s minimal annehmen (Supremum). Es ist dann $s-1$ *keine* obere Schranke, also gibt es ein $n \in \mathbb{N}$ mit $s-1 < n$. Daraus folgt der Widerspruch $s < n+1$.

(1) ergibt sich nun direkt, andernfalls wäre ja r eine obere Schranke von $\mathbb{N}$.

(2) folgt leicht aus (1) und (2.8.6). ∎

Wir geben eine einfache Anwendung — die Existenz von *Quadratwurzeln.*

(2.16) *Zu jeder reellen Zahl* $\alpha > 0$ *gibt es genau eine Zahl* $w \in \mathbb{R}$ *mit* $w \geq 0$ *und* $w^2 = \alpha\,.$

Beweis. Existenz: Wir betrachten die Mengen

$$A := \Big\{ x \in \mathbb{R}\,;\; x^2 < \alpha \Big\}$$

Wegen $0 \in A$ ist diese Menge nicht leer.

Weiter gilt für $x \in A$: $x^2 < \alpha < 1+2\alpha < 1+2\alpha+\alpha^2 = (1+\alpha)^2$. Daraus folgt $x < 1+\alpha$ und A ist nach oben beschränkt.

Nach dem Vollständigkeitsaxiom existiert also ein Supremum $w \in \mathbb{R}$ von A, für das natürlich $w \geq 0$ gilt.

Wir wollen zeigen, dass $w^2 = \alpha$. Wegen der Trichotomie genügt es die Fälle $w^2 < \alpha$ und $w^2 > \alpha$ auszuschließen.

1. Fall $w^2 < \alpha$: Ziel ist es, eine Zahl $n \in \mathbb{N}$ zu finden, sodass $\left(w + \frac{1}{n}\right)^2 < \alpha$. Dann wäre w nicht obere Schranke, ein Widerspruch. Durch Umformen dieser Ungleichung wird man auf folgende Bedingung für n geführt:

$$\frac{1}{n} < \frac{\alpha - w^2}{2w+1}.$$

Da die rechte Seite in diesem Fall positiv ist, existiert n nach (2.15). Weiter gilt

$$\frac{1}{n} < \frac{\alpha - w^2}{2w+1} \leq \frac{\alpha - w^2}{2w+\frac{1}{n}}, \quad \text{denn } 1 \geq \tfrac{1}{n}.$$

Daraus gewinnt man sofort den gewünschten Widerspruch.

2. Fall $w^2 > \alpha$: Nun suchen wir $n \in \mathbb{N}$ mit $\left(w - \frac{1}{n}\right)^2 > \alpha$, sodass w nicht *kleinste* obere Schranke wäre. Hier führt die Wahl (beachte (2.15))

$$\frac{1}{n} < \frac{w^2 - \alpha}{2w}.$$

zum Ziel. In der Tat

$$\left(w - \frac{1}{n}\right)^2 = w^2 - \frac{2w}{n} + \left(\frac{1}{n}\right)^2 > w^2 - \frac{2w}{n} > w^2 - (w^2 - \alpha) = \alpha.$$

Damit sind beide Fälle zum Widerspruch geführt und es bleibt nur die Möglichkeit $w^2 = \alpha$.

Eindeutigkeit: Übung. ∎

Die Zahl w wird natürlich mit $\sqrt{\alpha}$ bezeichnet und **Quadratwurzel** aus α genannt, wie Sie es gewohnt sind.

Zum Abschluss noch eine Aussage, die wir erst später zeigen werden.

(2.17) Satz. *Es gilt $\sqrt{2} \notin \mathbb{Q}$. Daher ist $\mathbb{Q}$ nicht vollständig.*

Das bedeutet, dass $\sqrt{2}$ nicht als Bruch dargestellt werden kann.

Betrachtet man auf der Zahlengerade nur die rationalen Zahlen, so treten gewissermaßen Lücken oder Löcher auf, z. B. $\sqrt{2}$. Vollständigkeit bedeutet anschaulich, dass solche Lücken alle ausgefüllt sind.

3 Abbildungen

Dieser Begriff ist fundamental für alle Gebiete der Mathematik und wird sogar schon in der Grundschule behandelt.[6] Er kommt im Alltag und in vielen Wissenschaften als einfache *Zuordnung* und als *funktionaler Zusammenhang* mit vielen unterschiedlichen Facetten vor. Er ist auch Ihnen aus Ihrer Schulzeit in verschiedenen Zusammenhängen begegnet. Abbildungen werden in der Mathematik auch als eigenständige Objekte (Sicht als Ganzes!) untersucht.

Wir betrachten zunächst einige

Beispiele

1.) Aktienkurse: Der Verlauf von Aktienkursen ist ein typischer *funktionaler Zusammenhang*. Der blaue Graph beschreibt den Verlauf des DAX in den vergangenen Monaten. Der glatte Graph stellt eine Mittelung über je 20 Tage dar.
Für uns ist wichtig: Der Kurs (und auch die Mittel-Kurve) wird in Abhängigkeit von der Zeit angegeben. Jeden Punkt auf der Kurve kann man als Paar auffassen (Datum,Kurs).

2.) Landkarten sind *Abbildungen* der realen Welt auf einen Bogen Papier (oder ein Display). Was man sieht, ist nicht der Graph einer Kurve, sondern nur die Bilder von Punkten in der Realität. Will man die Karte nutzen, muss man diese *Zuordnung* gewissermaßen selbst durchführen.

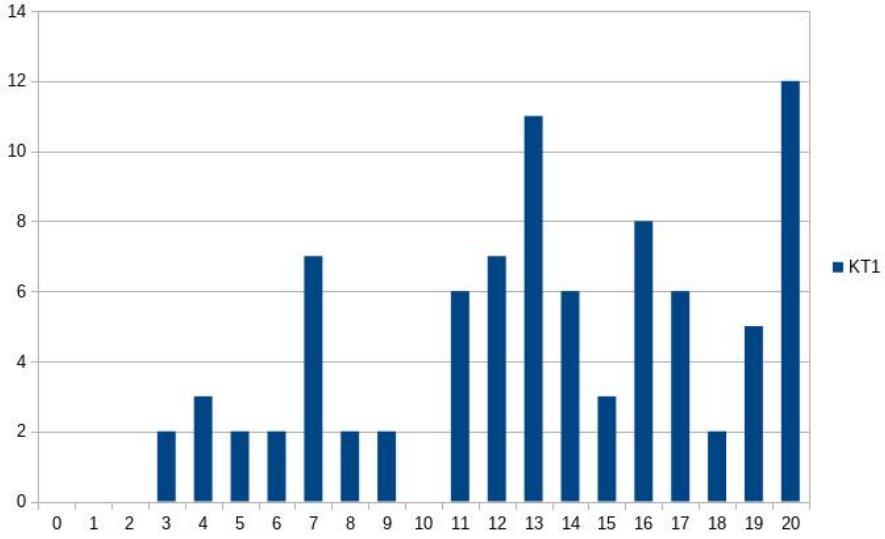
Eine topographische Karte enthält darüber hinaus Höhenlinien. So kann die geübte Kartenleserin Rückschlüsse über die Topographie der Landschaft ziehen. Hier liegt eine Zuordnung Punkt(mit zwei Koordinaten)—Höhe über dem Meeresspiegel vor.

3.) Verteilung der Punkte beim ersten Kurztest

[6] Siehe `http://www.hamburg.de/contentblob/2481796/data/mathematik-gs.pdf` auf S. 27.

n	a_n
0	0
1	0
2	0
3	2
4	3
5	3
6	3
7	7
8	2
9	2
10	0
11	6
12	7
13	11
14	6
15	3
16	8
17	6
18	2
19	5
20	12

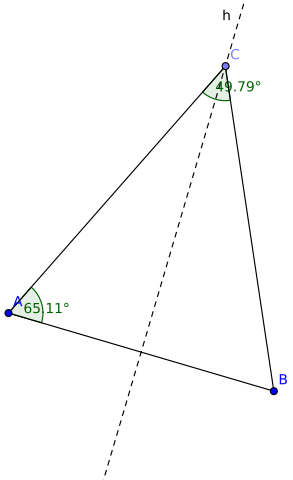
Die Tabelle zeigt die Anzahl a_n der Personen, die n Punkte erhalten haben. Graphisch sieht das so aus

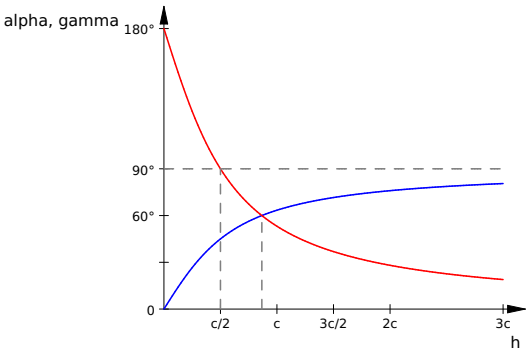


Man kann sich die Tabelle auch als Menge von Paaren der Form (n, a_n) vorstellen.

4.) Spiegelung an einer Geraden: Jedem Punkt der Ausschauungsebene wird ein Bildpunkt zugeordnet.

5.) Ein gleichschenkeliges Dreieck mit Basis AB entsteht, wenn man den Punkt C auf der Mittelsenkrechten von A, B wählt. Die Basislänge c sei gegeben. Variiert man den Abstand h von C zur Basis, so verändern sich die Winkel im Dreieck abhängig von h. Die blaue Kurve zeigt α, die rote γ. (Was ist mit β ?)





Man könnte diesen *funktionalen Zusammenhang* auch mit Hilfe einer Gleichung ausdrücken. Wie?

6.) Die Geburtstagsabbildung ordnet jeder Person ihren Geburtstag zu.

Wichtig ist, dass jedem Element der Ausgangsmenge (Definitionsmenge!) *genau ein* Element der Zielmenge *zugeordnet* wird.

Formale Definition

Es stellt sich heraus, dass man funktionale Zusammenhänge wie auch Zuordnungen auf dieselbe Weise mengentheoretisch adäquat beschreiben kann.

(3.1) Definition. Seien A, B beliebige Mengen. Eine Teilmenge f von $A \times B$ heißt **Abbildung** oder **Funktion**, wenn

$$\forall a \in A : \exists! \, b \in B \ : \ (a, b) \in f.$$

Dabei bedeutet $\exists!$ „es existiert genau ein“.

(3.2) Beispiele. 1.) $A = \{0, 1, 2\},\ B = \{u, v\}, \quad f = \{(0, u), (1, v), (2, u)\}.$

2.) $A = B = \mathbb{N},\ f = \big\{(n, 2n - 1)\,;\ n \in \mathbb{N}\big\}.$

3.) $Q = \big\{(x, x^2)\,;\ x \in \mathbb{R}\big\} \subseteq \mathbb{R} \times \mathbb{R}^{\geq 0}$ ist eine Funktion von $\mathbb{R}$ nach $\mathbb{R}^{\geq 0}$, nicht aber $\hat{Q} = \big\{(x^2, x)\,;\ x \in \mathbb{R}\big\} \subseteq \mathbb{R}^{\geq 0} \times \mathbb{R}$.

4.) Für eine Menge M ist $\mathrm{id}_M := \{(x,x) \in M \times M\,;\; x \in M\}$ eine Abbildung, die immer wieder auftaucht und trotz ihrer Einfachheit sehr wichtig ist. Sie wird **Identität** genannt.

In 1.) wird den Zahlen 0 und 2 der Buchstabe u und der Zahl 1 der Buchstabe v zugeordnet, in 2.) wird jeder natürlichen Zahl n unter der Abbildung f die Zahl $2n-1$ zugeteilt. Allgemein gehört auf Grund der Definition zu jedem Element $a \in A$ genau ein Element $b \in B$, daher können wir statt $(a,b) \in f$ die übliche Schreibweise $f(a) = b$ verwenden, statt $f \subseteq A \times B$ schreiben wir $f : A \to B$. Das Beispiel 2.) sieht dann so aus:

$$f : \mathbb{N} \to \mathbb{N}\,;\; n \mapsto 2n-1.$$

Die „Pfeilschreibweise“ deutet an, dass bei jedem Element aus A genau ein Pfeil beginnt. Das heißt aber nicht, dass verschiedene Pfeile nicht dasselbe Ziel haben dürfen (wie in Beispiel (3.2.1)). Es kann auch sein, dass es Elemente in B gibt, bei denen überhaupt kein Pfeil ankommt.

Man kann sich einfache Abbildungen auch mit Hilfe eines **Pfeildiagramm**s veranschaulichen (näheres in der Vorlesung).

Ist $f : A \to B$ eine Abbildung, so heißt A **Definitionsbereich** oder **Definitionsmenge**, B wird **Zielmenge** oder **Wertevorrat** genannt. $f(x)$ ist der **Wert** von f an der Stelle x und wird auch als **Bildelement** zu $x \in A$ in B bezeichnet.

VORSICHT: Man sollte $f(x)$ nie mit der Abbildung f verwechseln, auch wenn häufig (gerade auch in der Schule) etwas nachlässig von der Abbildung $f(x)$ gesprochen wird. Das ist formal falsch!

(3.3) Bemerkung. Eine Abbildung mit Definitionsbereich $A \times A$ und Zielmenge A, also $A \times A \to A$, wird auch **Verknüpfung** auf A genannt.

1.) Die wichtigsten Beispiele hierfür sind die **arithmetischen Operatoren** $+, \cdot$ mit $A = \mathbb{R}$ (oder $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$). Für welche dieser Mengen ist auch „$-$“ oder „$:$“ eine Verknüpfung?

2.) Das Axiom (A2) aus Kapitel 2 kann nun neu interpretiert werden: (A2) besagt (auch), dass $+ : \mathbb{K}^+ \times \mathbb{K}^+ \to \mathbb{K}^+$ eine Abbildung, also eine Verknüpfung auf $\mathbb{K}^+$ ist. Dasselbe gilt für „$\cdot$“.

3.) Auf der Menge $A = \mathrm{Pot}\, M$ sind $\cup$, $\cap$, $\setminus$ Verknüpfungen.

4.) Die Tatsache, dass bei einer Verknüpfung auf A das Ergebnis wieder in A liegen muss (wo steht das?), nennt man auch **Abgeschlossenheit**.

Abbildungen und Mengen

Für $S \subseteq A$ ist $\vec{f}(S) := \{f(x)\,;\ x \in S\}$ (**Bild** oder Bildmenge von S),

für $T \subseteq B$ ist $\overleftarrow{f}(T) := \{a \in A\,;\ f(a) \in T\}$ (**Urbild**(-menge) von T).

Bemerkung. Das Bild $\vec{f}(A)$ einer Abbildung $f : A \to B$ wird oft auch als **Wertebereich** bezeichnet. Es ist die Menge aller Werte, die herauskommen können. Es gilt natürlich $\vec{f}(A) \subseteq B$, aber es muss nicht $\vec{f}(A) = B$ gelten.

(3.4) Beispiele. 1.) Für $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}\,;\ (n,m) \mapsto n+m$ ist

$$\overleftarrow{f}(\{2,4\}) = \{(1,1),(1,3),(2,2),(3,1)\}.$$

2.) Sei M_1 die Menge der Hörer im Hörsaal und M_2 die Menge der Tage eines Jahres, also $M_2 = \{1,2,\ldots,366\}$. Weiter sei $g : M_1 \to M_2$ die Abbildung, bei der jeder Person ihr Geburtstag zugeordnet wird. Was ist dann mit $\overleftarrow{g}(\{1,2,\ldots,31\})$ gemeint; was mit $\overleftarrow{g}(\{60\})$?

(3.5) *Sei $f : A \to B$ eine beliebige Funktion und seien $A_1, A_2 \subseteq A$, $B_1, B_2 \subseteq B$.*

(1) $\vec{f}(A_1 \cup A_2) = \vec{f}(A_1) \cup \vec{f}(A_2)$

(2) $\vec{f}(A_1 \cap A_2) \subseteq \vec{f}(A_1) \cap \vec{f}(A_2)$

(3) $\overleftarrow{f}(B_1 \cup B_2) = \overleftarrow{f}(B_1) \cup \overleftarrow{f}(B_2)$

(4) $\overleftarrow{f}(B_1 \cap B_2) = \overleftarrow{f}(B_1) \cap \overleftarrow{f}(B_2)$

(5) $A_1 \subseteq \overleftarrow{f}(\vec{f}(A_1))$ *und* $\vec{f}(\overleftarrow{f}(B_1)) \subseteq B_1$

Beweis. (1) „$\subseteq$“: Sei $y \in \vec{f}(A_1 \cup A_2) \implies \exists x \in A_1 \cup A_2 : f(x) = y$. Da $x \in A_1$ oder $x \in A_2$ gilt, ist auch $f(x) \in \vec{f}(A_1)$ oder $f(x) \in \vec{f}(A_2)$, also $f(x) = y \in \vec{f}(A_1) \cup \vec{f}(A_2)$.

„$\supseteq$“: Sei $y \in \vec{f}(A_1) \cup \vec{f}(A_2)$, also $y \in \vec{f}(A_1)$ oder $y \in \vec{f}(A_2)$. In beiden Fällen folgt $y \in \vec{f}(A_1 \cup A_2)$.

(2) Übung! *Frage*: Warum gilt hier nicht die Gleichheit?

(3) Sei $x \in \overleftarrow{f}(B_1 \cup B_2) \iff f(x) \in B_1 \cup B_2 \iff f(x) \in B_1 \vee f(x) \in B_2$
$\iff x \in \overleftarrow{f}(B_1) \cup \overleftarrow{f}(B_2)$.

(4) Ersetze in (3) $\cup$ durch $\cap$ und $\vee$ durch $\wedge$.

(5) Für $a \in A_1$ gilt nach Definition $f(a) \in \vec{f}(A_1)$, also $a \in \overleftarrow{f}(\vec{f}(A_1))$.

Sei $y \in \vec{f}(\overleftarrow{f}(B_1))$, dann gibt es $a \in \overleftarrow{f}(B_1)$ mit $f(a) = y$. Das bedeutet aber gerade $y \in B_1$. ∎

Eigenschaften von Abbildungen

Injektiv, surjektiv und bijektiv sind besonders wichtige Begriffe, die Sie Ihr ganzes Studium über beschäftigen werden.

(3.6) Definition. Eine Abbildung $f : A \to B$ heißt

injektiv	$:\Longleftrightarrow$	$x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$ für alle $x_1, x_2 \in A$
surjektiv	$:\Longleftrightarrow$	zu jedem $b \in B$ existiert ein $a \in A$ mit $f(a) = b$
bijektiv	$:\Longleftrightarrow$	f ist injektiv und surjektiv.

Die Bedeutung von injektiv, surjektiv und bijektiv müssen Sie „im Schlaf“ wissen! Wir untersuchen die bisherigen Beispiele auf Injektivität/Surjektivtät/Bijektivität:

(3.7) Beispiele. 1.) $f = \{(0, x), (1, y), (2, x)\}$ ist nicht injektiv ($f(0) = f(2)$), aber surjektiv.

2.) $f : \mathbb{N} \to \mathbb{N}\,;\, n \mapsto 2n - 1$ ist injektiv, aber nicht surjektiv (2 hat kein Urbild).

3.) Auf $\mathbb{N}$ ist die Verknüpfung $+$ wegen $1 + 2 = 2 + 1$ nicht injektiv. Da es zu 1 kein Urbild gibt, ist sie auch nicht surjektiv.

Wenn wir $+$ auf $\mathbb{N}_0$ betrachten, folgt wegen $n = n + 0$ die Surjektivität.

4.) Die Hörer-Geburtstags-Funktion ist sicherlich nicht surjektiv. (Injektiv?)

5.) Was ist mit id_M ?

(3.8) Bemerkung. 1.) Die Definition von injektiv ist äquivalent zu

$$f(x_1) = f(x_2) \implies x_1 = x_2 \quad \text{für alle} \quad x_1, x_2 \in A.$$

Diese Form ist häufig günstiger für Beweise. Zur Begründung können Sie (1.15.7) heranziehen. Warum?

2.) Die Surjektivität der Abbildung $f : A \to B$ bedeutet gerade $\vec{f}(A) = B$.

3.) Das sogenannte „Geburtstagsparadoxon“[7] besagt z. B.:

Die Wahrscheinlichkeit, dass unter mehr als dreißig Personen zwei am gleichen Tag Geburtstag haben, ist größer als 70%.

[7] `http://www.mathematik.ch/anwendungenmath/wkeit/geburtstag`

Bei **reellen Funktionen** $f : \mathbb{R} \to \mathbb{R}$, kann man Injektivität usw. aus einer Zeichnung erkennen. So erhält man eine Visualisierung.

Wir hatten Abbildungen $f : A \to B$ als Teilmenge von $A \times B$ definiert. Im Fall reeller Funktionen ist das also eine Teilmenge von $\mathbb{R}^2$, der Anschauungsebene. In dieser (anschaulichen) Deutung spricht man vom Graphen von f. Genauer: Der **Graph** von f bezeichnet die Menge $\big\{(x, f(x))\,;\; x \in A\big\}$.

Wenn bei einer Funktion $f : \mathbb{R} \to \mathbb{R}$ *jede* Parallele zur x-Achse den Graphen von f höchstens/mindestens/genau einmal schneidet, dann ist die Funktion injektiv/surjektiv/bijektiv.

(3.9) Beispiele. 1.) Die Betragsfunktion $f : \mathbb{R} \to \mathbb{R}\,;\, x \mapsto |x|$, ist nicht injektiv (finde eine Parallele zur x-Achse, die den Graphen der Funktion *mehr als einmal* schneidet) und auch nicht surjektiv (finde eine Parallele zur x-Achse, die den Graphen *nicht* schneidet).

2.) Die **Potenzfunktion** $p_k : \mathbb{R} \to \mathbb{R}\,;\, x \mapsto x^k$ mit $k \in \mathbb{N}$ ist für ungerades k bijektiv. Für k gerade ist p_k wegen $p_k(x) = p_k(-x)$ nicht injektiv, und da $p_k(\mathbb{R})$ keine negativen Zahlen enthält, auch nicht surjektiv.

3.) Es gibt Funktionen von $\mathbb{R}$ nach $\mathbb{R}$, die genau eine der Eigenschaften injektiv/surjektiv besitzen, etwa

$$f(x) := (x-1)x(x+1), \quad g(x) := \begin{cases} x+1 & \text{für} \quad x < 0 \\ x-1 & \text{für} \quad x \geq 0 \end{cases}, \quad h(x) := e^x.$$

Frage: Welche Funktion hat welche Eigenschaft?

Verkettung

Wir fügen dem Hörer–Geburtstags–Beispiel eine weitere Menge

$$M_3 = \{Mo, Di, \ldots, Sa, So\}$$

hinzu und definieren $w : M_2 \to M_3$ durch die Zuordnung Jahrestag $\mapsto$ entsprechender Wochentag in 2018, beispielsweise $w(32) = Do$.[8] Jetzt kann jedem Hörer der Wochentag seines Geburtstages in 2018 zugeordnet werden, indem die Funktionen g und w miteinander **verkettet** bzw. **hintereinander ausgeführt** werden:

$$w \circ g : \begin{cases} M_1 & \to & M_2 & \to & M_3 \\ p & \mapsto & g(p) & \mapsto & w(g(p)) \end{cases}$$

Es ist also $(w \circ g)(x) := w(g(x))$ (beachte: „von rechts nach links“).

[8] Da 2018 kein Schaltjahr ist, setzen wir für den 29.02.18 $w(60) := w(61) = Do$.

(3.10) Definition. Es seien A, B, C, D Mengen, $f : A \to B$, $g : C \to D$ Abbildungen und es gelte $\vec{f}(A) \subseteq C$. Dann nennt man die durch

$$g \circ f : A \to D;\ x \mapsto g(f(x))$$

definierte Abbildung, die **Verkettung** der Abbildungen g nach f.

Auch gebräuchlich sind die Begriffe: **Komposition**, **Hintereinanderausführung**, oder auch **Verknüpfung**.

Beispiel. Seien $f, g, h : \mathbb{R} \to \mathbb{R}$ definiert durch $f(x) := x^2 + 1$, $g(x) := x - 2$, $h(x) := 2x$. Gesucht sind die Funktionen $g \circ h$, $h \circ g$, $(f \circ g) \circ h$ und $f \circ (g \circ h)$.

(3.11) Bemerkung. Die Verkettung von Funktionen ist in der Regel nicht kommutativ, es gilt nicht immer $g \circ f = f \circ g$.

Einfach, aber besonders wichtig ist

(3.12) Satz. *Die Verkettung von Abbildungen ist* ***assoziativ****, d. h. für $f : A \to B$, $g : C \to D$ und $h : E \to F$, mit $\vec{f}(A) \subseteq C$ und $\vec{g}(C) \subseteq E$ gilt*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Beweis. Sei $a \in A$ beliebig. Dann gilt

$$\Big(h \circ (g \circ f)\Big)(a) = h\Big((g \circ f)(a)\Big) = h\Big(g(f(a))\Big) = (h \circ g)(f(a)) = \Big((h \circ g) \circ f\Big)(a).$$

∎

(3.13) Bemerkung. Die Verkettung mit id ist besonders einfach: Sei $f : A \to B$ eine Abbildung, dann gilt $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$. D.h. id wirkt als **neutrales Element**.

Wir untersuchen nun bijektive Abbildungen etwas genauer. Umgangssprachlich ausgedrückt bedeutet bijektiv für eine Abbildung $f : A \to B$, dass bei jedem $b \in B$ genau ein Pfeil (mit Start in A) ankommt. In diesem Fall können wir die Pfeilrichtung umkehren und erhalten eine Abbildung, die jedem $b \in B$ genau ein $a \in A$ zuordnet. Wir erhalten eine durch die Abbildungsvorschrift von f eindeutig festgelegte Abbildung $g : B \to A$.

$$f : A \to B;\ a \mapsto b \quad \text{wird zu} \quad g : B \to A;\ b \mapsto a.$$

(3.14) Beispiele. 1. $f : \{a, b, c\} \to \{0, 1, 2\}$ mit $f(a) = 0$, $f(b) = 2$, $f(c) = 1$ ergibt $g : \{0, 1, 2\} \to \{a, b, c\}$ mit $g(0) = a$, $g(1) = c$, $g(2) = b$.

2. $f : \mathbb{Z} \to \mathbb{Z}$; $z \mapsto z + 1$. Hier ist $g : \mathbb{Z} \to \mathbb{Z}$; $z \mapsto z - 1$.

Etwas formaler ausgedrückt, machen wir Folgendes: Die Abbildung f ist eine Teilmenge von $A \times B$. Wir definieren die neue Menge

$$g := \big\{(b,a)\,;\ (a,b) \in f\big\} \subseteq B \times A.$$

Das entspricht dem „Umkehren der Pfeilrichtung“. Was muss gelten, damit g wieder eine Abbildung ist?

- ▷ Jedes Element von B wird abgebildet: f ist surjektiv
- ▷ Jedem Element von B wird höchstens ein Element aus A zugeordnet: f ist injektiv

f muss also bijektiv sein! Dann kann die Zuordnung Urbild – Bild umgekehrt werden.

(3.15) Definition. Sei $f : A \to B$ eine bijektive Abbildung. Dann heißt die eben definierte Abbildung $g : B \to A$ die zu f gehörende **Umkehrabbildung** oder **inverse Abbildung**, geschrieben $g = f^{-1}$.

Es gilt $\overleftarrow{f}(\{b\}) = \{g(b)\}$ für alle $b \in B$.

Der Begriff der Umkehrabbildung macht nur bei Bijektionen Sinn. Ist eine Abbildung $f : A \to B$ nicht surjektiv, gibt es $b \in B$, bei denen kein Pfeil ankommt; ist f nicht injektiv, gibt es $b \in B$, bei denen mehrere Pfeile ankommen. Man vergleiche diesen Sachverhalt nochmals mit der Definition der Abbildung!

(3.16) Beispiele. 1.) Die Identität $\mathrm{id}_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}; x \mapsto x$, ist zu sich selbst invers.

2.) Zu $f : \mathbb{R} \to \mathbb{R}; x \mapsto 2x$ ist g mit $g(x) = f^{-1}(x) = \frac{1}{2}x$ invers.

3.) Wie lauten die inversen Abbildungen von $x \mapsto x^3$ und $x \mapsto 5x + 2$?

(3.17) *Es sei $f : A \to B$ eine Bijektion mit Umkehrabbildung f^{-1}.*

(1) *f^{-1} ist ebenfalls bijektiv und besitzt die Umkehrabbildung f, d.h. $\big(f^{-1}\big)^{-1} = f$.*

(2) *Es gilt $f^{-1} \circ f = \mathrm{id}_A$ und $f \circ f^{-1} = \mathrm{id}_B$.*

Beweis. Klar! ∎

(3.18) *Seien $f : A \to B$ und $g : B \to C$ bijektiv. Dann ist auch $g \circ f$ bijektiv. Für die Umkehrabbildung gilt $(g \circ f)^{-1} = f^{-1} \circ g^{-1} : C \to A$.*

Beweis. Übung (es sind injektiv und surjektiv nachzuweisen). ∎

Bemerkung. Einige Links zum Thema Funktionen (hauptsächlich reell)

- ▷ Funktionen bei Mathe Online

  `http://www.mathe-online.at/mathint/fun1/i.html`

- ▷ Online Calculator der Universität Nizza (F), `http://wims.unice.fr/wims/` wählen Sie den „Function calculator“.

Folgen

Eine Folge stellt man sich am einfachsten als eine Aneinanderreihung von Zahlen (oder Elementen irgendeiner anderen Menge) vor, die immer weiter geht. Etwa

$$\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \ldots \quad \text{oder} \quad 1, 2, 4, 8, 16, 32, 64, \ldots \quad \text{oder} \quad 0, 1, -1, 2, -2, 3, -3, 4, \ldots$$

In vielen Fällen kann man ein „Bildungsgesetz“ angeben — welche Gesetzmäßigkeiten stecken hinter den Beispielen?

Formal haben wir die

Definition. Sei M eine beliebige Menge. Eine Abbildung $a : \mathbb{N} \to M$ oder $a : \mathbb{N}_0 \to M$ heißt eine **Folge**.

Der Funktionswert $a(n)$ wird normalerweise a_n geschrieben. a_n ist also das n–te **Folgenglied**. (Wenn nichts anderes gesagt wird, fangen wir mit a_1 an.) Man schreibt Folgen im Allgemeinen $(a_n)_{n\in\mathbb{N}}$ oder kürzer (a_n). Wenn klar ist, welche Folge gemeint ist, reicht auch die Angabe der ersten Folgenglieder $a_1, a_2, a_3, \ldots$ (vgl. die einführenden Beispiele). In dieser Vorlesung werden wir uns hauptsächlich mit *reellen* Folgen beschäftigen, d. h. $M = \mathbb{R}$ (und gelegentlich $M = \mathbb{Q}$ oder $M = \mathbb{C}$).

(3.19) Beispiele. 1.) Sind die Folgen 1,2,1,2,1,2,... und 2,1,2,1,2,1,... gleich?

2.) $1, 2, 3, \ldots$. Gemeint ist die Folge (a_n) mit $a_n := n$. Es handelt sich um die Folge der natürlichen Zahlen.

3.) Sei $a_1 := 1$, $a_{n+1} := a_n + 1$. Diese Folge ist **rekursiv** definiert: Man gibt das erste Glied an und eine Vorschrift, wie die weiteren Glieder zu berechnen sind. Diese Folge kam übrigens bereits unter den anderen Beispielen vor.

4.) Durch $f_1 = f_2 := 1$, $f_{n+2} := f_n + f_{n+1}$ wird die sogenannte **Fibonacci-Folge** ebenfalls rekursiv definiert. Sie ist nach Leonardo di Pisa[9] ($\sim$1170 – $>$1240) benannt, und kommt an vielen Stellen innerhalb und außerhalb der Mathematik vor.

5.) Viele mathematische Größen können rekursiv *definiert* werden.

▷ Für ein fest vorgegebenes $q \in \mathbb{R}$ definieren wir rekursiv die **Potenzen** von q

$$q^0 := 1, \quad \text{und} \quad q^n := q^{n-1} \cdot q \quad \text{mit } n \in \mathbb{N}.$$

Für das Beispiel mit $q = 2$ sind die ersten Folgenglieder oben aufgeführt. Im Allgemeinen ergibt sich die Folge $(q^n)_{n\in\mathbb{N}_0}$.

[9] `http://turnbull.mcs.st-and.ac.uk/~history/Mathematicians/Fibonacci.html`

▷ Entsprechend wird die **Fakultät** von $n \in \mathbb{N}_0$ rekursiv erklärt

$$0! := 1, \quad \text{und} \quad (n+1)! := n! \cdot (n+1) \quad \text{mit } n \in \mathbb{N}_0.$$

Die Sprechweise: $n!$: n-Fakultät.

6.) Weitere Beispiele von Folgen: $a_n := \left(1 + \frac{1}{n}\right)^n$, $b_{n+1} := \frac{1}{2}\left(b_n + \frac{2}{b_n}\right)$ mit $b_1 = 2$, $c_n := \frac{1}{2^n\sqrt{5}}\left((1+\sqrt{5})^n - (1-\sqrt{5})^n\right)$.

7.) Die Folge

$$f : \mathbb{N} \to \mathbb{Z}; n \mapsto \begin{cases} \frac{n}{2} & \text{für} \quad n \in 2\mathbb{N} \qquad (n \text{ gerade}) \\ -\frac{n-1}{2} & \text{für} \quad n \in 2\mathbb{N}-1 \quad (n \text{ ungerade}) \end{cases}$$

ist bijektiv. Man bekommt also alle ganzen Zahlen durch $0, 1, -1, 2, -2, 3, -3, 4, \ldots$ genau einmal.

Wir müssen stets den Unterschied zwischen einer Folge (a_n) (immer unendlich viele Glieder) und der Menge ihrer Folgenglieder (Wertemenge, kann endlich sein) vor Augen haben.

Mächtigkeit

Das Zählen einer endlichen Menge kann durch eine Abbildung beschrieben werden (genaueres in der Vorlesung). Diese Idee kann auf alle Mengen übertragen und dadurch formalisiert werden.

(3.20) Definition. Zwei Mengen A, B heißen **gleichmächtig**, geschrieben $|A| = |B|$, wenn es eine bijektive Abbildung $f : A \to B$ gibt.

Die Menge A heißt **unendlich**, wenn sie eine echte Teilmengen besitzt, die zu A gleichmächtig ist. Andernfalls heißt sie **endlich**.

Unsere Definition von unendlich macht aus der Not eine Tugend: Die Tatsache, dass unendliche Mengen „gleichgroße“ Teilmengen besitzen, war die Quelle vieler vermeintlicher Paradoxien, die von Philosophen und Theologen bis ins 19. Jahrhundert diskutiert wurden. Mehr dazu in [Heu03, § 19].

(3.21) Beispiele. 1.) Die Abbildung $\mathbb{N}_0 \to \mathbb{N}; n \mapsto n+1$ ist bijektiv (warum?). Daher gilt $|\mathbb{N}_0| = |\mathbb{N}|$, obwohl doch $\mathbb{N}_0$ ein Element mehr hat!?

Tatsächlich ist $\mathbb{N}$ eine echte Teilmenge von $\mathbb{N}_0$, die gleichmächtig ist. Daher ist $\mathbb{N}_0$ (wie auch $\mathbb{N}$ selbst) unendlich.

2.) Die Mengen $\varnothing$, $\{1\}$, und $\{1,2\}$ besitzen sicher keine echten gleichmächtigen Teilmengen. Sie sind also endlich.

3.) Wir haben in (3.19.7) eine bijektive Abbildung $\mathbb{N} \to \mathbb{Z}$ angegeben. Daher sind $\mathbb{Z}$ und $\mathbb{N}$ gleichmächtig, also $|\mathbb{Z}| = |\mathbb{N}|$.

Etwas anders betrachtet, können wir die ganzen Zahlen als Glieder einer Folge auffassen, nämlich $0, 1, -1, 2, -2, \ldots$. Wir können sie gewissermaßen *durchnummerieren.*

(3.22) Bemerkung. 1.) „gleichmächtig“ ist transitiv wegen (3.18).

„gleichmächtig“ ist auch symmetrisch, d.h. $|A| = |B| \implies |B| = |A|$. Das ergibt sich aus (3.17).

2.) Man kann zeigen, dass es zu jeder nicht leeren, endlichen Menge A stets ein $n \in \mathbb{N}$ und eine bijektive Abbildung $\{1, \ldots, n\} \to A$ gibt.

Wir schreiben $|A| = n$. Außerdem gilt $|\varnothing| = 0$.

3.) Falls eine Menge M zu $\mathbb{N}$ gleichmächtig ist, so schreibt man auch $|M| = \aleph_0$. Da $\mathbb{Z}$ und $\mathbb{N}$ gleichmächtig sind, gilt $|\mathbb{Z}| = \aleph_0$.

4.) Interessante Ergänzungen sind bei Wikipedia zu finden:

- ▷ Unendlichkeit[10]
- ▷ endliche Mengen[11] und unendliche Mengen[12]

Definition. Eine Menge M heißt **abzählbar**, wenn M endlich ist oder es eine bijektive Abbildung $\mathbb{N} \to M$ (bzw. $\mathbb{N}_0 \to M$) gibt.

M heißt **überabzählbar**, wenn M nicht abzählbar ist.

Die Beobachtungen aus (3.19.7) können wir jetzt folgendermaßen formulieren:

(3.23) Satz. *$\mathbb{Z}$ ist abzählbar unendlich.* ∎

Für jede unendliche abzählbare Menge M gilt $|M| = |\mathbb{N}| = \aleph_0$. Die Menge der Glieder einer beliebigen Folge ist stets abzählbar.

Beispiel. Die Menge $G = \{2, 4, 6, \ldots\}$ der geraden natürlichen Zahlen ist abzählbar. Wir geben eine bijektive Abbildung $f : \mathbb{N} \to G$ an. Mit anderen Worten: Wir können die Elemente von G *durchnummerieren.*

n	1	2	3	4	5	6	7	$\cdots$
$f(n)$	2	4	6	8	10	12	14	$\cdots$

oder $f(n) := 2n$.

[10] http://de.wikipedia.org/wiki/Unendlichkeit
[11] http://de.wikipedia.org/wiki/Endliche_Menge
[12] http://de.wikipedia.org/wiki/Unendliche_Menge

Etwas überraschend ist vielleicht die nächste Aussage.

(3.24) Satz (*G. Cantor*). $\mathbb{Q} = \left\{ \frac{a}{b} ;\ a, b \in \mathbb{Z}, b \neq 0 \right\}$ *ist abzählbar.*

Beweis. Wir zeigen zunächst, dass die Menge $\mathbb{Q}^+$ der positiven rationalen Zahlen abzählbar ist. Wir machen dies mit dem sog. **Cantorschen Diagonalverfahren** und ordnen die Elemente aus $\mathbb{Q}^+$ in dem folgenden Schema an. Wir folgen bei der Nummerierung der Elemente von $\mathbb{Q}^+$ (dies entspricht einer Bijektion $\mathbb{N} \to \mathbb{Q}^+$) den Pfeilen. Dabei überspringen wir alle Zahlen, die in der Nummerierung schon einmal (in anderer Darstellung) aufgetreten sind.

$$
\begin{array}{ccccccccccc}
\frac{1}{1} & & \frac{2}{1} & \to & \frac{3}{1} & & \frac{4}{1} & \to & \frac{5}{1} & & \frac{6}{1} & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \\
\frac{1}{2} & & \frac{2}{2} & & \frac{3}{2} & & \frac{4}{2} & & \frac{5}{2} & & \frac{6}{2} & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \\
\frac{1}{3} & & \frac{2}{3} & & \frac{3}{3} & & \frac{4}{3} & & \frac{5}{3} & & \frac{6}{3} & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \\
\frac{1}{4} & & \frac{2}{4} & & \frac{3}{4} & & \frac{4}{4} & & \frac{5}{4} & & \frac{6}{4} & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \\
\frac{1}{5} & & \frac{2}{5} & & \frac{3}{5} & & \frac{4}{5} & & \frac{5}{5} & & \frac{6}{5} & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \\
\frac{1}{6} & & \frac{2}{6} & & \frac{3}{6} & & \frac{4}{6} & & \frac{5}{6} & & \frac{6}{6} & \cdots \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & \ddots
\end{array}
$$

Auf diese Art erhält man eine bijektive Abbildung $q : \mathbb{N} \to \mathbb{Q}^+$, nämlich

$$q_1 = 1,\ q_2 = \frac{1}{2},\ q_3 = 2,\ q_4 = 3,\ q_5 = \frac{1}{3},\ q_6 = \frac{1}{4}, \ldots$$

Hieraus kann man dann nach folgendem Schema eine Abzählung aller Elemente von $\mathbb{Q}$ gewinnen: $0,\ q_1,\ -q_1,\ q_2,\ -q_2,\ q_3,\ -q_3, \ldots$. ∎

(3.25) Bemerkung. 1.) Das Diagonalverfahren und die Erkenntnis, dass $\mathbb{Q}$ abzählbar ist (und $\mathbb{R}$ nicht) gehört zu den größten Errungenschaften des Mathematikers Georg Cantor, der schon in Kapitel 1 erwähnt wurde.

2.) Auch der folgende Satz und sein Beweis gehen auf Cantor zurück. Er zeigt, dass es auch Mengen gibt, die man nicht mehr durchnummerieren kann.

3.) Cantor hat seine Entdeckungen zum Anlass genommen, eine Theorie der *Kardinalzahlen* und der *Ordinalzahlen* zu entwickeln. Sie ist ein wichtiger Bestandteil der Mengenlehre.

4.) Mit dem Diagonalverfahren (analog zum letzten Beweis) können wir die Abzählbarkeit von Mengen wie $\mathbb{Q} \times \mathbb{Q}$ oder $\mathbb{Z}^n$ nachweisen.

5.) Die abzählbare Vereinigung von abzählbaren Mengen ist ebenfalls abzählbar (Beweis mit modifiziertem Diagonalverfahren).

Im Gegensatz dazu:

(3.26) Satz (G. Cantor). $\mathbb{R}$ *ist überabzählbar.*

Beweis. Wir zeigen, dass bereits die Menge $I =]0,1[$ aller reeller Zahlen zwischen 0 und 1 überabzählbar ist. Wir führen einen Widerspruchsbeweis und nehmen an, dass I doch abzählbar ist. Die Folge $r_1,\ r_2,\ r_3, \ldots$ sei das Resultat einer fiktiven bijektiven Abbildung $r : \mathbb{N} \to I$.

Wir stellen die Zahlen $r_1,\ r_2,\ r_3, \ldots$ als unendliche Dezimalbrüche dar:

$$\begin{array}{lcll} r_1 & = & 0.s_{11}s_{12}s_{13}s_{14}s_{15} & \ldots \\ r_2 & = & 0.s_{21}s_{22}s_{23}s_{24}s_{25} & \ldots \\ r_3 & = & 0.s_{31}s_{32}s_{33}s_{34}s_{35} & \ldots \\ r_4 & = & 0.s_{41}s_{42}s_{43}s_{44}s_{45} & \ldots \\ \vdots & & & \ddots \end{array}$$

Allgemein:

$$r_i \quad = \quad 0.s_{i1}s_{i2}s_{i3}s_{i4}s_{i5} \quad \ldots$$

Es bezeichnet $s_{ij} \in \{0, 1, 2, \ldots, 9\}$ die j-te Stelle der Dezimalbruchdarstellung von r_i. Es sei vorausgesetzt, dass in diesen Dezimaldarstellungen nicht alle Ziffern von einer bestimmten Stelle an 9 sind, zum Beispiel schreiben wir $0.2000\ldots$ anstelle von $0.19999\ldots$.

Es sei nun $u \in I$ die Zahl mit der Dezimaldarstellung $u = 0.s_1s_2s_3s_4s_5\ldots$, wobei gelte

$$s_i = \begin{cases} s_{ii} - 1, & \text{falls } \ s_{ii} \geq 1 \\ 1, & \text{falls } \ s_{ii} = 0 \end{cases}$$

Dann kommt u unter den Zahlen $r_1,\ r_2,\ \ldots$ garantiert nicht vor, da sich u und r_i für jedes i an der i-ten Stelle unterscheiden $(i = 1, 2, \ldots)$. Dies ist ein Widerspruch, und der Satz ist somit bewiesen. ∎

Frage: Warum kann man mit dem Beweis von Satz (3.26) nicht analog die „Überabzählbarkeit“ von $\mathbb{Q}$ nachweisen?

Bemerkung. Aufgrund des letzten Satzes wissen wir, dass es mehr irrationale als rationale Zahlen gibt. Wäre $\mathbb{R} \setminus \mathbb{Q}$ nämlich abzählbar, müsste auch $\mathbb{R} = \mathbb{R} \setminus \mathbb{Q} \cup \mathbb{Q}$ abzählbar sein. Etwas lax formuliert können wir sagen, dass bereits die Anzahl der irrationalen Zahlen zwischen 0 und 1 größer ist als die aller rationalen Zahlen.

In den Übungen wird die Gleichmächtigkeit von zwei beliebigen echten reellen Intervallen gezeigt. Jedes noch so kleine Intervall enthält also überabzählbar viele reelle Zahlen. Trotzdem ist jede Menge paarweise disjunkter echter Intervalle höchstens abzählbar, da es in jedem Intervall eine rationale Zahl gibt und $\mathbb{Q}$ abzählbar ist! Kaum vorstellbar ist ferner, dass man in beliebiger Nähe jeder der überabzählbar vielen reellen Zahlen stets auch unendlich viele rationale Zahlen findet, obwohl es hiervon „nur“ abzählbar viele gibt!

Zum Schluss zeigen wir, dass sich die Theorie der *Kardinalzahlen* nicht auf abzählbar vs. überabzählbar beschränkt. Zu jeder Menge gibt es eine Menge mit *größerer* Mächtigkeit.

(3.27) Satz. *Sei M eine beliebige Menge. Dann gilt $|M| \neq |\operatorname{Pot} M|$.*

Beweis. Für endliche Mengen ist die Behauptung klar.

Für unendliche Mengen argumentieren wir indirekt. Angenommen, es gibt eine Bijektion $f : M \to \operatorname{Pot} M$, bei der jedem Element $x \in M$ eine Teilmenge $f(x) \subseteq M$ zugeordnet wird. Wir interessieren uns für diejenigen $x \in M$, die nicht in ihrem Bild $f(x)$ liegen. Sei $A := \{x \in M\,;\, x \notin f(x)\} \subseteq M$. Da f nach Annahme bijektiv ist, hat auch die Menge A ein Urbild $a \in M$. Wir untersuchen, ob a in A liegt.

1. Fall $a \in A$: Geht nicht wegen $a \in A = f(a) \implies a \notin A$

2. Fall $a \notin A$: Geht nicht wegen $a \notin A = f(a) \implies a \in A$

Damit ist die Annahme der Existenz einer Bijektion zwischen M und ihrer Potenzmenge ad absurdum geführt, diese Mengen sind nicht gleichmächtig. ∎

Dieser Beweis erinnert an das Dilemma des Barbiers (Friseurs), der genau die Personen rasieren soll, die sich nicht selbst rasieren!

(3.28) Bemerkung. 1.) Die Menge aller Folgen auf einer Menge M hat größere Mächtigkeit als M. Die Beweisidee ist analog zum Beweis von (3.26). (siehe auch [Heu03, S.139f]).

2.) Die Menge aller Abbildungen $\mathbb{R} \to \mathbb{R}$ ist nicht gleichmächtig zu $\mathbb{R}$ (vgl. [AA05, Bsp. 2.18S. 57]).

4 Die natürlichen Zahlen

„*Die natürlichen Zahlen hat der liebe Gott geschaffen, alles andere ist Menschenwerk*“

Leopold Kronecker[13] (1823–1891)

„*Die natürlichen Zahlen sind freie Schöpfungen des menschlichen Geistes*“

Richard Dedekind[14] (1831–1916)

Sicher ist, dass sich die Menschheit seit frühester Zeit mit Zahlen beschäftigt und diese Beschäftigung *ein*, wenn nicht *der*, Ursprung der Mathematik ist.

Das Ziel dieses Kapitels ist es, die Menge $\mathbb{N}$ (bzw. $\mathbb{N}_0$) der natürlichen Zahlen axiomatisch aufzubauen und alle bekannten Operationen abzuleiten.

Noch strenger als in den vorherigen Kapiteln gilt: Wir dürfen uns bei der Argumentation nicht auf Schulwissen und Anschauung zurückziehen, sondern müssen ausgehend von den Axiomen jede Aussage beweisen; jedes mathematische Objekt (wie z.B. die Multiplikation) definieren. Außerdem kommen natürlich Mengenlehre und Aussagenlogik zur Anwendung.

Zunächst sammeln wir in der Vorlesung wichtige Bausteine der natürlichen Zahlen und ihre Eigenschaften. Dann versuchen wir beispielhaft zu ergründen, welche davon man von anderen ableiten kann. Um die Axiome möglichst einfach zu halten, werden die ableitbaren Objekte nicht in die Liste der Axiome aufgenommen.

Die Peanoschen Axiome

Um die Axiome zu motivieren (man kann sie nicht *herleiten*!), überlegen wir nochmals, wie „*Zählen*“ funktioniert. Wir geben uns eine Menge M vor, die als Vergleich dient. Das wird später die Menge $\mathbb{N}_0$ sein.

Zunächst brauchen wir einen Startpunkt. Üblicherweise beginnt man beim Zählen mit 1. Wir könnten also fordern $1 \in M$. Aus beweistechnischen (und anderen) Gründen, die später hoffentlich einleuchten werden, setzen wir den Startpunkt bei 0, also

$$0 \in M.$$

Vorgreifend kann man sagen: Die Mächtigkeit der leeren Menge ist ein Element von M.

Beim Zählen wird dann schrittweise die Menge M durchlaufen. Jedes Element n in M hat also einen eindeutig bestimmten **Nachfolger**; das Element $\nu(n)$, das beim Zählen als nächstes benutzt wird. Etwas formaler ausgedrückt:

$$\text{Es gibt eine Abbildung} \qquad \nu : M \to M.$$

[13] `http://de.wikipedia.org/wiki/Leopold_Kronecker`
[14] `http://de.wikipedia.org/wiki/Richard_Dedekind`

Die nächsten Schritte bestehen darin, die (wichtigsten, einfachsten) Eigenschaften dieser Nachfolger-Abbildung festzulegen.

Zunächst einmal kann unser Startelement 0 nicht selbst Nachfolger eines anderen Elementes sein.

Kann es sein, dass zwei Elemente $n, m \in M, n \neq m$, den selben Nachfolger haben? Das würde unserer Vorstellung vom Zählen sicher widersprechen, wir fordern also, dass ν injektiv ist.

Wenn alle diese Eigenschaften erfüllt sind, dann gibt es immer noch Möglichkeiten für die Menge M, die wir ausschließen wollen, weil sie mit unserer Vorstellung vom Zählen nicht vereinbar sind. Sie werden in der Vorlesung durch Skizzen veranschaulicht. So muss jedes Element aus M durch sukzessives Anwenden von ν aus 0 zu gewinnen sein. In gewissem Sinne ist M die „kleinste“ Menge, die die oben angeführten Eigenschaften besitzt. Dieser Sachverhalt wird mit dem **Induktionsaxiom** formalisiert:

$$\forall A \subseteq M : 0 \in A \wedge \vec{\nu}(A) \subseteq A \implies A = M.$$

Es sollte klar sein, dass die angegebenen Bedingungen für natürliche Zahlen erfüllt sein müssen, bzw., dass diese Bedingungen unserer Intuition von natürlichen Zahlen entsprechen. Dass man alles, was Sie über natürliche Zahlen wissen, aus diesen Axiomen herleiten kann, ist an dieser Stelle nicht klar. In der Tat wird sich herausstellen, dass man Anordnung, Addition, und Multiplikation aus der Nachfolger-Abbildung ableiten und alle bekannten Eigenschaften beweisen kann.

Das Axiomensystem stammt von dem italienischen Mathematiker Giuseppe Peano[15] (1858 – 1932). Wir fassen zusammen:

(4.1) Definition (Die Peanoschen Axiome). Es existiert eine Menge $\mathbb{N}_0$, ein Element $0 \in \mathbb{N}_0$ und eine Abbildung $\nu : \mathbb{N}_0 \to \mathbb{N}_0$, für die gilt

(P1) $\forall n \in \mathbb{N}_0 : \nu(n) \neq 0$. Dazu äquivalent: $0 \notin \vec{\nu}(\mathbb{N}_0)$.

(P2) ν ist injektiv.

(P3) $\forall A \subseteq \mathbb{N}_0 : 0 \in A \wedge (\forall n \in A : \nu(n) \in A) \implies A = \mathbb{N}_0$.

Wir nennen $\mathbb{N} := \mathbb{N}_0 \setminus \{0\}$ die **Menge der natürlichen Zahlen**.

Bevor wir weiter machen, einige Bemerkungen zu unserer Definition.

(4.2) Bemerkung. 1.) Die **Existenz** von $\mathbb{N}_0$, der Zahl 0 und der Abbildung ν wird einfach postuliert. Im Rahmen der Mengenlehre kann man dieses Problem umgehen. Genauer: Die Axiome der Mengenlehre sind so formuliert, dass die Existenz von $\mathbb{N}_0$ mit den genannten Eigenschaften folgt.

[15] `http://de.wikipedia.org/wiki/Peano`

2.) Die **Eindeutigkeit** werden wir nicht diskutieren. Dazu müssten wir

- ▷ klären, was *eindeutig* in diesem Zusammenhang bedeuten soll;
- ▷ den Dedekindschen Rekursionssatz beweisen, der auch eine formale Rechtfertigung für „Definition durch Rekursion“ gibt (siehe z.B. [AA05, Satz 6.1]).

Beides ist begrifflich nicht ganz einfach und soll hier übersprungen werden.

3.) Wir stellen aber fest: Bis auf Bezeichnung der Elemente ist die Menge $\mathbb{N}_0$ und damit auch $\mathbb{N}$ eindeutig festgelegt.

4.) Wir haben nicht gesagt, was eine natürliche Zahl *ist*. Wir haben lediglich die Menge der natürlichen Zahl über gewisse Eigenschaften definiert. Diese Vorgehensweise ist typisch für die moderne Mathematik. Auch bei der Definition der reellen Zahlen sind wir so vorgegangen. Ähnliches wird Ihnen noch häufiger begegnen.

5.) Für historisch interessierte ist die Orginalarbeit von Richard Dedekind [Ded65] lesenswert. Sie enthält neben dem Rekursionssatz eine Axiomatik für die natürlichen Zahlen, die aber etwas umständlicher ist als Peanos.

6.) Bei der Formulierung und Nummerierung der Axiome weichen wir von der historischen Darstellung ab, die in vielen Büchern übernommen wird. So werden die Objekte deutlicher von ihren Eigenschaften unterschieden.

Wir ziehen einige einfache (selbstverständliche?) Folgerungen aus den Axiomen. Es sei nochmals betont: Wir müssen *jede* Aussage, auch wenn sie noch so banal aussieht, aus den Axiomen herleiten.

(4.3) $\vec{\nu}(\mathbb{N}_0) = \mathbb{N}$.

Beweis. Offenbar gilt $\vec{\nu}(\mathbb{N}_0) \subseteq \mathbb{N}$ (wg. (P1)).

Also bleibt zu zeigen, dass $\vec{\nu}(\mathbb{N}_0) \supseteq \mathbb{N}$. Dazu nutzen wir (P3) und setzen

$$A := \{0\} \cup \big\{m \in \mathbb{N}_0\,;\ \exists n \in \mathbb{N}_0 : \nu(n) = m\big\} = \{0\} \cup \vec{\nu}(\mathbb{N}_0).$$

Diese Menge enthält das Startelement und die Menge aller Nachfolger. Es gilt $0 \in A$ nach Definition. Weiter ist für jedes $m \in A$ auch $\nu(m) \in A$, da $\nu(m)$ der Nachfolger von m ist.

Mit (P3) folgt $A = \mathbb{N}_0$, also $\mathbb{N} = A \setminus \{0\} \subseteq \vec{\nu}(\mathbb{N}_0)$. ∎

Damit ist die Abbildung $\bar{\nu} : \mathbb{N}_0 \to \mathbb{N}; n \mapsto \nu(n)$ bijektiv, und $\mathbb{N}_0$ und $\mathbb{N}$ sind unendliche Mengen.

Der vorige und auch der folgende Beweis sind typisch für Aussagen, die für alle Elemente aus $\mathbb{N}$ oder $\mathbb{N}_0$ getroffen werden. Wir werden diese Methode unter dem Namen *vollständige Induktion* noch genauer studieren. Sie basiert wesentlich auf Axiom (P3).

(4.4) *Für alle* $n \in \mathbb{N}_0$ *gilt* $\nu(n) \neq n$.

Beweis (erste Version). Wir setzen $A := \{n \in \mathbb{N}_0 \,;\, \nu(n) \neq n\}$. Klar ist $0 \in A$, denn $0 \notin \vec{\nu}(\mathbb{N}_0)$. Für $n \in A$ gilt $\nu(n) \neq n$ und mit (P2) auch $\nu(\nu(n)) \neq \nu(n)$. Es folgt $\nu(n) \in A$. Mit (P3) folgt $A = \mathbb{N}_0$ und das ist die Behauptung. ∎

Bemerkung. Wir haben in wenigen Zeilen eine Aussage für unendlich viele Fälle bewiesen! Hier gibt es keine Alternative zu einem formalen Beweis, indem man etwa versucht, alle Fälle auszuprobieren. (Alles durchprobieren kann natürlich auch ein Beweis sein!)

Wir definieren jetzt ein erstes neues Element in $\mathbb{N}_0$ durch

$$1 := \nu(0).$$

Die Aussage (P3) gilt dann in modifizierter Form auch für $\mathbb{N}$.

(4.5) $\forall A \subseteq \mathbb{N} : 1 \in A \wedge \vec{\nu}(A) \subseteq A \implies A = \mathbb{N}$.

Beweis. Wir setzen $A_0 := A \cup \{0\} \subseteq \mathbb{N}_0$. Dann gilt $0 \in A_0$. Für alle $n \in A_0$ gilt entweder $n = 0$ und $\nu(0) = 1 \in A_0$ oder $n \in A$ und $\nu(n) \in A \subseteq A_0$. Insgesamt also $\vec{\nu}(A_0) \subseteq A_0$. Mit (P3) folgt $A_0 = \mathbb{N}_0$ und damit $A = \mathbb{N}$. ∎

Vollständige Induktion (einfache Form)

Das Induktionsaxioms (P3) liefert eine Beweismethode, mit der man Aussagen für alle natürlichen Zahlen (oder ganz $\mathbb{N}_0$) beweisen kann. Diese Methode heißt **vollständige Induktion**. Wir haben sie in Beweisen im vorigen Abschnitt schon angewendet. Hier wollen wir diese Methode etwas genauer beschreiben und formalisieren.

Gegeben sei eine Aussageform $A(n)$ in einer Variablen n aus der Grundmenge $\mathbb{N}_0$ (oder $\mathbb{N}$). Die Menge $\mathcal{A} := \{n \in \mathbb{N}_0 : A(n)\}$ enthält alle natürlichen Zahlen oder 0, für die $A(n)$ wahr ist. Dann gilt nach Konstruktion

$$n \in \mathcal{A} \iff A(n).$$

Daher kann man das Induktionsaxiom (P3) umformulieren in

$$A(0) \wedge \Big(\forall\, n \in \mathbb{N}_0 : A(n) \implies A(\nu(n))\Big) \implies \forall\, n \in \mathbb{N}_0 : A(n)$$

oder gemäß (4.5)

$$A(1) \wedge \Big(\forall\, n \in \mathbb{N} : A(n) \implies A(\nu(n))\Big) \implies \forall\, n \in \mathbb{N} : A(n).$$

Wie also funktioniert ein Induktionsbeweis? Wir formulieren das Schema für $\mathbb{N}$. Für $\mathbb{N}_0$ geht es analog.

▷ Gegeben ist eine Aussageform $A(n)$ mit Grundmenge $\mathbb{N}$.

▷ Beweise $A(1)$.

▷ Für fest gewähltes, aber beliebiges $n \in \mathbb{N}$ zeige:

Falls $A(n)$ gilt, dann gilt auch $A(\nu(n))$.

▷ Dann ist bewiesen: $\forall n \in \mathbb{N} : A(n)$.

Die wesentlichen Schritte ergeben das

Beweisschema zur vollständige Induktion:

IA *Induktionsanfang*: $A(1)$.

IV *Induktionsvoraussetzung*: Es gelte $A(n)$ für ein beliebiges (aber festes) $n \in \mathbb{N}$.

IS *Induktionsschluss*: Für das feste n aus der IV gilt mit $A(n)$ auch $A(\nu(n))$.

Zur Illustration führen wir nochmals den

Beweis (von (4.4); zweite Version). Wir definieren die Aussageform $A(n) := (n \neq \nu(n))$ mit $n \in \mathbb{N}_0$. Das ist die Aussage, dass n nicht mit seinem Nachfolger übereinstimmt. Nun arbeiten wir das Schema ab:

IA: Gemäß (P1) ist $A(0)$ wahr (i.a.W.: $0 \neq \nu(0) = 1$).

IV: Es gelte $A(n)$ für ein beliebiges (aber festes) $n \in \mathbb{N}_0$.

IS: Nach IV ist $n \neq \nu(n)$. Wegen (P2) gilt dann auch $\nu(n) \neq \nu\Big(\nu(n)\Big)$, was gleichbedeutend ist mit $A(\nu(n))$. ∎

(4.6) Bemerkung. 1.) Der erste Beweis zu (4.4) und die obige zweite Version unterscheiden sich nicht in der Beweisidee. Sie sind nur verschieden aufgeschrieben.

2.) Die Aussageform wird meist nicht explizit formuliert. Sie ergibt sich aus der Formulierung des zu beweisenden Satzes. Das Schema wird dann noch etwas kürzer.

3.) Die Formulierung von IV ist nur ein formaler Akt, der das Aufschreiben des eigentlichen Beweises in IS unterstützen soll. Das bedarf keiner Arbeit. Experten lassen die Induktionsvoraussetzung gerne einfach weg.

4.) IV darf *nicht* mit der zu beweisenden Aussage verwechselt werden; es bedeutet *nicht*, dass man $A(n)$ *für alle* n annimmt! Vielmehr geht es darum von einer beliebigen Stelle aus einen Schritt weiter zu kommen (zu $A(\nu(n))$). Man spricht auch vom Domino-Prinzip, das in der Vorlesung erläutert wird.

Die Addition

Der nächste Schritt auf unserem Weg zu den bekannten Eigenschaften der natürlichen Zahlen ist die Einführung einer Addition. Wie kann man von der Nachfolger-Abbildung auf die Summenbildung von natürlichen Zahlen kommen?

Die Setzungen $n+0 := n$ und $n+1 := \nu(n)$ sind naheliegend. Aber wie ist $n+m$ zu definieren?

(4.7) Definition. Für alle $n, m \in \mathbb{N}_0$ setzen wir rekursiv

$$n + 0 := n \quad \text{und} \quad n + \nu(m) := \nu(n + m).$$

Dadurch wird eine Verknüpfung

$$+ : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0; (n, m) \mapsto n + m$$

auf $\mathbb{N}_0$ erklärt, die **Addition** genannt wird.

Bemerkung. 1.) Diese Definition ist *kein* neues Axiom, sondern lediglich eine Abkürzung für eine (komplizierte?) Konstruktion auf Basis der Axiome. Man kann an jeder Stelle das Symbol $+$ durch die Definition ersetzen (auch wenn das sehr schwerfällig würde).

2.) Eigentlich wird durch die Rekursion für jedes $n \in \mathbb{N}_0$ eine Folge $(\alpha_m)_{m\in\mathbb{N}_0}$ definiert.

Wir formulieren eine erste wichtige Eigenschaft der Addition.

(4.8) Satz. *Die Addition auf* $\mathbb{N}_0$ *ist* ***assoziativ*** *mit* ***neutralem Element*** 0 *d.h. es gilt*

$$\forall a, b, n \in \mathbb{N}_0 : (a + b) + n = a + (b + n) \quad \textit{und} \quad n + 0 = 0 + n = n.$$

Beweis. Für die zweite Aussage muss nur $0 + n = n$ gezeigt werden. Der Induktionsanfang ist trivial. Wir nehmen also $0 + n = n$ für ein $n \in \mathbb{N}_0$ an und erhalten

$$0 + \nu(n) \overset{\text{Def}}{=} \nu(0 + n) \overset{\text{IV}}{=} \nu(n).$$

Nun zur Assoziativität: Wir machen eine Induktion nach n. Dabei seien $a, b \in \mathbb{N}_0$ fest gewählt.

IA: $(a + b) + 0 = a + b = a + (b + 0)$ nach Definition.

IV: Für ein $n \in \mathbb{N}_0$ gelte $(a + b) + n = a + (b + n)$.

IS: Wir müssen zeigen, dass $(a + b) + \nu(n) = a + (b + \nu(n))$. Es gilt

$$(a + b) + \nu(n) \overset{\text{Def}}{=} \nu\Big((a + b) + n\Big) \overset{\text{IV}}{=} \nu\Big(a + (b + n)\Big) \overset{\text{Def}}{=} a + \nu(b + n) \overset{\text{Def}}{=} a + (b + \nu(n)).$$

Damit ist die Behauptung gezeigt. ∎

Ebenfalls wichtig

(4.9) Satz. *Für die Addition auf* $\mathbb{N}_0$ *gilt*

(1) $\forall m \in \mathbb{N}_0 : \nu(m) = m + 1 = 1 + m\,.$

(2) $\forall a, n \in \mathbb{N}_0 : a + n = n + a.$ ***(Kommutativgesetz)***

(3) $\forall a, b \in \mathbb{N}_0 : a + b = 0 \implies a = 0 \wedge b = 0\,.$

Beweis. (1) Es gilt $(\star)$ $\quad \nu(m) = \nu(m + 0) = m + \nu(0) = m + 1$ für alle $m \in \mathbb{N}_0\,.$

Die zweite Gleichheit wird mit Induktion nach m gezeigt.

IA steht in (4.8).

IV: Für ein $m \in \mathbb{N}_0$ gelte $1 + m = m + 1\,.$

IS: Es gilt $1 + \nu(m) = \nu(1 + m) \overset{\text{IV}}{=} \nu(\underbrace{m + 1}_{=\nu(m)}) \overset{(\star)}{=} \nu(\nu(m)) \overset{(\star)}{=} \nu(m) + 1\,.$

(2) Mit Induktion nach n:

IA steht in (4.8).

IV: Für ein $n \in \mathbb{N}_0$ gilt $a + n = n + a\,.$

IS: Wir rechnen

$$\begin{aligned} a + \nu(n) &= \nu(a + n) \overset{\text{IV}}{=} \nu(n + a) = n + \nu(a) \overset{(1)}{=} n + (1 + a) \\ &\overset{(4.8)}{=} (n + 1) + a \overset{(1)}{=} \nu(n) + a. \end{aligned}$$

(3) Angenommen $b \neq 0$, dann existiert $c \in \mathbb{N}_0$ mit $\nu(c) = b$ nach (4.3). Es folgt

$$0 = a + b = a + \nu(c) = \nu(a + c),$$

ein Widerspruch zu (P1). ∎

Wir haben bis dato gezeigt, dass $+$ eine assoziative und kommutative Verknüpfung auf $\mathbb{N}_0$ mit neutralem Element 0 ist. Wir führen jetzt die bekannten Zahlzeichen ein. Die Verwendung des Dezimalsystems muss später noch gerechtfertigt werden.

(4.10) Definition. Ist ν die Nachfolger-Abbildung auf $\mathbb{N}_0$, so definiert man (im üblichen Dezimalsystem mit indisch-arabischen Ziffern $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$)

$2 := \nu(1)$, $3 := \nu(2)$, $4 := \nu(3)$, $5 := \nu(4)$, $6 := \nu(5)$, $7 := \nu(6)$, $8 := \nu(7)$, $9 := \nu(8)$, $10 := \nu(9)$, $11 := \nu(10)$ usw.

Bemerkung. Es ist wichtig, sich klar zu machen, dass man anstelle von $1 = \nu(0)$, $2 := \nu(1)$, $3 := \nu(2)$, ... auch I:= $\nu(0)$, II:= $\nu(\mathrm{I})$, III:= $\nu(\mathrm{II})$, IV:= $\nu(\mathrm{III})$ usw. oder etwas beliebiges anderes hätte definieren können. Entscheidend ist, dass die natürlichen Zahlen durch die Zahlzeichen eindeutig bestimmt sind.

Wir können jetzt z.B. beweisen, dass $1 + 1 = 2$ ist, und $5 + 3 = 8 = 3 + 5$:

$$\begin{aligned} 5+3 &= 5+\nu(2) = \nu(5+2) = \nu\Big(5+\nu(1)\Big) = \nu\Big(\nu(5+1)\Big) = \nu\Big(\nu\Big(\nu(5)\Big)\Big) = \\ &= \nu\Big(\nu\Big(6\Big)\Big) = \nu(7) = 8 = 3+5. \end{aligned}$$

Wobei mehrfach (4.10) bzw. (4.7) und am Schluss (4.9) angewendet wurden.

Die obigen Sätze rechtfertigen es, die Nachfolger-Abbildung ν durch $x \mapsto x + 1$ zu ersetzen, d.h. wir werden ab sofort meist $u+1$ statt $\nu(u)$ schreiben. Insbesondere werden dann die Induktionsbeweise so aussehen, wie Sie es gewohnt sind. Die Rechengesetze werden wir häufig ohne Referenzen anwenden.

Zum Abschluss dieses Abschnitts zeigen wir die

(4.11) Kürzregel der Addition. *Für $a, b, n \in \mathbb{N}_0$ gilt $a + n = b + n \implies a = b$.*

Beweis (Induktion nach n; Kurzform). IA ist trivial (warum?).

$n \rightsquigarrow n+1$: Es gilt $a + (n + 1) = b + (n + 1) \implies \nu(a + n) = \nu(b + n) \overset{\text{(P2)}}{\implies}$
$a + n = b + n \overset{\text{IV}}{\implies} a = b$. ∎

Wir haben diesen Induktionsbeweis in einer Weise aufgeschrieben, die nur die wesentlichen Beweisschritte darstellt. Wir nennen das die **Kurzform**.

Anordnung und allgemeine Induktion

Direkt aus der Addition erhält man die Anordnung „$<$“ auf den natürlichen Zahlen. Für sie *soll* gelten

$$\forall n, m \in \mathbb{N}_0 \ : \ (n < m \iff \exists k \in \mathbb{N} : n + k = m).$$

Im Unterschied zu den reellen Zahlen — vgl. (2.5) — haben wir hier eine Definition von „$<$“ angegeben, die nur die vorher definierte Addition voraussetzt. Die Rolle der Menge $\mathbb{K}^+$ spielt $\mathbb{N}$ selbst. Wir beweisen

(4.12) Satz. *Für alle $n, m, u \in \mathbb{N}_0$ gilt*

(1) *genau eine Aussage $m < n \ \vee \ n = m \ \vee \ n < m$ (**Trichotomie**).*

(2) $m < n \ \wedge \ n < u \implies m < u$ *(**Transitivität**).*

Beweis. (1) Wir zeigen zunächst, dass sich die drei Möglichkeiten gegenseitig ausschließen. Im Fall $n = m$ ist das klar.

Es sei also $n, m \in \mathbb{N}_0$ mit $n < m$, dann existiert $k \in \mathbb{N}$ mit $n+k = m$. Aus $n = m$ würde $n+k = n$ und mit der Kürzregel (4.11) $k = 0$ folgen, ein Widerspruch. Falls nun $m < n$ wäre, so existierte $\ell \in \mathbb{N}$ mit $m + \ell = n$. Es würde folgen $n + k + \ell = n = n + 0$ (nach (4.8)) und mit der Kürzregel (4.11) $k+\ell = 0$. Hieraus folgt mit (4.9.3) der Widerspruch $k = \ell = 0$.

Um zu zeigen, dass je zwei Elemente n, m vergleichbar sind, wählen wir ein festes aber beliebiges $n \in \mathbb{N}_0$ und führen eine Induktion nach m durch.

IA: $m = 0$. Man hat $0 = n$ oder $0 < n$ wegen (4.8) und (4.9.3).

IV: Für ein $m \in \mathbb{N}_0$ gelte $m < n \ \vee \ n = m \ \vee \ n < m$.

IS: Nun betrachten wir $m + 1$ statt m. Wir führen eine Fallunterscheidung unter Rückgriff auf die Induktionsvoraussetzung durch.

1. Fall $m < n$: Dann gibt es $k \in \mathbb{N}$ mit $m + k = n$. Nach (4.3) existiert $k' \in \mathbb{N}_0$ mit $k' + 1 = \nu(k') = k$. Daher folgt $m + 1 + k' = n$. Im Fall $k' = 0$ gilt $m + 1 = n$; im Fall $k' \in \mathbb{N}$ gilt $m + 1 < n$.

2. Fall $n = m$: Dann gilt $n < m + 1$.

3. Fall $n < m$: Dann gilt $m = n+k$ für ein $k \in \mathbb{N}$ und mit (4.8) auch $m+1 = n+(k+1)$, also $n < m + 1$.

Somit tritt auch für $m + 1$ einer der Fälle auf. Das zeigt die Behauptung.

(2) Transitivität folgt direkt aus (4.8). ∎

Wir benutzen ab sofort die üblichen Symbole $\leq, >, \geq$ mit der bekannten Bedeutung. Sie leiten sich direkt aus der Definition von $<$ ab.

Das Zusammenspiel von „$+$“ und „$\leq$“ regelt das

(4.13) Monotoniegesetz für die Addition. *Für alle* $a, b, c \in \mathbb{N}_0$ *gilt*

(1) *Aus* $a \leq b$ *folgt* $a + c \leq b + c$

(2) *Aus* $a < b$ *folgt* $a + c < b + c$.

Beweis. (1) und (2) folgen direkt aus der Definition, (4.9) und (4.8). ∎

(4.14) Bemerkung. Nun können wir auch eine **Subtraktion** definieren. Für $a, b \in \mathbb{N}_0$ gelte $a \leq b$, dann existiert ein $k \in \mathbb{N}_0$ mit $a+k = b$. Wir setzen in diesem Fall $b-a := k$.

1.) Wegen der Kürzregel ist $b - a$ eindeutig bestimmt, falls es existiert.

2.) „$-$“ ist keine Verknüpfung auf $\mathbb{N}_0$. Eine entsprechende Abbildung ist nur auf einer Teilmenge von $\mathbb{N}_0 \times \mathbb{N}_0$ definiert (welche ist das?).

Die letzte Aussage dieses Abschnitts ist äquivalent zum Induktionsprinzip. Wir zeigen nur eine Richtung.

(4.15) Satz. *Jede nicht leere Menge natürlicher Zahlen besitzt ein Minimum.*

Beweis. Es sei $U := \{n \in \mathbb{N}\,;\, \forall m \in M : n \leq m\}$, die Menge der unteren Schranken von M in $\mathbb{N}$. Dann gilt $1 \in U$, denn $\forall n \in \mathbb{N} : 1 \leq n$. Weiter gilt $U \neq \mathbb{N}$, denn für alle $m \in M$ gilt $m + 1 > m$, also $m + 1 \notin U$.

Nach (P3) muss es also ein $k \in U$ geben mit $k + 1 \notin U$ (sonst würde $U = \mathbb{N}$ folgen).

Wir behaupten, dass $k = \min M$: Nach Konstruktion ist k untere Schranke. Wäre $k \notin M$, dann wäre $k + 1$ untere Schranke von M, also $k + 1 \in U$, ein Widerspruch. ∎

Eine direkte Folgerung ist

(4.16) *Jede beschränkte Menge natürlicher Zahlen besitzt ein Maximum.*

Zum Beweis betrachte man die Menge der oberen Schranken.

Exkurs. Wie Satz (4.15) klassische Induktionsbeweise *ersetzt* und verallgemeinert, sei durch ein Beispiel illustriert. Wir definieren die Mengen

$$G := \{n \in \mathbb{N}_0\,;\, \exists a \in \mathbb{N}_0 : n = a + a\} \quad \text{und} \quad U := \{n \in \mathbb{N}_0\,;\, \exists a \in \mathbb{N}_0 : n = a + a + 1\}$$

So gilt z.B. $0 \in G$ und $1 \in U$. Wir beweisen nun zwei Aussagen über G und U, die uns fast selbstverständlich erscheinen. Zur Abkürzung setzen wir $a \cdot 2 := a + a$.

Vorsicht. Wir kennen (noch) keine Rechenregeln für „$a \cdot 2$“.

(4.17) *$G \cap U = \varnothing$ und $G \cup U = \mathbb{N}_0$.*

Beweis. Mit dem Ziel, einen Widerspruch herbeizuführen, nehmen wir an, dass $M := G \cap U \neq \varnothing$. Dann existiert nach (4.15) $m := \min M$. Wegen $0 \notin U$, gilt $m \geq 1$. Wir können also $m-1 \in \mathbb{N}_0$ betrachten. Nach Voraussetzung gibt es $a, b \in \mathbb{N}_0$ mit $m = a \cdot 2$, $a \geq 1$, und $m = b \cdot 2 + 1$. Dann folgt einerseits $m-1 = a \cdot 2 - 1 = (a-1) + (a-1) + 1 \in U$; und andererseits $m - 1 = b \cdot 2 \in G$. Damit gilt $m - 1 \in G \cap U$, ein Widerspruch zur Minimalität von m.

Für die zweite Aussage sei $k \in \mathbb{N}_0$ der *kleinste Verbrecher*, d.h. es sei k minimal so, dass die Aussagen *nicht* gelten. Konkret: $k \notin G \cup U$. Erneut müssen wir einen Widerspruch herstellen.

Sicher gilt $k > 1$, daher können wir $k - 1 \in \mathbb{N}_0$ betrachten. Wegen der Minimalität von k gilt $k - 1 \in G \cup U$.

1. Fall: $k - 1 \in G$, d.h. $k - 1 = a \cdot 2$ mit $a \in \mathbb{N}_0$. Dann folgt $k = a \cdot 2 + 1 \in U$, ein Widerspruch.

2. Fall: $k - 1 \in U$, d.h. $k - 1 = b \cdot 2 + 1$ mit $b \in \mathbb{N}_0$. Dann folgt $k = b + b + 1 + 1 \in G$, ebenfalls ein Widerspruch.

Daher kann es keinen Verbrecher geben und die Aussage ist bewiesen. ∎

Bemerkung. Hinter der Formulierung „sei k der kleinste Verbrecher“ steckt (4.15): Wir betrachten die Menge M aller $n \in \mathbb{N}$, für die die Aussage falsch ist (die Menge aller Verbrecher). Wir müssen zeigen, dass $M = \varnothing$. Im Zuge eines Widerspruchbeweises nehmen wir $M \neq \varnothing$ an. Dann besitzt M ein Minimum k, eben den kleinsten Verbrecher. Daraus müssen wir den Widerspruch herleiten. Dieser besteht oft darin, dass die Aussage für k doch gilt, oder dass sie auch für ein $n_0 < k$ falsch ist.

Der Vorteil dieser Vorgehensweise besteht darin, dass man auf *alle* $\ell < k$ zurückgreifen kann und nicht nur auf $k - 1$. Für alle diese ℓ gilt ja nach Annahme die zu beweisende Aussage!

Wir werden später weitere Anwendungen dieser Vorgehensweise kennenlernen.

Übrigens, auch m aus dem ersten Teil des Beweises könnte man einen „kleinsten Verbrecher“ nennen.

Halbgruppen und Potenzen

Wir lösen uns nun für kurze Zeit von $\mathbb{N}_0$ und untersuchen abstrakt Strukturen mit assoziativen Verknüpfungen.

(4.18) Definition. Sei H eine Menge mit Verknüpfung $* : H \times H \to H$.

▷ Wir sagen $(H, *)$ oder $*$ sei **assoziativ**, wenn für alle $a, b, c \in H$ gilt $(a * b) * c = a * (b * c)$.

Dann nennt man $(H, *)$ eine **Halbgruppe**.

▷ Wir sagen, $e \in H$ sei ein **neutrales Element**, wenn für alle $a \in H$ gilt $a * e = e * a = a$.

▷ $(H, *)$ oder $*$ heißt **kommutativ**, wenn für alle $a, b \in H$ gilt $a * b = b * a$.

(4.19) Beispiele. 1.) Die Sätze (4.8) und (4.9) besagen: $(\mathbb{N}_0, +)$ ist eine kommutative Halbgruppe mit neutralem Element 0.

2.) Auch $(\mathbb{N}, +)$ ist eine kommutative Halbgruppe, besitzt aber kein neutrales Element. Was ist hier zu beweisen?

3.) Sei M eine Menge. $(\mathrm{Pot}(M), \cup)$ ist eine kommutative Halbgruppe mit neutralem Element $\varnothing$. Das ist der Inhalt von (1.7) (1), (2) und (4).

Was ist mit $(\mathrm{Pot}(M), \cap)$?

4.) Wir betrachten die Menge $\mathcal{F} := \{f : \mathbb{R} \to \mathbb{R}\,;\ f \text{ ist Abbildung}\}$. Dann ist $(\mathcal{F}, \circ)$ eine Halbgruppe mit neutralem Element $\mathrm{id}_{\mathbb{R}}$, die aber nicht kommutativ ist. Vgl. dazu (3.12), (3.13), und (3.11).

5.) „$-$“ ist nicht assoziativ. In $\mathbb{N}_0$ ist noch nicht einmal gesichert, dass $(a - b) - c$ existiert, wenn $a - (b - c)$ existiert.

6.) Für $m \in \mathbb{N}$ sind $(\mathbb{Z}_m, +_m)$ und $(\mathbb{Z}_m, \cdot_m)$ kommutative Halbgruppen mit neutralen Elementen $\overline{0}$, bzw. $\overline{1}$.

Begründung: Mit (1.28.4), der Assoziativität, und der Kommutativität von $(\mathbb{Z}, +)$ bzw. von $(\mathbb{Z}, \cdot\,)$ erkennt man, dass „$+_m$“ und „$\cdot_m$“ assoziativ und kommutativ sind. $\overline{0}$ bzw. $\overline{1}$ sind offenbar neutrale Elemente.

7.) Welche der folgenden Strukturen sind Halbgruppen und/oder haben ein neutrales Element: $(\mathbb{R}, +)$, $(\mathbb{R}, -)$, $(\mathbb{R}, \cdot\,)$, $(\mathbb{R}^*, \cdot\,)$, $(\mathbb{R}^+, +)$, $(\mathbb{R}^+, \cdot\,)$?

Neutrale Elemente sind, falls sie existieren, eindeutig.

(4.20) *In einer Halbgruppe $(H, *)$ kann es höchstens ein neutrales Element geben.*

Beweis. Wir nehmen an es gäbe zwei, nämlich e und e'. Nun gilt $e = e * e' = e'$. Dabei gilt das erste „$=$“, weil e' neutral ist; das zweite, weil e neutral ist. ∎

(4.21) Definition. In einer Halbgruppe $(H, *)$ mit neutralem Element e sei ein Element a fest gewählt. Dann setzt man rekursiv

$$a^0 := e \quad \text{und} \quad a^{n+1} := a^n * a \quad \text{für alle} \quad n \in \mathbb{N}_0.$$

Man nennt a^n die n-te **Potenz** von a in H. Es heißen a **Basis** und n **Exponent**.

(4.22) Beispiele. 1.) $(-2)^n = \ldots$ für $n \in \{0 \ldots 4\}$ (in der Halbgruppe $(\mathbb{R}, \cdot\,)$).

2.) Was ist a^1; was e^n in einer allgemeinen Halbgruppe?

3.) Was ergibt sich für die Verknüpfung „$+$“ auf $\mathbb{R}$; auf $\mathbb{N}_0$?

4.) Wir untersuchen die Potenzen in der Halbgruppe $(\mathrm{Pot}(M), \cup)$ in der Vorlesung.

Aus der Schule bekannt sind die

(4.23) Potenzrechengesetze. *Sei $(H, *)$ eine Halbgruppe mit neutralem Element e. Dann gilt für alle $a \in H$ und $n, m \in \mathbb{N}_0$*

(1) $a^{n+m} = a^n * a^m$

(2) *Sei H kommutativ und $b \in H$ so hat man $(a * b)^n = a^n * b^n$.*

Beweis. (1) mit Induktion nach m. Wegen $a^{n+0} = a^n = a^n * e = a^n * a^0$ gilt IA.

$m \rightsquigarrow m+1$: $a^{n+(m+1)} = a^{(n+m)+1} = a^{n+m} * a = (a^n * a^m) * a = a^n * (a^m * a) = a^n * a^{m+1}$.

(2) Übung! ∎

Die Multiplikation

Wir untersuchen die „Potenzen“ der Addition. Diese werden üblicherweise als **Vielfache** bezeichnet und mit „$\cdot$“ geschrieben. Definition (4.21) sieht dann so aus:

$$a \cdot 0 = 0 \quad \text{und} \quad a \cdot (n+1) := a \cdot n + a \quad \text{für } a, n \in \mathbb{N}_0.$$

Die resultierende Verknüpfung auf $\mathbb{N}_0$ wird **Multiplikation** genannt.

(4.24) Bemerkung. 1.) Wir benutzen (auch schon in der Definition) die bekannte Regel „Punkt vor Strich“, sonst müsste man $a \cdot (n+1) := (a \cdot n) + a$ schreiben.

2.) Man beachte, dass 0 in dieser Definition eine Doppelrolle spielt: Die erste Null ist einfach $0 \in \mathbb{N}_0$; die zweite Null ist das neutrale Element der Halbgruppe $(\mathbb{N}_0, +)$.

3.) Üblicherweise wird „n mal a“ als $a + a + \cdots + a$ (n-mal) gedeutet. Unsere Definition vertauscht die Rollen von a und n. Wir werden bald das Kommutativgesetz beweisen. Dann erledigt sich dieser Unterschied.

Wichtiger ist, dass unsere rekursive Definition den Begriff präzisiert, sodass man Beweise führen kann!

4.) Üblich ist auch statt $a \cdot b$ kurz ab zu schreiben.

Direkt aus (4.23) ergibt sich mit (4.19.1)

(4.25) Distributivgesetze. *Für alle $a, b, c \in \mathbb{N}_0$ gilt*

$$a \cdot (b+c) = a \cdot b + a \cdot c \quad \textit{und} \quad (a+b) \cdot c = a \cdot c + b \cdot c.$$ ∎

Wir ergänzen nun (4.23) durch

(4.26) Potenzrechengesetze (Ergänzung). *Sei $(H, *)$ eine Halbgruppe mit neutralem Element e. Dann gilt für alle $a \in H$ und $n, m \in \mathbb{N}_0$*

$$(a^n)^m = a^{n \cdot m}.$$

Beweis. Induktion nach m. IA ist klar.

$$m \rightsquigarrow m+1: \qquad (a^n)^{m+1} = (a^n)^m * a^n \overset{\text{IV}}{=} a^{n\cdot m} * a^m = a^{n\cdot m+n} = a^{n(m+1)}.$$ ∎

(4.27) Satz. $(\mathbb{N}_0, \cdot)$ *ist eine kommutative Halbgruppe mit neutralem Element* 1.

Außerdem gilt $\forall a, b \in \mathbb{N}_0 : ab = 0 \implies a = 0 \vee b = 0$.

Beweis. Das Assoziativgesetz ist genau (4.26) in anderer Schreibweise.

Für $a \in \mathbb{N}_0$ gilt $a \cdot 1 = a \cdot 0 + a = 0 + a = a$ mit (4.8) (vgl. auch (4.22)). Wir zeigen $1 \cdot a = a$ mit Induktion nach a.

IA ist trivial.

$a \rightsquigarrow a+1$: $1(a+1) = 1a + 1 \overset{\text{IV}}{=} a + 1$. Daher ist 1 neutrales Element.

Nun folgt mit (4.25) $(n+1)m = nm + 1 \cdot m = nm + m$ für alle $n, m \in \mathbb{N}_0$ und daraus mit Induktion die Kommutativität der Multiplikation. Die Details sind als Übung empfohlen!

Wir zeigen mit Induktion nach $b \in \mathbb{N}$: $a \neq 0 \implies ab \neq 0$ (Kontraposition!).

Der Induktionsanfang mit $b = 1$ ist trivial.

$b \rightsquigarrow b+1$: Es gilt $a(b+1) = ab + a = 0 \iff ab = a = 0$, also $a(b+1) \neq 0$. ∎

(4.28) Monotoniegesetz und Kürzregel für die Multiplikation. *Seien* $a, b, c \in \mathbb{N}_0$. *Dann gilt*

(1) *Aus* $a \leq b$ *folgt* $ac \leq bc$.

(2) *Aus* $a < b$ *und* $c \neq 0$ *folgt* $ac < bc$.

(3) *Aus* $ac = bc$ *und* $c \neq 0$ *folgt* $a = b$.

Beweis. (1) und (2): Es gibt ein $k \in \mathbb{N}_0$ mit $a + k = b$. Unter Anwendung von (4.25) rechnen wir $bc = (a+k) \cdot c = ac + kc$. Also gilt $ac \leq bc$.

(2) Hier gilt $k \neq 0$ also $kc \neq 0$ nach (4.27). Wegen (4.11) folgt $a \neq b$.

(3) folgt mit (4.12) direkt aus (2). ∎

Bemerkung. Für $c = 0$ gilt die Kürzregel (bekanntlich?) nicht. Warum?

Mehr noch als bei der Subtraktion, kann man eine Division auf $\mathbb{N}_0$ nur sehr eingeschränkt erklären. Dieses Thema wird im folgenden Kapitel 5 diskutiert, und in Kapitel 7 nochmals aufgegriffen.

Auch die Potenzbildung $(m, n) \mapsto m^n$ ist eine Verknüpfung auf $\mathbb{N}_0$. Sie hat aber keine „schönen“ Eigenschaften. Deshalb wurde und wird dieser Pfad nicht weiter verfolgt.

5 Stellenwertsysteme

In diesem kurzen Kapitel werden wir uns mit der üblichen Darstellung natürlicher Zahlen — dem Dezimalsystem — beschäftigen.

Grundlage ist die Division mit Rest, die wir zunächst auf die natürlichen Zahlen beschränken. Wir werden sie in einem späteren Kapitel auf die ganzen Zahlen ausdehnen und auch jetzt schon darauf hinweisen, wie das geht.

Der folgende Satz wird implizit bereits in der Grundschule angewandt. Er ist ein Behelf für die stark eingeschränkte Division auf $\mathbb{N}_0$. Seine Bedeutung geht aber weit darüber hinaus; er ist von fundamentaler Bedeutung für die Zahlentheorie. Insbesondere spielt er beim Beweis der Eindeutigkeit der Primfaktorzerlegung eine wichtige Rolle.

(5.1) Division mit Rest. *Zu $a \in \mathbb{N}_0$, $b \in \mathbb{N}$ gibt es immer eindeutig bestimmte Zahlen $q, r \in \mathbb{N}_0$ mit $0 \leq r < b$, so dass $a = q \cdot b + r$ gilt.*

Beweis. Existenz: Es sei $M := \{a - kb;\ k \in \mathbb{N}_0 \wedge kb \leq a\} \subseteq \mathbb{N}_0$.

Mit $k = 0$ erkennt man $a \in M$, also $M \neq \varnothing$. Nach (4.15) besitzt M ein kleinstes Element $r = a - qb \geq 0$. Angenommen $r \geq b$, dann gilt $0 \leq r - b = a - (q+1)b \in M$. Das steht im Widerspruch zur Wahl von r.

Eindeutigkeit: Es gelte auch $a = q'b + r'$ mit $q', r' \in \mathbb{N}_0$ und $0 \leq r' < b$. Ohne Einschränkung dürfen wir $r \leq r'$ annehmen (Trichotomie!). Dann folgt $0 \leq (q - q')b = r' - r < b$. Wäre nun $q \neq q'$, dann wäre $(q - q')b < b$ — ein Widerspruch. Das zeigt $q = q'$ und in der Folge auch $r' = r$. ∎

Man nennt q den **Quotienten** und r den **Rest**.

Beispiel. Wir wählen $a = 27,\ b = 12$. Es ist $27 = 2 \cdot 12 + 3$, d. h. $q = 2$ und $r = 3$. In einer Schreibweise, wie sie in manchen Schulen üblich ist $\quad 27 : 12 = 2$ Rest 3.

Mit einem Taschenrechner kann man wie folgt vorgehen:

Berechne $q := \left\lfloor \frac{a}{b} \right\rfloor$, und setze $r := a - q \cdot b$.

Im Beispiel ergibt sich $\frac{a}{b} = 2.25$, also $q = \lfloor 2.25 \rfloor = 2$ und $27 - 2 \cdot 12 = 3$.

Bemerkung. 1.) Die Berechnung der Reste bei der Division ist ein wichtiges Thema in der Grundschule. Dabei interessieren zwei Zahlen, wenn man a durch m dividiert: Zum einen die Zahl q ohne Berücksichtigung des Restes und dann der Rest $r \in \{0, 1, \ldots, m-1\}$ selbst. Insgesamt gilt $a = q \cdot m + r$. Wie die Schüler ein solches Ergebnis notieren sollen, ist umstritten: Eine Möglichkeit ist $a : m = q$ Rest r, wie eben angedeutet.

2.) In anderem Zusammenhang schreibt man auch $r = a \bmod m$. Dabei wird q nicht angegeben.

3.) Man kann die Division mit Rest leicht auf ganze Zahlen ausdehnen. Hier nur einige Zahlenbeispiele

$$-17 = (-3) \cdot 7 + 4 \qquad -27 = (-3) \cdot 12 + 9 \qquad -27 = 3 \cdot (-12) + 9$$

Wichtig ist, dass für die Reste nun gelten muss $0 \leq r < |b|$.

Die g-adische Darstellung natürlicher Zahlen

Wir alle sind mit dem Dezimalsystem aufgewachsen. Das ist eine Zahlendarstellung für jedes $a \in \mathbb{N}$ mit Hilfe von Zehnerpotenzen:

$$a = \sum_{i=0}^{n} a_i \cdot 10^i \quad \text{wobei die } a_i \in \{0, \ldots, 9\} \text{ „Ziffern“ sind.}$$

Beispiel. $a = 345 = 3 \cdot 10^2 + 4 \cdot 10 + 5 \cdot 10^0$. Hier ist $n = 2$.

Gerade weil es uns so selbstverständlich erscheint, müssen wir uns mit den mathematischen Hintergründen einer solchen Darstellung befassen. Dabei sind insbesondere Existenz und Eindeutigkeit zu klären.

Es zeigt sich, dass die Grundrechenarten im Dezimalsystem besonders einfach ausgeführt werden können. Das ist ein Grund dafür, dass man sie in der Grundschule überhaupt unterrichten kann.

In der Tat ist die Nutzung des Dezimalsystems keineswegs selbstverständlich. In früheren Kulturkreisen (Maya, Babylonier) wurden andere Zahlen statt 10 als Grundzahl von Rechnungen gewählt. Computer rechnen intern mit Zahlen, die aus Zweierpotenzen zusammengesetzt sind. Es gibt also gute Gründe, sich mit anderen Darstellungen zu befassen und zu klären, wie man Zahlen in andere Systeme umformen kann.

In den folgenden Aussagen bis zum Ende dieses Abschnitts steht $g \in \mathbb{N} \setminus \{1\}$ für die Grundzahl, die im Dezimalsystem die Zahl 10 ist.

Gegeben sei die Zahl $a \in \mathbb{N}$. Wir starten mit einer Divsion durch g. Danach existieren $q_0 \in \mathbb{N}_0$ und $a_0 \in \{0, \ldots, g-1\}$ mit $a = q_0 g + a_0$.

Ist $q_0 \neq 0$, so erhalten wir durch erneute Division: $q_0 = q_1 g + a_1$. Das führt auf die (eindeutige) Darstellung

$$a = q_0 g + a_0 = (q_1 g + a_1) g + a_0 = q_1 g^2 + a_1 g + a_0 = \ldots .$$

Wiederholt man dieses bis im n-ten Schritt $q_n = 0$, so erhält man

$$a = \sum_{i=0}^{n} a_i \cdot g^i \quad \text{mit } a_i \in \{0, \ldots, g-1\} \quad .$$

Offenbar gilt $q_n < \cdots < q_{i+1} < q_i < \cdots < q_1 < q_0 < a$. Daher bricht das Verfahren nach endlich vielen Schritten ab.

Bemerkung. Es gilt sogar $q_{i+1} \cdot g \leq q_i$. Hieraus kann man schließen, dass es ungefähr $\left\lfloor \log_g(a) \right\rfloor$ viele Schritte sind.

Beispiel. Sei $a = 123,\ g = 5$. Die eindeutig bestimmten Zahlen q_0 und a_0 sind 24 und 3. Man erhält

$$\begin{aligned} 123 &= 24 \cdot 5 + 3 \\ 24 &= 4 \cdot 5 + 4 \\ 4 &= 0 \cdot 5 + 4 \end{aligned}$$

Also $123 = 4 \cdot 5^2 + 4 \cdot 5 + 3$.

Wir haben einen Algorithmus beschrieben, wie man *jede* natürliche Zahl mit Hilfe von g-Potenzen eindeutig darstellen kann. Als Satz formuliert lauten unsere Erkenntnisse

(5.2) Satz. *Sei $a \in \mathbb{N}$ und $g \in \mathbb{N} \setminus \{1\}$. Dann existieren eindeutig bestimmte Zahlen $n \in \mathbb{N}_0, a_i \in \{0, \ldots, g-1\},\ a_n \neq 0,$ mit*

$$a = \sum_{i=0}^{n} a_i \cdot g^i.$$

Beweis. Die *Existenz* ergibt sich aus unserem Algorithmus.

Eindeutigkeit: Es sei $a \in \mathbb{N}$ der kleinste Verbrecher, sodass a zwei verschiedene Darstellungen besitzt:

$$a = \sum_{i=0}^{n} a_i \cdot g^i = \sum_{i=0}^{m} b_i \cdot g^i.$$

Division mit Rest ergibt $a = qg + r$. Andererseits erhalten wir

$$a = \sum_{i=1}^{n} a_i \cdot g^i + a_0 = \left(\sum_{i=1}^{n} a_i \cdot g^{i-1} \right) \cdot g + a_0 \stackrel{!}{=} \left(\sum_{i=1}^{m} b_i \cdot g^{i-1} \right) \cdot g + b_0.$$

Somit gilt nach (5.1) $q = \sum_{i=1}^{n} a_i \cdot g^{i-1} = \sum_{i=1}^{m} b_i \cdot g^{i-1} < a$ und $r = a_0 = b_0$.

Da q eine eindeutige Darstellung besitzt, folgt $n = m$ und $a_i = b_i$ für alle $i \in \{0, \ldots, n\}$. Dieser Widerspruch zur Annahme zeigt die Behauptung. ∎

Definition. Sei $g \in \mathbb{N} \setminus \{1\}$ und $z_i \in \{0, \ldots, g-1\}$. Dann heißt

$$(z_n z_{n-1} \ldots z_1 z_0)_g := \sum_{i=0}^{n} z_i \cdot g^i = a$$

die g–**adische Darstellung** der Zahl $a \in \mathbb{N}_0$. OE. kann man annehmen, dass $z_n \neq 0$, außer für $(0)_g := 0$.

Die Zahl g heißt **Grundzahl** oder **Basis**; die Zahlen z_i heißen **Ziffern** der Darstellung.

Im Fall $g = 2$ spricht man von der **Binärdarstellung**; im Fall $g = 10$ von der **Dezimaldarstellung**.

Allgemein spricht man auch von einem **Stellenwertsystem**[16], weil die „Stelle“ die „Wertigkeit“ (bezogen auf g) der entsprechenden Ziffer angibt.

Bemerkung. Der bekannte Mathematiker Adam Ries[17] (1492(?) – 1559) war maßgeblich daran beteiligt, das Dezimalsystem im deutschsprachigen Raum zu verbreiten. Bis zu dieser Zeit konnten nur Rechenmeister schwierigere Rechnungen durchführen. Heute werden diese Fertigkeiten in der Grundschule gelehrt.

Beispiel (Fortsetzung). $123 = (443)_5$.

Im Fall $g = 10$, also bei der gewohnten Dezimaldarstellung von Zahlen, verzichtet man auf die Wiedergabe des Index, etwa $(2019)_{10} = 2019$.

(5.3) Beispiele. 1.) 350 soll in eine 6-adische Zahl umgewandelt werden:

$$\begin{aligned}
350:6 &= 58 \text{ Rest } 2 &&\iff 350 = 58\cdot 6 + 2\\
58:6 &= 9 \text{ Rest } 4 &&\iff 58 = 9\cdot 6 + 4\\
9:6 &= 1 \text{ Rest } 3 &&\iff 9 = 1\cdot 6 + 3\\
1:6 &= 0 \text{ Rest } 1 &&\iff 1 = 0\cdot 6 + 1
\end{aligned}$$

$$\Longrightarrow \quad 350 = 58\cdot 6+2 = (9\cdot 6+4)\cdot 6+2 = \ldots = 1\cdot 6^3+3\cdot 6^2+4\cdot 6^1+2\cdot 6^0 = (1342)_6$$

2.) $a = 345 = 2\cdot 5^3 + 3\cdot 5^2 + 4\cdot 5^1 + 0\cdot 5^0 = (2340)_5$.

3.) $a = 100, \quad g = 2: \quad 100 = (?\ldots?)_2$

Die Umrechnung von g-adisch in dezimal ist einfacher.

Beispiel. $(123)_7 = 1\cdot 7^2 + 2\cdot 7 + 3 = 66 = (66)_{10} = (?\ldots?)_4$

Der entscheidende Vorteil von Stellenwertsystemen ist, dass man in ihnen relativ leicht addieren und multiplizieren kann. Die Methoden sind analog zu den bekannten für das Dezimalsystem.

Man kann also mit jeder Grundzahl g Arithmetik betreiben (Addition, Subtraktion, Multiplikation, Division, ...). Dies ist weniger schwierig als gewöhnungsbedürftig. Wir wollen uns hier auf ein Beispiel beschränken und verweisen für weitere Rechnungen auf die Übungen.

[16] `http://de.wikipedia.org/wiki/Stellenwertsystem`
[17] `https://de.wikipedia.org/wiki/Adam_Ries`

Beispiel. $(203)_4 \cdot (33)_4 = ??$ Wir rechnen schriftlich mit $g = 4$:

$$\begin{array}{cccccc} 2 & 0 & 3 & \cdot & 3 & 3 \\ \hline & 1 & 2 & 2 & 1 & \\ & & 1 & 2 & 2 & 1 \\ \hline & 2 & 0 & 0 & 3 & 1 \end{array}$$

Damit ist $(203)_4 \cdot (33)_4 = (20031)_4$

Wir hätten natürlich auch die gegebenen Zahlen in das Zehnersystem umrechnen, sie dort multiplizieren und dann das Ergebnis zurück in das Vierersystem übertragen können.

Für Grundzahlen $g > 10$ erfindet man zur eindeutigen Darstellung weitere Ziffern, zum Beispiel kann man für $g = 11$ (diese Grundzahl kommt bei ISBN im Buchhandel vor) die Menge der Ziffern $\{0, 1, \ldots, 9, X\}$ setzen. Statt X einfach 10 zu schreiben geht nicht, weil 10 im 11-er System schon eine andere Bedeutung hat (welche?).

Frage: Wie lautet $(230)_{11}$ im Zwölfersystem?

Bemerkung. Mit Hilfe der g-adischen Darstellung kann man auch leicht prüfen, ob $a \leq b$. Wie?

6 Die ganzen Zahlen

Wir haben im vorletzten Kapitel 4 gesehen, dass Gleichungen der Form $b + x = a$, $a, b \in \mathbb{N}_0$, nicht immer Lösungen in $\mathbb{N}_0$ haben. Um eine Lösung zu bekommen, müssten wir „Negative“, bzw. additive Inverse konstruieren. Dazu führen wir eine Erweiterung des Zahlbereichs $\mathbb{N}_0$ durch.

Genauer: wir wollen die Menge $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$ einführen. Dazu gibt es zwei Möglichkeiten:

Umbau, es wird eine neue Menge $\mathbb{Z}$ konstruiert, die die gewünschten Eigenschaften besitzt. Insbesondere wird eine Addition erklärt. Dann wird $\mathbb{N}_0$ „eingebettet“. Das bedeutet, dass wir einen Teil der Menge $\mathbb{Z}$ durch die Elemente aus $\mathbb{N}_0$ „ersetzen“. Dieser Zugang ist im Anhang zu diesem Kapitel ausgeführt. Er ähnelt der Konstruktion der rationalen Zahlen, die wir später noch durchführen werden.

Anbau, es werden zur bestehenden Menge $\mathbb{N}_0$ neue Elemente hinzugefügt; nämlich die negativen Zahlen. So wie es die obige Darstellung der Menge $\mathbb{Z}$ suggeriert.

Beide Zugänge haben Vor- und Nachteile. Der *Umbau* ist konzeptionell schwieriger, aber beweistechnisch einfacher. Beim *Anbau* sind die Beweise durch eine Vielzahl von Fallunterscheidungen geprägt. Auch wirkt die Definition z.B. der Addition sehr umständlich. Dafür muss man keine „Einbettung“ durchführen.

Wir werden hier den *Anbau* (nur teilweise) ausführen, und den *Umbau* in einem Anhang zeigen. Wir werden bei der Konstruktion der rationalen Zahlen sehen, dass man mit einem *Anbau* nicht immer durchkommt.

Um die Essenz unseres *Anbau*s bequem formulieren zu können, eine wichtige

(6.1) Definition. Es sei $(H, *)$ eine Halbgruppe mit neutralem Element e. Das Element $a \in H$ heißt **invertierbar**, wenn es ein $b \in H$ gibt mit $a * b = b * a = e$. Das Element b wird **inverses Element** zu a genannt.

Es gilt

(6.2) *Jedes Element einer Halbgruppe besitzt höchstes ein Inverses.*

Beweis. Es seien a_1 und a_2 Inverse von a, dann gilt

$$a_1 = a_1 * (a * a_2) = (a_1 * a) * a_2 = a_2. \qquad \blacksquare$$

(6.3) Beispiele. 1.) In jeder Halbgruppe mit neutralem Element e ist e invertierbar und zu sich selbst invers.

2.) In $(\mathbb{R}, +)$ ist jedes Element invertierbar nach (K3).

3.) In $(\mathbb{R}, \cdot)$ ist jedes Element außer 0 invertierbar nach (K3).

4.) In $(\mathbb{N}_0, +)$ besitzt einzig 0 ein Inverses; siehe (4.9.3).

5.) Eine Abbildung $f : A \to A$ ist invertierbar genau dann, wenn f bijektiv ist, also eine Umkehrabbildung besitzt. Diese ist zugleich die Inverse; siehe (3.17.2).

Konstruktion (Anbau)

Um die Lösbarkeit von Gleichungen der Form $b+x = a$ sicherzustellen, ergänzen wir die Menge $\mathbb{N}_0$ mit negativen Elementen, sprich additiven Inversen. Dass man damit so leicht durchkommt, ist eine Besonderheit der Halbgruppe $(\mathbb{N}_0, +)$ und keineswegs selbstverständlich. Siehe dazu auch unseren Versuch in (2.2.2), ein multiplikatives Inverses zu 0 zu definieren. Andere Komplikationen treten bei der Konstruktion von $\mathbb{Q}$ auf.

Definition. Zu jeder natürlichen Zahl $n \in \mathbb{N}$ definieren wir zunächst ein neues Symbol $-n$ (gesprochen: „*minus* n“). Es sei $-\mathbb{N} := \{-n\,;\ n \in \mathbb{N}\}$. Dann heißt

$$\mathbb{Z} := \mathbb{N}_0 \cup -\mathbb{N}$$

die **Menge der ganzen Zahlen**.

Wir erinnern an die Subtraktion für Elemente $a, b \in \mathbb{N}_0$ aus (4.14):

Falls $a \leq b$, so gibt es $k \in \mathbb{N}_0$ mit $a + k = b$ und $a - b := k$.

Definition. Auf der Menge $\mathbb{Z}$ definieren wir die Verknüpfung

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z};\ (a, b) \mapsto a + b$$

durch folgende Setzungen für $n, m \in \mathbb{N}_0$: Es sei $n + m$ die Summe von n und m wie in (4.7) erklärt. Weiter sei, unter Verwendung der Konvention $-0 = 0$

$$\begin{aligned} n + (-m) := (-m) + n &:= \begin{cases} n - m & \text{für } n \geq m \\ -(m - n) & \text{für } n < m \end{cases} \\ (-n) + (-m) &:= -(n + m) \end{aligned}$$

Wir nennen $+$ die **Addition** auf $\mathbb{Z}$.

Nun beginnt die mühevoll Arbeit. Vor allem um das Assoziativgesetz für „$+$“ nachzuweisen, sind sehr viele Fälle zu unterscheiden.

(6.4) Satz. *$(\mathbb{Z}, +)$ ist eine kommutative Halbgruppe mit neutralem Element 0.*

Beweis. Dass „$+$“ kommutativ und 0 neutral ist, folgt direkt aus der Definition.

Wir prüfen exemplarisch in einigen Fällen die Assoziativität für $a, b, c \in \mathbb{Z}$:

1. Fall $a, b, c \in \mathbb{N}_0$. Dann gilt die Behauptung nach (4.8).

2. Fall $a, b, c \in -\mathbb{N}$. Dann folgt die Behauptung sehr einfach ebenfalls mit (4.8).

3. Fall genau einer der drei Summanden ist in $-\mathbb{N}$.

Fall 3.1: $a, b \in \mathbb{N}_0$ und $c = -n \in -\mathbb{N}$.

Fall 3.1.1 $b \geq n$. Dann existiert $k \in \mathbb{N}_0$ mit $b = n + k$. Wir rechnen

$$\begin{aligned}(a+b)+(-n) &= (a+n+k)+(-n) = ((a+k)+n)-n = a+k \\ &= a+(b-n) = a+(b+(-n)).\end{aligned}$$

Hier gibt es noch einige weitere Unterfälle, die wir nicht vorführen wollen. So muss z.B. bei $b < n$ unterschieden werden ob $a \geq n - b$ oder nicht.

Fall 3.2: $a, c \in \mathbb{N}_0$ und $b = -n \in -\mathbb{N}$. Wir rechnen mit Hilfe des Kommutativgesetzes und Fall 3.1:

$$\begin{aligned}(a+(-n))+c &= c+(a+(-n))=(c+a)+(-n) = (a+c)+(-n) \\ &= a+(c+(-n)) = a+((-n)+c).\end{aligned}$$

Fall 3.3: $b, c \in \mathbb{N}_0$ und $a = -n \in -\mathbb{N}$. Geht ähnlich wie Fall 3.2.

4. Fall genau einer der drei Summanden ist in $\mathbb{N}_0$.

Hier kann man ähnlich wie in 3. Fall vorgehen, mit vielen Unterfällen. ∎

Man erkennt an der Definition von „+“, dass jedes Element $a \in \mathbb{Z}$ ein additives Inverses besitzt:

$$-a = \begin{cases} -n & \text{falls } a = n \in \mathbb{N} \\ 0 & \text{falls } a = 0 \\ n & \text{falls } a = -n \in -\mathbb{N} \end{cases} . \tag{1}$$

Wir nennen $-a$ das **Negative** (= additives Inverses) von $a \in \mathbb{Z}$.

Schließlich können wir eine **Subtraktion** auf $\mathbb{Z}$ definieren durch $a - b := a + (-b)$. Im Fall $a, b \in \mathbb{N}_0$ mit $a \geq b$ ergibt sich offenbar dasselbe wie in (4.14).

Gruppen

Wir haben gesehen, dass $(\mathbb{Z}, +)$ eine Halbgruppe mit neutralem Element ist, in der jedes Element ein Inverses besitzt. Eine solche Struktur heißt Gruppe. Ähnlich wie im Kapitel 4 verlassen wir nun $\mathbb{Z}$ für einen Moment und untersuchen Gruppen abstrakt.

(6.5) Definition. Eine Halbgruppe $(G, *)$ heißt **Gruppe**, wenn es ein neutrales Element gibt, und jedes Element ein Inverses besitzt. Das inverse Element zu $g \in G$ wird mit g^{-1} bezeichnet.

Wir haben bereits gesehen, dass das neutrale Element und das jeweilige Inverse zu einem Element eindeutig bestimmt sind. Das rechtfertigt insbesondere die Schreibweise g^{-1}.

Abweichend hiervon wird bei additiver Schreibweise — etwa bei $(\mathbb{R}, +)$ — die Inverse von g mit $-g$ bezeichnet.

Der Vollständigkeit halber seien diese Aussagen nochmals mit aufgeführt.

(6.6) *Sei $(G, *)$ eine Gruppe mit neutralem Element e. Dann gilt für alle $a, b \in G$:*

(1) *e ist das einzige neutrale Element in G.*

(2) *a besitzt genau ein inverses Element in G.*

(3) $(b^{-1})^{-1} = b$

(4) $(a * b)^{-1} = b^{-1} * a^{-1}$

Beweis. (1) und (2) stehen schon in (4.20) bzw. (6.2).

(3) $b * b^{-1} = b^{-1} * b = e \implies (b^{-1})^{-1} = b$ mit (2).

(4) $(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$ und entsprechend $(b^{-1} * a^{-1}) * (a * b) = e$. Wendet man (2) an, so folgt die Behauptung. ∎

Kommutative Gruppen werden auch **abelsch** genannt. Die Bezeichnung ehrt den norwegischen Mathematiker Niels Henrik Abel[18] (1802–1829).

(6.7) Beispiele. 1.) $(\{e\}, \cdot)$ mit $e \cdot e := e$ ist eine abelsche Gruppe.

2.) $(\mathbb{Z}, +)$ ist eine abelsche Gruppe nach (6.4) und Gleichung (1).

3.) Die Körperaxiome (K1) – (K4) bedeuten gerade, dass $(\mathbb{K}, +)$ für jeden Körper $\mathbb{K}$ eine abelsche Gruppe ist.

Auch $(\mathbb{K}^*, \cdot)$ ist eine abelsche Gruppe. Das folgt aus (K1) – (K4) mit (2.4.1). (0 ist ja nicht invertierbar, aber alle anderen Elemente!)

[18] `http://turnbull.mcs.st-and.ac.uk/~history/Mathematicians/Abel.html`

4.) $(\mathbb{R}^+, \cdot)$ ist ebenfalls eine Gruppe, nicht aber $(\mathbb{N}_0, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{R}, \cdot)$.

Welche Axiome sind verletzt?

5.) Die Halbgruppen $(\operatorname{Pot} M, \cup)$ und $(\operatorname{Pot} M, \cap)$ sind keine Gruppen. Warum?

6.) Für $n \in \mathbb{N}$ und $S_n := \{f : \{1, \ldots, n\} \to \{1, \ldots, n\}\,;\ f \text{ ist bijektiv}\}$ ist $(S_n, \circ)$ eine Gruppe, die **symmetrische Gruppe**.

Nach (3.18) ist $\circ$ eine Verknüpfung auf S_n; nach (3.12) gilt das Assoziativgesetz. Neutrales Element ist $\mathrm{id} \in S_n$ (vgl. (3.13)), und zu jedem $f \in S_n$ ist die Umkehrabbildung nach (3.17) das inverse Element.

7.) $(\mathbb{Z}_m, +_m)$ ist für jedes $m \in \mathbb{N} \setminus \{1\}$ eine kommutative Gruppe: Nach (4.19.6) ist $(\mathbb{Z}_m, +_m)$ assoziativ und kommutativ mit neutralem Element $\overline{0}$. Zu $\overline{a} \in \mathbb{Z}_m$ ist $\overline{-a}$ das inverse Element.

8.) Sei $\varnothing \neq U \subseteq G$ mit $a * b^{-1} \in U$ für alle $a, b \in U$, so ist U selbst Gruppe, genannt **Untergruppe** von G.

(a) $(\mathbb{Z}, +)$ und $(\mathbb{Q}, +)$ sind Untergruppen von $(\mathbb{R}, +)$.

(b) $(\mathbb{Q}^*, \cdot\,)$ und $(\mathbb{R}^+, \cdot\,)$ sind Untergruppen von $(\mathbb{R}^*, \cdot\,)$.

(c) S_3 ist Untergruppe von S_4.

(d) $\{e\}$ und G sind Untergruppen jeder Gruppe G. Man nennt sie die **trivialen Untergruppen**.

(6.8) Bemerkung. Beispiel (6.7.2) erlaubt eine kompakte Umformulierung der Körperaxiome:

$(\mathbb{K}, +, \cdot\,)$ ist ein **Körper**, wenn

(Kk 1) $(\mathbb{K}, +)$ eine kommutative Gruppe ist;

(Kk 2) $(\mathbb{K}^*, \cdot\,)$ eine kommutative Gruppe ist;

(Dg) das Distributivgesetz gilt.

Beachten Sie, dass wir im Vergleich zu Kapitel 2 die Axiome gewissermaßen „spaltenweise“ lesen! Siehe dazu auch (2.2.1).

Die nächste Aussage löst das Problem, mit dem wir in dieses Kapitel eingestiegen sind. Es ist eine Verallgemeinerung und Verschärfung der Kürzregel.

(6.9) Satz. *In jeder Gruppe $(G, *)$ gilt für alle $a, b \in G$*

(1) *Die Gleichungen*

$$a * x = b \quad \textit{und} \quad y * a = b$$

sind eindeutig nach x bzw. y lösbar.

Genauer: Die Lösungen sind $x = a^{-1} * b$ und $y = b * a^{-1}$.

(2) $\forall g \in G : a * g = b * g \implies a = b \quad \textit{und} \quad g * a = g * b \implies a = b$ ***(Kürzregel)***.

Beweis. (1) *Existenz:* Direktes Einsetzen verifiziert, dass die angegebenen Größen Lösungen sind.

Eindeutigkeit: Sei $s \in G$ irgendeine Lösung der ersten Gleichung. Dann gilt

$$a * s = b \implies a^{-1} * (a * s) = a^{-1} * b \implies (a^{-1} * a) * s = a^{-1} * b \implies s = a^{-1} * b.$$

Daher ist die angegebene Lösung auch die einzige. Der Beweis für die andere Gleichung läuft analog.

(2) a und b sind Lösung der Gleichung $y * g = a * g$, also $a = b$ wegen der Eindeutigkeit. Die andere Aussage zeigt man analog. ∎

(6.10) Bemerkung. 1.) Es gilt auch folgende Verschärfung von (1) des Satzes, die eine Umkehrung beinhaltet:

Eine Halbgruppe $(G, *)$ ist genau dann eine Gruppe, wenn die Gleichungen

$$a * x = b \quad \text{und} \quad y * a = b$$

für alle $a, b \in A$ eindeutig lösbar sind.

Es ist zunächst zu zeigen, dass es ein neutrales Element gibt. Dieser Beweisschritt hat ein Paar Feinheiten! Dabei ist das Assoziativgesetz essentiell, wie Beispiel (6.11) zeigt.

2.) Die Kürzregel ist uns schon in (2.3)(1),(2) begegnet. Jetzt haben wir sie für alle Gruppen verallgemeinert. Die Beweise sind übrigens nicht wesentlich anders.

3.) Der Satz löst unser Problem vom Anfang: Es seien $a, b \in \mathbb{Z}$, dann existiert genau eine $x \in \mathbb{Z}$ mit $a + x = b$, nämlich $x = -a + b \stackrel{!}{=} b - a$.

(6.11) Beispiel. Wir versehen $\mathbb{Q}$ mit der Verknüpfung $a \star b := \frac{a+b}{2}$. Man verifiziert leicht, dass die Aussagen aus (6.9) gelten. Aber

$$1 \star (1 \star 2) = \frac{5}{4} \quad \text{und} \quad (1 \star 1) \star 2 = \frac{3}{2}.$$

Daher ist $\star$ nicht assoziativ, und also $(\mathbb{Q}, \star)$ keine Gruppe. Gibt es ein neutrales Element?

Auf Gruppen kann man den Begriff der Potenz erweitern, indem man ganzzahlige Exponenten zulässt.

(6.12) Definition. Es sei $(G, *)$ eine Gruppe und $g \in G$. Wir setzen für alle $k \in \mathbb{Z}$

$$g^k := \begin{cases} g^k & \text{falls } k \in \mathbb{N}_0 \quad \text{(vgl. (4.21))} \\ (g^{-1})^n & \text{falls } k = -n \in -\mathbb{N} \end{cases}$$

Man nennt g^k die k-te **Potenz** von g in G. Wieder heißt g **Basis**; k **Exponent**.

Wir halten einige sehr einfache Beobachtungen fest.

(6.13) Bemerkung. 1.) Für alle $g \in G$ gilt $g^1 = g^0 * g = e * g = g$.

2.) Insbesondere ist die für das inverse Element benutzte Schreibweise g^{-1} kompatibel zur Potenzbildung mit dem Exponenten -1.

3.) $e^k = e$ für alle $k \in \mathbb{Z}$, denn auch $e^{-1} = e$.

Auch hier gelten die aus der Schule bekannten

(6.14) Potenzrechengesetze für Gruppen. *Sei $(G, *)$ eine Gruppe. Dann gilt für alle $g \in G$ und $k, \ell \in \mathbb{Z}$*

(1) $g^{k+\ell} = g^k * g^\ell$.

(2) $(g^k)^{-1} = g^{-k}$.

(3) *Sei G kommutativ und $h \in G$, so hat man* $(g * h)^k = g^k * h^k$

Beweis. (1) Der Fall $k = 0$ oder $\ell = 0$ ist trivial.

Im Fall $k, \ell \in \mathbb{N}$ oder $k, \ell \in -\mathbb{N}$ folgt die Behauptung mit (4.23.1); im zweiten Fall in Verbindung mit (6.6.4).

Wir betrachten nun den Fall $k \in \mathbb{N}$ und $\ell = -m$ mit $m \in \mathbb{N}$.

Es sei $m \in \mathbb{N}$ minimal so, dass es ein $k \in \mathbb{N}$ gibt, für das die Behauptung falsch wird. Auch k sei minimal mit dieser Bedingung gewählt. Möglich ist das alles wegen (4.15); m und k sind kleinste Verbrecher!

Nach (4.3) gibt es $m', k' \in \mathbb{N}_0$ mit $m' + 1 = m$ und $k' + 1 = k$. Wir rechnen

$$\begin{aligned} g^k * g^\ell &= g^k * (g^{-1})^m = g^{k'} * g * g^{-1} * (g^{-1})^{m'} = g^{k'} * e * (g^{-1})^{m'} \\ &= g^{k'} * (g^{-1})^{m'} \overset{(\star)}{=} g^{k'-m'} = g^{(k'+1)-(m'+1)} = g^{k+\ell}, \end{aligned}$$

im Widerspruch zur Wahl von k, m. Die Gleichung $(\star)$ gilt wegen der Minimalität von m und k, bzw. weil die Behauptung für alle kleineren Elemente aus $\mathbb{N}_0$ (!) richtig ist.

Der verbleibende Fall geht genauso.

(2) $g^{-k} * g^k = g^{-k+k} = g^0 = e$ und $g^k * g^{-k} = g^{k-k} = g^0 = e$. Mit (6.2) folgt die Behauptung!

(3) folgt im Fall $k \in \mathbb{N}_0$ sofort aus (4.23.2). Gilt $k = -m$ mit $m \in \mathbb{N}_0$, so gilt mit (6.6.4) und (4.23.2)

$$(g * h)^k = ((g * h)^{-1})^m = (h^{-1} * g^{-1})^m = (g^{-1} * h^{-1})^m = (g^{-1})^m * (h^{-1})^m = g^k * h^k.$$

■

Multiplikation

Wie schon bei $\mathbb{N}_0$ untersuchen wir die „Potenzen“ der Addition, diesmal für $(\mathbb{Z}, +)$, sodass auch negative „Exponenten“ zugelassen sind. Auch hier könnte man sie als **Vielfache** bezeichnet. Sie sie werden wie üblich mit „$\cdot$“ geschrieben. Definition (6.12) sieht dann so aus:

$$\text{Sei } a, k \in \mathbb{Z}, \text{ dann gilt} \quad a \cdot k := \begin{cases} a \cdot k & \text{für } k \in \mathbb{N}_0 \qquad (k \geq 0) \\ (-a) \cdot n & \text{für } k = -n \in -\mathbb{N} \quad (k < 0) \end{cases}$$

Die resultierende Verknüpfung auf $\mathbb{Z}$ wird ebenfalls **Multiplikation** genannt. Sie stimmt nach Konstruktion für Elemente aus $\mathbb{N}_0$ mit der Multiplikation auf $\mathbb{N}_0$ überein.

Wir ziehen zunächst einige nützliche Folgerungen.

(6.15) *Die Struktur $(\mathbb{Z}, +, \cdot)$ erfüllt folgende Rechenregeln für alle $a, b, c \in \mathbb{Z}$*

(1) $a \cdot (b + c) = a \cdot b + a \cdot c$ *und* $(a + b) \cdot c = a \cdot c + b \cdot c$ *(**Distributivgesetze**).*

(2) $0 \cdot a = a \cdot 0 = 0$.

(3) $a(-b) = (-a)b = -(ab)$.

Beweis. (1) ergibt sich mit (6.7.2) direkt aus (6.14).

(2) $a0 + 0 = a0 = a(0 + 0) = a0 + a0$, mit der Kürzregel für „$+$“ folgt $0 = a0$. Analog behandelt man $0a$; siehe auch (2.3.4) mit Beweis.

(3) $(-a)b + ab = (-a + a)b = 0b = 0$, also $(-a)b = -(ab)$; und analog für $a(-b)$. ■

Nun wird (6.14) ergänzt durch

(6.16) Potenzrechengesetze für Gruppen (Ergänzung). *Sei $(G, *)$ eine Gruppe. Dann gilt für alle $g \in G$ und $k, \ell \in \mathbb{Z}$*

$$(g^k)^\ell = g^{k \cdot \ell}.$$

Beweis. Z.B. $k = -n$, $\ell \in \mathbb{N}$: $(g^k)^\ell = ((g^{-1})^n)^\ell = (g^{-1})^{n\ell} = g^{-n\ell} = g^{k\ell}$. Hier wurde (6.15.3) benutzt! ■

Wir fassen nun alle wichtigen Eigenschaften der Multiplikation zusammen.

(6.17) Satz. $(\mathbb{Z}, \cdot)$ *ist eine kommutative Halbgruppe mit neutralem Element* 1. *Weiter gelten die Distributivgesetze und für alle* $a, b, c \in \mathbb{Z}$

(1) $ab = 0 \implies a = 0 \vee b = 0$*;*

(2) *aus* $ac = bc$ *und* $c \neq 0$ *folgt* $a = b$ ***(Kürzregel)****.*

Beweis. Das Assoziativgesetz ist genau (6.16) in anderer Schreibweise. Die Distributivgesetze stehen in (6.15.1)

Sei $a \in \mathbb{Z}$, dann gilt nach (6.13.1) $a \cdot 1 = a$. Im Fall $a \in \mathbb{N}_0$ folgt $1 \cdot a = a$ aus (4.27). Es bleibt der Fall $a = -n$ mit $n \in \mathbb{N}$. Mit (6.15.3) rechnet man

$$1 \cdot a = 1 \cdot (-n) = -(1 \cdot n) = -n = a.$$

Daher ist 1 neutrales Element.

Die Kommutativität von $(\mathbb{Z}, \cdot)$ lässt sich mit Hilfe von (6.15.3) aus der Kommutativität von $(\mathbb{N}_0, \cdot)$ herleiten. Wir führen den Fall $a \in \mathbb{N}_0$, $b = -m \in -\mathbb{N}$ exemplarisch vor:

$$a \cdot b = a \cdot (-m) = -(a \cdot m) \stackrel{!}{=} -(m \cdot a) = (-m) \cdot a = b \cdot a.$$

Die übrigen drei Fälle gehen ähnlich.

(1) Es gilt $n \cdot (-1) = 0 \iff -n = 0 \iff n = -0 = 0$. Nun kann man die Aussage auf die entsprechende aus (4.27) zurückführen.

(2) $ac = bc \iff (a - b)c = 0$ und mit (1) folgt $a - b = 0$ also $a = b$. ∎

Frage: Welches sind die invertierbaren Elemente von $(\mathbb{Z}, \cdot)$?

Ringe

Abermals abstrahieren wir Eigenschaften in diesem Fall der Strukturen $(\mathbb{Z}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ zu einem neuen Begriff. Dabei geht es im Kern um das Zusammenwirken zweier Verknüpfungen.

(6.18) Definition. Gegeben sei eine Menge R mit zwei Verknüpfungen „$+$“ und „$\cdot$“. Dann heißt $(R, +, \cdot)$ **Ring**, wenn gilt

(R1) $(R, +)$ ist eine kommutative Gruppe;

(R2) $(R, \cdot)$ ist eine Halbgruppe mit neutralem Element $1 \neq 0$;

(Dg) Für alle $a, b, c \in R$ gelten die **Distributivgesetze**

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{und} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Das neutrale Element der Addition wird meist 0 geschrieben und auch **Nullelement** genannt. 1 heißt auch **Einselement**. Ein Ring heißt **kommutativ**, wenn „$\cdot$“ kommutativ ist.

Es sei angemerkt, dass es tatsächlich Ringe gibt, bei denen „$\cdot$“ nicht kommutativ ist. Daher muss man bei (Dg) beide Distributivgesetze verlangen!

(6.19) Beispiele. 1.) $(\mathbb{Z}, +, \cdot)$ ist nach den Erkenntnissen von oben ein kommutativer Ring.

2.) Jeder Körper $(\mathbb{K}, +, \cdot)$ ist nach den Körperaxiomen aus Kapitel 2 ein kommutativer Ring.

3.) Insbesondere erfüllt $(\mathbb{R}, +, \cdot)$ die obigen Axiome, ist also auch ein Ring.

4.) $(\mathbb{N}_0, +, \cdot)$ ist kein Ring (warum?).

5.) Die Menge $\mathbb{R}[x]$ aller Polynome mit Koeffizienten aus $\mathbb{R}$ bilden mit der üblichen Addition und Multiplikation von Polynomen einen Ring, aber keinen Körper (warum?).

6.) Für jedes $m \in \mathbb{N} \setminus \{1\}$ ist $(\mathbb{Z}_m, +_m, \cdot_m)$ ein kommutativer Ring. (R1) gilt nach (6.7.7); (R2) und (Dg) zeigt man ganz ähnlich (vgl. auch Aufg. 21(c)).

Was ist mit $m = 1$?

7.) Was ist mit $(\operatorname{Pot} M, \cup, \cap)$ für eine Menge M?

8.) Die Menge der 2×2-Matrizen $\mathbb{R}^{2\times 2}$ über $\mathbb{R}$ bildet mit der üblichen Addition und der Matrizenmultiplikation einen Ring, der nicht kommutativ ist.

Wir ziehen einige weitere Folgerungen aus den Ringaxiomen, die Ihnen für $\mathbb{R}$ und $\mathbb{Z}$ bereits vertraut sind. Die Beweise wiederholen sich!

(6.20) *Sei R ein Ring und $a \in R$ beliebig. Dann gilt*

(1) $0 \cdot a = 0 = a \cdot 0$*;*

(2) $a(-b) = (-a)b = -ab$

(3) $(-a) \cdot (-b) = ab$*.*

Beweis. (1) Es gilt $0a = (0+0)a = 0a+0a$, mit der Kürzregel (6.9.2) (für die Addition!) folgt $0a = 0$. Die andere Gleichung ergibt sich analog aus dem anderen Distributivgesetz.

(2) $ab + (-a)b = (a + (-a))b = 0 \cdot b = 0 \implies (-a)b = -ab$; mit (1) und (6.6.2). Und analog für $a \cdot (-b) = -ab$ (siehe auch den Beweis zu (2.3.5).

(3) Mit (2) gilt $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-ab) = ab$.; vgl (6.6.3). ∎

Die (wohlbekannte) Aussage $0a = 0$ besagt, dass 0 in keinem Ring R eine multiplikative Inverse besitzen kann. Andernfalls würde der Widerspruch $1 = 0$ folgen; genau wie in (2.2.2) ausgeführt.

Andererseits kann $(R\setminus\{0\}, \cdot)$ sehr wohl eine Gruppe sein, etwa in den Fällen: $\mathbb{Q}$ oder $\mathbb{R}$. Allgemeiner: $(R \setminus \{0\}, \cdot)$ ist genau dann eine Gruppe, wenn R ein Körper ist. Es hat dann jedes Element ungleich 0 ein multiplikatives Inverses.

Vergleichen Sie die Axiome (R1), (R2) und (Dg) nochmals mit denen aus (6.8), und machen Sie sich die — wenigen — Unterschiede klar!

Anordnung

Statt die Anordnung von $\mathbb{N}_0$ auf $\mathbb{Z}$ zu übertragen, analog zum Vorgehen bei der Addition, werden wir die Anordnung neu definieren; und zeigen, dass diese Definition mit der alten auf $\mathbb{N}_0$ übereinstimmt.

Wir gehen genauso vor wie in Kapitel 2 für Körper. Wir definieren

$$a < b :\iff b - a \in \mathbb{N}$$

In der Tat erfüllt $\mathbb{N}$ die Axiome (A1) und (A2) für angeordnete Körper:

- ▷ Für alle $a \in \mathbb{Z} \setminus \{0\}$ gilt $a \in \mathbb{N}$ oder $-a \in \mathbb{N}$, aber nicht beides; das ist (A1).
- ▷ Außerdem sind $(\mathbb{N}, +)$ und $(\mathbb{N}, \cdot\,)$ abgeschlossen und das ist genau (A2).

$\mathbb{N}$ übernimmt also die Rolle von $\mathbb{K}^+$.

Wie üblich seien auch wieder $\leq$, $>$ und $\geq$ erklärt.

(6.21) Satz. *Auf $(\mathbb{Z}, +, \cdot, <)$ gilt für alle $a, b, c \in \mathbb{Z}$*

(1) *genau eine Aussage $a < b \ \vee\ a = b \ \vee\ b < a$ (**Trichotomie**).*

(2) $a < b \ \wedge\ b < c \implies a < c$ *(**Transitivität**).*

(3) $a \leq b \ \wedge\ b \leq a \implies a = b$ *(**Antisymmetrie**).*

(4) *Die Relation $<$ stimmt für Elemente aus $\mathbb{N}_0$ mit der in (4.12) definierten Relation überein.*

Beweis. (1) Es gilt $b - a \in \mathbb{N} \ \vee\ b - a = 0 \ \vee\ b - a \in -\mathbb{N}$. Das führt direkt auf die drei Fälle im Satz.

(2) Nach Voraussetzung gilt $b - a \in \mathbb{N}$ und $c - b \in \mathbb{N}$. Es folgt

$$c - a = b - a + c - b \in \mathbb{N}, \quad \text{also} \quad a < c.$$

(3) folgt direkt aus (1).

(4) Es gilt $n < m \iff \exists k \in \mathbb{N} : n + k = m \iff m - n = k \in \mathbb{N}$. ∎

Auch die Monotoniegesetze lassen sich erweitern.

(6.22) Monotoniegesetze. *Seien $a, b, c \in \mathbb{Z}$. Dann gilt*

(1) *Aus $a < b$ folgt $a + c < b + c$.*

(2) *Aus $a < b$ und $c > 0$ folgt $ac < bc$.*

(3) *Aus $a < b$ und $c < 0$ folgt $ac > bc$.*

Beweis. (1) direkt aus der Definition.

(2) $a < b \iff b - a \in \mathbb{N} \implies bc - ac = (b - a)c \in \mathbb{N} \implies ac < bc$.

(3) Es gilt mit (6.15) $ac - bc = (a - b)c = (a - b)(-1)(-c) = (b - a)(-c) \in \mathbb{N}$, denn $b - a$ und $-c$ sind in $\mathbb{N}$. Also $-bc + ac > 0 \implies ac > bc$. ∎

Wie im Kapitel 2 lässt sich der Absolutbetrag einer ganzen Zahl definieren.

Definition. $|a| := \begin{cases} a & \text{falls} \quad a \geq 0 \\ -a & \text{falls} \quad a < 0 \end{cases}$ heißt der **(Absolut-)Betrag** von a.

Die Eigenschaften (und auch die Beweise) können wörtlich aus Kapitel 2 übernommen und brauchen hier nicht wiederholt zu werden.

Anhang: Konstruktion der ganzen Zahlen (Umbau)

Da Gleichungen der Form $b + x = a,\ a, b \in \mathbb{N}_0$, nicht immer Lösungen in $\mathbb{N}_0$ haben erweitern wir den Zahlbereich $\mathbb{N}_0$. Wir zeigen hier, wie der *Umbau* funktioniert. Die Idee ist einfach: Jeder Gleichung wird die „Lösung“ (a, b) zugeordnet.

Dadurch ergeben sich sofort zwei neue Probleme.

▷ Es gibt viele Gleichungen, die dieselbe Lösung besitzen.

▷ Man muss eine evtl. schon vorhandene Lösung mit den neuen Lösungen *identifizieren.*

Wie sehen alle Paare (a, b) aus, die dieselbe Lösung darstellen? Um diese Frage zu beantworten, nehmen wir zunächst an, es gäbe schon *eine* Lösung x der beiden Gleichungen $b + x = a$ und $b' + x = a'$. Nun wird x eliminiert: Wir addieren die beiden Gleichungen und *kürzen* x mit Hilfe von (4.11)

$$a + b' + x = b + x + a' \iff a + b' = b + a'.$$

Diese heuristischen Überlegungen nehmen wir zum Anlass für eine Behauptung, die eine Konstruktion ermöglicht.

(6.23) *Durch* $(a,b) \sim (a',b') :\iff a+b' = b+a'$ *wird eine Äquivalenzrelation auf* $\mathbb{N}_0 \times \mathbb{N}_0$ *definiert.*

Beweis. Übung. ∎

Nun können wir eine geeignete Menge zu definieren.

Definition. Der Quotientenraum $\mathbb{Z} := \mathbb{N}_0 \times \mathbb{N}_0 / \sim$ heißt **Menge der ganzen Zahlen**.

Für die Äquivalenzklasse von (a,b) schreiben wir zunächst $[(a,b)]$. Wir werden bald zur geläufigen Schreibweise übergehen.

(6.24) *Durch* $[(a,b)] \oplus [(c,d)] := [(a+c, b+d)]$ *wird eine Verknüpfung* $\oplus : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *definiert.*

Es ist $(\mathbb{Z}, \oplus)$ *eine kommutative Gruppe mit neutralem Elenemt* $[(0,0)]$.

Beweis. Wir müssen zeigen, dass $\oplus$ **wohldefiniert** ist. D.h. wenn wir $[(a,b)] = [(a',b')]$ und $[(c,d)] = [(c',d')]$ haben, dann muss auch $[(a+c, b+d)] = [(a'+c', b'+d')]$ gelten. Sonst wäre $\oplus$ keine Abbildung.

Es gilt $[(a,b)] = [(a',b')]$ und $[(c,d)] = [(c',d')]$ nach Voraussetzung, also $(a,b) \sim (a',b')$ und $(c,d) \sim (c',d')$. Das bedeutet $a+b' = a'+b$ und $c+d' = c'+d$. Nun folgt sofort $a+c+b'+d' = a'+b+c'+d$, und damit $(a+c, b+d) \sim (a'+c', b'+d')$.

Der Rest ist einfach: Alle Rechenregeln folgen direkt aus den entsprechenden Regeln für $\mathbb{N}_0$. Wir zeigen exemparisch das Kommutativgesetz.

$$[(a,b)] \oplus [(c,d)] = [(a+c, b+d)] = [(c+a, d+b)] = [(c,d)] \oplus [(a,b)].$$

Schließlich besitzt jedes Element von $(\mathbb{Z}, \oplus)$ ein Inverses. In der Tat, ist $[(a,b)] \in \mathbb{Z}$ gegeben, dann gilt

$$[(a,b)] \oplus [(b,a)] = [(a+b, b+a)] = [(0,0)].$$

∎

Was hat das alles mit $(\mathbb{N}_0, +)$ zu tun? Wenn wir nochmals an die heuristischen Überlegungen vom Anfang denken, dann müsste $[(a,0)]$ zur Zahl $a \in \mathbb{N}_0$ korrespondieren. In der Tat funktioniert auch die Addition in beiden Darstellungen gleich. Es gilt nämlich $[(a,0)] \oplus [(b,0)] = [(a+b, 0)]$. Der Unterschied liegt also nur in der Darstellungsform, nicht in ihren wesentlichen Eigenschaften.

(6.25) Bemerkung. Mit der Teilmenge $\mathcal{N} := \big\{ [(a,0)] \,;\, a \in \mathbb{N}_0 \big\}$ von $\mathbb{Z}$ gilt genauer: $(\mathcal{N}, \oplus)$ ist eine kommutative Halbgruppe mit neutralem Element, die sich in allen Belangen wie $(\mathbb{N}_0, +)$ verhält.

Diesen Sachverhalt nehmen wir zum Anlass für eine

(6.26) Definition. Es seien zwei Halbgruppen $(H, *)$ und $(G, \star)$ gegeben. Eine Abbildung $\sigma : H \to G$ heißt **Homomorphismus**, wenn

$$\text{für alle } a, b \in H \text{ gilt} \quad \sigma(a * b) = \sigma(a) \star \sigma(b).$$

Ein bijektiver Homomorphismus heißt **Isomorphismus**. Wenn es einen Isomorphismus $\sigma : H \to G$ gibt, dann heißen die Halbgruppen **isomorph**.

Mit diesem neuen Begriff können wir unsere Überlegungen von oben formal präzise fassen.

(6.27) $\iota : (\mathbb{N}_0, +) \to (\mathbb{Z}, \oplus);\ a \mapsto [(a, 0)]$ *ist ein injektiver Homomorphismus.*

$(\mathbb{N}_0, +)$ *und* $(\iota(\mathbb{N}_0), \oplus)$ *sind isomorphe Halbgruppen. Dabei gilt* $\iota(\mathbb{N}_0) = \mathcal{N}$*.*

Beweis. Es seien $a, b \in \mathbb{N}_0$, dann gilt

$$\iota(a + b) = [(a + b, 0)] = [(a, 0)] \oplus [(b, 0)] = \iota(a) \oplus \iota(b).$$

Somit ist ι ein Homomorphismus. Falls $\iota(a) = \iota(b)$, dann gilt $[(a, 0)] = [(b, 0)]$, also $(a, 0) \sim (b, 0)$. Daraus folgt $a = a + 0 = 0 + b = b$; und ι ist injektiv.

Die letzte Aussage ist klar. ∎

Die letzte Aussage des Satzes stellt eine Neuformulierung von (6.25) dar:

$(\mathbb{N}_0, +)$ und $(\mathcal{N}, \oplus)$ sind isomorph.

Bemerkung (zur Vorsicht). Über Anordnung und Multiplikation ist an dieser Stelle noch nichts gesagt. Das geht — nach einigen Vorbereitungen — genauso wie es weiter oben beschrieben wurde.

Das zu jedem Element $[(a, b)]$ existierende — nach (6.2) eindeutig bestimmte — Inverse wird (wie üblich) mit $-[(a, b)]$ bezeichnet und das **Negative** von $[(a, b)]$ genannt.

Nun können wir uns von der schwerfälligen Notation lösen. Zunächst kürzen wir die Elemente $[(n, 0)]$ einfach durch $n \in \mathbb{N}_0$ ab. Nach (6.27) funktioniert die Addition dieser Elemente wie in $\mathbb{Z}$.

Was ist mit den anderen Elementen $[(a, b)]$?

Im Fall $a \geq b$ gilt $[(a, b)] = [(a - b, 0)] = [(n, 0)] = n \in \mathbb{N}_0$.

Im Fall $a < b$ gilt $[(a, b)] = -[(b, a)] = -[(b - a, 0)] = -[(m, 0)] = -m$, mit $m \in \mathbb{N}$.

Insgesamt ergibt sich die gewohnte Darstellung ganzer Zahlen als $n \in \mathbb{N}_0$ oder $-m$ mit $m \in \mathbb{N}$. Es gilt genauer

(6.28) *Für jedes Element* $z \in \mathbb{Z}$ *gilt genau eine von drei Bedingungen* $z = 0$, $z \in \mathbb{N}$ *oder es gibt* $m \in \mathbb{N}$ *mit* $z = -m$. *Insbesondere gilt* $z = -z \iff z = 0$.

Anders ausgedrückt: $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}$.

Beweis. Wir zeigen zunächst $z = -z \implies z = 0$. Man beachte, dass „$\Longleftarrow$“ trivial ist.

Es sei $z = [(a, b)]$. Dann ist zu zeigen: $(a, b) \sim (b, a) \implies a = b$.

Angenommen, das wäre falsch. Nach (4.12) dürfen wir o.E. annehmen, dass $a > b$. Nun gilt nach (4.13.2)

$$a + a > a + b > b + b \implies a + a \neq b + b \implies (a, b) \not\sim (b, a),$$

ein Widerspruch.

Mit den Vorüberlegungen folgt jetzt direkt die Behauptung. ∎

Bemerkung. $\mathbb{N}_0$ ist in $\mathbb{Z}$ „eingebettet“. D.h., die Elemente von $\mathbb{N}_0$ werden als Elemente von $\mathbb{Z}$ aufgefasst (neue Schreibweise!). Insbesondere gilt $\mathbb{N}_0 \subseteq \mathbb{Z}$.

Für die Addition dürfen wir wegen (6.27) die übliche Bezeichnung $a + b$ statt $a \oplus b$ für $a, b \in \mathbb{Z}$ benutzen, weil für $a, b \in \mathbb{N}_0$ stets dasselbe herauskommt.

Man überlegt sich schnell, dass die oben gewonnene Addition mit der auf Seite 63 übereinstimmt. Ab dieser Stelle kann man mit dem Abschnitt über Gruppen auf Seite 65 weitermachen, um auch die Multiplikation und die Anordnung zu behandeln.

7 Grundbegriffe der Zahlentheorie

In diesem Abschnitt werden wir einige wichtige Begriffe aus der Theorie der ganzen Zahlen untersuchen. Es wird um Primzahlen, Kongruenzen und den Euklidischen Algorithmus gehen.

Wie angekündigt kommt hier die Verallgemeinerung von (5.1). Der Beweis ergibt sich mit einigen Fallunterscheidungen leicht aus (5.1).

(7.1) Division mit Rest (allgemeine Version). *Zu $a, b \in \mathbb{Z},\ b \neq 0$ gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit $0 \leq r < |b|$, so dass $a = q \cdot b + r$ gilt.* ∎

Wie gehabt, nennt man q den **Quotienten** und r den **Rest**.

Primzahlen

Auf S. 12 in Kapitel 1 wurde die Relation $a|b$, „a ist ein Teiler von b“ auf der Menge $\mathbb{Z}$ eingeführt. Bei der Division von b durch a ist der Rest dann 0.

Jede ganze Zahl a besitzt die sogenannten **trivialen Teiler**, das sind $1, -1, a$ und $-a$.

Definition. Eine natürliche Zahl $n \geq 2$ heißt **Primzahl**, wenn n nur die trivialen Teiler $1, -1, n$ und $-n$ besitzt. Die Menge der Primzahlen sei mit $\mathbb{P}$ bezeichnet.

Ist $n \in \mathbb{Z}$ und $p \in \mathbb{P}$ mit $p|n$, so heißt p ein **Primteiler** von n.

(7.2) *Jede natürliche Zahl $n \geq 2$ besitzt mindestens einen Primteiler.*

Genauer: Der kleinste Teiler $t \geq 2$ von n ist immer eine Primzahl.

Beweis. Nach (4.15) existiert ein kleinster Teiler $t \geq 2$ von n, denn die Menge aller solcher Teiler enthält n, ist also nicht leer.

Wäre t keine Primzahl, so gäbe es $u \in \mathbb{N} \setminus \{1, t\}$ mit $u|t$, einen nicht trivialen Teiler von t. Insbesondere gilt $2 \leq u < t$. Mit (1.26.2) folgt aber $u|n$; im Widerspruch zur Minimalität von t. ∎

Die ersten zwölf Primzahlen sind 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, eine etwas größere Primzahl ist 845 100 400 152 152 934 331 135 470 251.

Wieviele Primzahlen gibt es insgesamt? Der älteste bekannte Beweis stammt von EUKLID ($\sim$325 – $\sim$265 v. Chr.)

(7.3) Satz (*Euklid*). *Es gibt unendlich viele Primzahlen.*

Beweis. Wir nehmen an, es gibt nur endlich viele Primzahlen $p_1, p_2, \ldots, p_n$, und führen dies zum Widerspruch. Sei $a = p_1 \cdot p_2 \cdot \cdots \cdot p_n$. Die Zahl $a + 1$ hat nach (7.2) einen Primteiler p. Da $p_1, p_2, \ldots, p_n$ nach unserer Annahme die einzigen Primzahlen sind, muss $p = p_i$ für ein i gelten, d. h. $p_i \mid a + 1$. Wegen $a = p_1 \cdot p_2 \cdot \cdots \cdot p_n$ gilt $p_i \mid a$. Es ist aber unmöglich, dass p_i sowohl $a+1$ als auch a teilt. (Z.B. müsste p_i ein Teiler von $a + 1 - a = 1$ sein!) Damit haben wir aus unserer Annahme, es gebe nur endlich viele Primzahlen, einen Widerspruch hergeleitet. ∎

Leider ist dies ein reiner *Existenzbeweis*: Wir wissen zwar, dass es unendlich viele Primzahlen gibt, Satz und Beweis helfen aber nicht weiter, wenn wir eine konkrete Primzahl suchen. Primzahlen gehören zu den willkürlichsten Objekten in der Mathematik. So schreibt der bekannte Mathematiker D. Zagier: „Sie wachsen wie Unkraut unter den natürlichen Zahlen, scheinbar keinem anderen Gesetz als dem Zufall unterworfen, und kein Mensch kann voraussagen, wo wieder eine sprießen wird, noch einer Zahl ansehen, ob sie prim ist oder nicht“. [Zag77, S. 42]

Vor dem Einsatz elektronischer Rechenanlagen vor fast 70 Jahren war die größte bekannte Primzahl $2^{127} - 1$, bestehend aus 39 Ziffern, gefunden im Jahr 1876. Erst 75 Jahre später wurde sie übertroffen (nämlich 1952 mit den Zahlen $2^{521} - 1$, $2^{607} - 1$ und einige Monate später noch Weiteren). Der letzte Rekord wurde im Dezember 2018 aufgestellt. Demnach ist die größte bekannte Primzahl $2^{82\,589\,933} - 1$. Sie wurde im Rahmen des GIMPS-Projekts[19] zur Suche neuer Mersennescher Primzahlen entdeckt und besteht aus 24 862 048 Ziffern.

(7.4) Bemerkung. 1.) Der Exponent 82 589 933 ist selbst eine Primzahl.

2.) Primzahlen der Gestalt $2^p - 1$ heißen **Mersennesche Primzahlen** (benannt nach Marin Mersenne,[20] 1588–1648). Für $p = 2, 3, 5$ erhält man so die Primzahlen $3, 7, 31$. — *Frage*: Was ist für $p = 7, 11$?

3.) Ist $n \geq 2$ keine Primzahl, so ist $2^n - 1$ niemals eine Primzahl. In der Tat zeigt die geometrische Summenformel, dass die Zahl $2^d - 1$ im Fall $d|n$ ein Teiler von $2^n - 1$ ist.

4.) Siehe auch Wikipedia über Mersenne-Zahlen.

`http://de.wikipedia.org/wiki/Mersenne-Zahl`

5.) In ähnlicher Weise zeigt man, dass $a^n - 1$ für $a > 2$, $n \geq 2$, niemals eine Primzahl sein kann (auch wenn n eine Primzahl ist!).

Der folgende Satz über die Primfaktorzerlegung ist ebenfalls grundlegend für die Zahlentheorie. Wir beweisen hier nur die Existenz.

[19] `http://www.mersenne.org/`
[20] `http://de.wikipedia.org/wiki/Marin_Mersenne`

(7.5) Satz. *Jede natürliche Zahl $n \geq 2$ ist bis auf die Reihenfolge der Faktoren eindeutig als Produkt von Primzahlen darstellbar:*

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_m \qquad (m \geq 1).$$

Beweis. Existenz: Es sei $n \in \mathbb{N} \setminus \{1\}$ der kleinste Verbrecher, also die kleinste Zahl ≥ 2 die keine Primfaktorzerlegung besitzt. Dann ist n keine Primzahl! Also gibt es eine Zerlegung $n = a \cdot b$ mit $a, b \in \mathbb{N} \setminus \{1\}$. Wegen $a, b < n$ besitzen sie beide eine Primfaktorzerlegung: $a = p_1 \cdot p_2 \cdot \dots \cdot p_k$ und $b = q_1 \cdot q_2 \cdot \dots \cdot q_\ell$. Dann ist aber

$$n = ab = p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot q_1 \cdot q_2 \cdot \dots \cdot q_\ell$$

eine Primfaktorzerlegung von n, im Widerspruch zur Annahme.

Die *Eindeutigkeit* wird in den meisten Büchern zur elementaren Zahlentheorie ausgeführt; z.B. [Pad08, IV.3]. ∎

(7.6) Bemerkung. 1.) Die Primfaktoren $p_1, p_2, \dots, p_m$ sind in der Regel nicht alle verschieden.

2.) Mit dem Satz ist nochmals gezeigt, dass jede natürliche Zahl $n \geq 2$ mindestens einen Primteiler besitzt.

3.) Die Eindeutigkeit ist etwas schwieriger zu beweisen und soll hier nicht ausgeführt werden. Wichtigstes Hilfsmittel ist der Satz

$$p|ab \implies p|a \vee p|b \quad \text{für } p \in \mathbb{P} \text{ und } a, b \in \mathbb{Z}.$$

Beispiel. $6600 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11, \quad 126 = 2 \cdot 3 \cdot 3 \cdot 7$

Zur besseren Übersicht fasst man gleiche Faktoren zusammen:

$6600 = 2^3 \cdot 3 \cdot 5^2 \cdot 11, \quad 126 = 2 \cdot 3^2 \cdot 7.$

Das Ergebnis von Satz (7.5) lautet dann:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_s^{\alpha_s}.$$

Hierbei sind die p_i *verschiedene* Primzahlen und $\alpha_1, \dots, \alpha_s \in \mathbb{N}$.

Rechnen mit Kongruenzen

Wir kommen zurück zu Kongruenzen und zeigen eine Behauptung, die das modulo-Rechnen vereinfacht.

(7.7) *Es seien $a_1, a_2 \in \mathbb{Z}$, $m \in \mathbb{N}$, und es gelte $a_i = q_i \cdot m + r_i$ mit $0 \leq r_i < m$, $i \in \{1, 2\}$. Dann gilt*

$$a_1 \equiv a_2 \mod m \iff r_1 = r_2$$

Insbesondere enthält jede Äquivalenzklasse der Relation „$\equiv \mod m$“ genau ein Element $v \in \mathbb{Z}$ mit $0 \leq v < m$.

Beweis. OE. gelte $r_1 \leq r_2$. Wir haben $a_2 - a_1 = (q_2 \cdot m + r_2) - (q_1 \cdot m + r_1) = (q_2 - q_1) \cdot m + (r_2 - r_1)$. Wegen (1.26) gilt $m|(a_2 - a_1) \iff m|(r_2 - r_1)$. Andererseits ist $0 \leq r_2 - r_1 < m$ (addiere die Ungleichungen $r_2 < m$ und $-r_1 \leq 0$). Also gilt $m|(r_2 - r_1) \iff r_2 - r_1 = 0$ und das ist die erste Aussage. Sei K eine Äquivalenzklasse der Relation „$\equiv \mod m$“.

Eindeutigkeit: Alle Elemente in K sind zueinander kongruent $\mod m$. Nach dem eben gezeigten kann es daher in K höchstens ein Element der gesuchten Form geben.

Existenz: Sei $a \in K$. Nach (7.1) gibt es $0 \leq v < m$ und $q \in \mathbb{Z}$ mit $a = qm + v$. Da $m|q \cdot m = a - v$ ist $v \equiv a \mod m$, also $v \in K$. ∎

(7.8) Bemerkung. Es gilt also für den Quotientenraum $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$. Das haben wir für Beispiele in (1.31) schon gesehen und später gelegentlich benutzt.

Man nennt die Menge $\{0, 1, \ldots, m-1\}$ ein **Repräsentantensystem** der **Restklassen** modulo m. Es gibt auch andere Repräsentantensysteme: So ist $\{-3, -2, -1, 0, 1, 2, 3\}$ ein Repräsentantensystem modulo 7.

Es gilt nach (6.19.6)

(7.9) *Für jedes $m \in \mathbb{N} \setminus \{1\}$ ist $(\mathbb{Z}_m, +_m, \cdot_m)$ ein kommutativer Ring. Es sind $\overline{0}$ das Nullelement und $\overline{1}$ das Einselement.*

Wir zeigen einige Phänomene, die in den Ringen $\mathbb{Z}_m$ auftreten können. Sie sind uns in den Übungen alle schon begegnet.

(7.10) Beispiele. 1.) $m = 6$: Es ist $\overline{2} \cdot_6 \overline{3} = \overline{0}$, obwohl $\overline{2} \neq \overline{0}$ und $\overline{3} \neq \overline{0}$. Man sagt „Der Ring $\mathbb{Z}_6$ ist nicht nullteilerfrei“.

2.) In den Ringen $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$ besitzt jedes Element $\neq \overline{0}$ ein Inverses, d.h. diese Ringe sind Körper.

Explizit: $\overline{2} \cdot_5 \overline{3} = \overline{1}$ und $\overline{4} \cdot_5 \overline{4} = \overline{1}$.

3.) Die Gruppe $(\mathbb{Z}_{12}, +_{12})$ ist *isomorph* zur Uhr-Gruppe aus Aufgabe 70.

4.) In der Vorlesung erstellen wir eine Verknüpfungstafel der invertierbaren Elemente aus $\mathbb{Z}_8$.

(7.11) *Ist p eine Primzahl, so ist $\mathbb{Z}_p$ ein Körper.*

Beweis. Es sei $a \in \mathbb{Z}$ mit $0 < a < p$, dann ist der größte gemeinsame Teiler von p und a die Zahl 1. Nach Aufgabe 71 gibt es $x, y \in \mathbb{Z}$ mit $ax + py = 1$. Dann folgt $p|ax - 1$, bzw. $ax \equiv 1 \mod p$. Daher sind alle Elemente aus $\mathbb{Z}_p \setminus \left\{\overline{0}\right\}$ invertierbar. ∎

Der Euklidische Algorithmus

Wir beschäftigen uns mit den Begriffen **größter gemeinsamer Teiler** (ggT) und **kleinstes gemeinsames Vielfaches** (kgV).

Mit kleinen lateinischen Buchstaben sind stets ganze Zahlen gemeint.

Gilt $t|a$ und $t|b$, so heißt t ein **gemeinsamer Teiler** von a und b. Es ist klar, dass die Menge der gemeinsamen Teiler von a und b ein Maximum besitzt, wenn nicht $a = b = 0$. Dieses Maximum wird **größter gemeinsamer Teiler** von a und b genannt und $\mathrm{ggT}(a, b)$ geschrieben. Der Ausdruck $\mathrm{ggT}(0, 0)$ ist nicht definiert. Aufgabe 71 zeigt:

(7.12) *Es seien* $a, b \in \mathbb{Z}$, $a \neq 0$.

(1) *Es gibt* $x, y \in \mathbb{Z}$ *mit* $\mathrm{ggT}(a, b) = ax + by$.

(2) *Für jeden gemeinsamen Teiler* t *von* a *und* b *gilt* $t|\,\mathrm{ggT}(a, b)$.

Ist die Primfaktorzerlegung von a und b gegeben, so kann man $\mathrm{ggT}(a, b)$ leicht bestimmen.

Beispiel. $a = 2^4 \cdot 3 \cdot 5^2 \cdot 7 \cdot 13^4$, $b = 2^2 \cdot 5 \cdot 7^2 \cdot 13^3 \cdot 17 \cdot 23$, $\mathrm{ggT}(a, b) = 2^2 \cdot 5 \cdot 7 \cdot 13^3$.

Gilt $a|c$ und $b|c$, so heißt c ein **gemeinsames Vielfaches** von a und b. Die Menge der gemeinsamen Vielfachen in $\mathbb{N}$ besitzt ein Minimum. Es wird **kleinstes gemeinsames Vielfaches** genannt und $\mathrm{kgV}(a, b)$ geschrieben. Wieder kann man zeigen, dass für jedes gemeinsame Vielfache v von a und b gilt $\mathrm{kgV}(a, b)|v$.

Beispiel (Fortsetzung). Für a und b wie vorhin ist

$$\mathrm{kgV}(a, b) = 2^4 \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 13^4 \cdot 17 \cdot 23.$$

(7.13) Bemerkung. 1.) $\mathrm{ggT}(a, 0) = |a|$.

2.) $\mathrm{kgV}(a, 0) = 0$.

3.) Abgesehen von der einzigen Ausnahme 2.) gilt: $\mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$ sind immer positiv, also in $\mathbb{N}$, auch wenn a oder b negativ ist.

Es gilt allgemein

(7.14) $\forall a, b \in \mathbb{Z} : \mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = |a| \cdot |b|$.

Beweis. Siehe [RS14, Satz 5.3.4]. ∎

Sind a und b gegeben, so genügt es $\mathrm{ggT}(a,b)$ zu berechnen — $\mathrm{kgV}(a,b)$ kann dann mit Hilfe von (7.14) bestimmt werden. Außerdem kann man sich auf $a,b \geq 0$ beschränken.

Wir kommen zum **Euklidischen Algorithmus**, mit dem man für $a,b \in \mathbb{N}$ den größten gemeinsamen Teiler $\mathrm{ggT}(a,b)$ berechnen kann. Dem Euklidischen Algorithmus liegt die folgende einfache Beobachtung über die Division mit Rest zu Grunde:

(7.15) *Seien* $a,b \in \mathbb{N}$ *und* $a = q \cdot b + r$ *mit* $0 \leq r < b$*, so folgt* $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,r)$.

Beweis. Ist t ein gemeinsamer Teiler von b und r, so auf Grund von (1.26.5) auch von a und b.

Ist umgekehrt t ein gemeinsamer Teiler von a und b, so ist wegen $r = a - q \cdot b$ gemäß (1.26.5) t auch ein gemeinsamer Teiler von b und r. Die Menge der gemeinsamen Teiler von b und r ist also gleich der Menge der gemeinsamen Teiler von a und b; insbesondere gilt $\mathrm{ggT}(b,r) = \mathrm{ggT}(a,b)$. ∎

Es folgt ein Kochrezept zur Anwendung des Euklidischen Algorithmus. Wie schon bemerkt, kann oE $a,b > 0$ angenommen werden.

Euklidischer Algorithmus. Für $a,b \in \mathbb{N}$ bestimme $\mathrm{ggT}(a,b)$:

1. Teile a durch b und bestimme den Rest r (d. h. bestimme r, so dass gilt $a = q \cdot b + r$, wobei $q, r \in \mathbb{Z},\ \ 0 \leq r < b$).

2. Im Fall $r = 0$ ist man fertig, b ist der gesuchte Wert.

3. Andernfalls setze man $a := b,\ b := r$ und gehe nach **1.**

Beispiel. $a = 816,\ b = 294$:

$$\begin{aligned} 816 &= 2 \cdot 294 + 228 \\ 294 &= 1 \cdot 228 + 66 \\ 228 &= 3 \cdot 66 + 30 \\ 66 &= 2 \cdot 30 + 6 \\ 30 &= 5 \cdot 6 + 0 \qquad \Longrightarrow \quad \mathrm{ggT}(816,294) = 6 \end{aligned}$$

Der Algorithmus endet nach endlich vielen Schritten, da bei jeder Ausführung der Anweisung $b := r$ der Wert von b verkleinert wird.

Dass der Euklidische Algorithmus tatsächlich den $\mathrm{ggT}(a,b)$ berechnet, lässt sich wie folgt einsehen:

Ist $r > 0$, so wird in **3.** die Anweisung $a := b,\ b := r$ ausgeführt und anschließend nach **1.** gegangen. Dies bedeutet, dass man die Aufgabe, den $\mathrm{ggT}(a,b)$ zu berechnen, durch die Aufgabe, den $\mathrm{ggT}(b,r)$ zu berechnen, ersetzt hat; wegen (7.15) gilt aber $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,r)$.

Ist $r = 0$, so gilt $\mathrm{ggT}(b, r) = b$ nach Bemerkung (7.13.1) und man ist fertig.

Aus dem Euklidischen Algorithmus ergibt sich durch Rücksubstitution ein konstruktiver Beweis für (7.12). Man findet also $u, v \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = au + bv$.

Man spricht auch vom **erweiterten Euklidischen Algorithmus**.

Beispiel (Fortsetzung).

$$\begin{aligned}
& 6 &=& \ 66 - 2 \cdot 30 \\
& 30 &=& \ 228 - 3 \cdot 66 \\
\Longrightarrow \quad & 6 &=& \ 66 - 2 \cdot (228 - 3 \cdot 66) = 7 \cdot 66 - 2 \cdot 228 \\
& 66 &=& \ b - 1 \cdot 228 \\
\Longrightarrow \quad & 6 &=& \ 7 \cdot (b - 1 \cdot 228) - 2 \cdot 228 = 7 \cdot b - 9 \cdot 228 \\
& 228 &=& \ a - 2 \cdot b \\
\Longrightarrow \quad & 6 &=& \ 7 \cdot b - 9 \cdot (a - 2 \cdot b) = 25 \cdot b - 9 \cdot a
\end{aligned}$$

Daher gilt $\mathrm{ggT}(a, b) = (-9)a + 25\, b$.

(7.16) Bemerkung. 1.) $m = 101$ ist eine Primzahl. Wir zeigen, dass $a = 49$ invertierbar $\mod m$ ist, indem wir die Inverse bestimmen:

$$m = 2a + 3; \quad a = 16 \cdot 3 + 1 \implies 1 = a - 16 \cdot 3 = a - 16(m - 2a) = 33a - ?? \cdot m;$$

es folgt $1 \equiv 33 \cdot a \mod m$. Daher ist $\overline{33}$ die Inverse von $\overline{49}$ in $\mathbb{Z}_{101}$.

2.) Ähnlich erkennt man erneut (vgl. auch (7.11)), dass für jede Primzahl p der Ring $\mathbb{Z}_p$ ein Körper ist: Es gilt nämlich $\mathrm{ggT}(a, p) = 1$ für alle $a \in \{1, \ldots, p-1\}$. Daher liefert der erweiterte Euklidische Algorithmus (vgl. (7.12)) $u, v \in \mathbb{Z}$ mit $au + pv = 1$; also $au \equiv 1 \mod p$.

3.) Die Abbildung $\mathrm{ggT} : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \to \mathbb{Z} \setminus \{0\}$ ist eine Verknüpfung.

4.) Man kann leicht sehen, dass $(\mathbb{Z} \setminus \{0\}, \mathrm{ggT})$ eine kommutative Halbgruppe ist.

5.) Insbesondere gilt $\mathrm{ggT}(\mathrm{ggT}(a, b), c) = \mathrm{ggT}(a, \mathrm{ggT}(b, c))$ (Assoziativität!) für alle $a, b, c \in \mathbb{Z} \setminus \{0\}$. Daher ist der Ausdruck $\mathrm{ggT}(a, b, c) := \mathrm{ggT}(a, \mathrm{ggT}(b, c))$ sinnvoll. Entsprechend definiert man $\mathrm{ggT}(a_1, \ldots, a_n)$ für $a_i \in \mathbb{Z} \setminus \{0\}$.

Literatur

[AA05] Appell, K. ; Appell, J.: *Mengen – Zahlen – Zahlbereiche. Eine elementare Einührung in die Mathematik.* 1. Aufl. Spektrum Akademischer Verlag, Heidelberg, 2005

[Ded65] Dedekind, Richard: *Was sind und was sollen die Zahlen?* 10. Aufl. Vieweg-Verlag, Braunschweig-Wiesbaden, 1965. – Auch: Gesammelte Werke, Band 3, S. 335-391; und Scan der 2. Auflage (1893)[21]

[Ebb03] Ebbinghaus, Heinz-Dieter: *Einführung in die Mengenlehre.* 4. Spektrum Akademischer Verlag, Heidelberg, 2003

[GM04] Gröger, Detlef ; Marti, Kurt: *Grundkurs Mathematik für Ingenieure, Natur- und Wirtschaftswissenschaftler.* 2. Aufl. Physica-Verlag, 2004

[Hal60] Halmos, Paul R.: *Naive set theory.* Van Nostrand, Princeton, 1960

[Heu03] Heuser, Harro: *Lehrbuch der Analysis.* 15. Aufl. Vieweg-Verlag, Braunschweig-Wiesbaden, 2003

[Leu10] Leuders, Timo: *Erlebnis Arithmetik.* Spektrum Akademischer Verlag, Heidelberg, 2010

[LS07] Lehmann, Ingmar ; Schulz, Wolfgang: *Menge — Relationen — Funktionen.* 3. Aufl. Vieweg+Teubner, Wiesbaden, 2007

[MM11] Meinel, Christoph ; Mundhenk, Martin: *Mathematische Grundlagen der Informatik — Mathematisches Denken und Beweisen — Eine Einführung.* 5. Aufl. Vieweg+Teubner, Wiesbaden, 2011

[Ovc15] Ovchinnikov, Sergei: *Number Systems.* Amer. Math. Soc., 2015

[Pad08] Padberg, Friedhelm: *Elementare Zahlentheorie.* 3. Aufl. Spektrum Akademischer Verlag, Heidelberg, 2008

[PDS95] Padberg, Friedhelm ; Danckwerts, Rainer ; Stein, Martin: *Zahlbereiche.* Spektrum Akademischer Verlag, Heidelberg, 1995

[RS14] Reiss, K. ; Schmieder, G.: *Basiswissen Zahlentheorie.* 3. Aufl. Springer-Verlag, Berlin-Heidelberg-New York, 2014

[SS09] Schichl, Hermann ; Steinbauer, Roland: *Einführung in das mathematische Arbeiten.* Springer-Verlag, Berlin-Heidelberg-New York, 2009

[Zag77] Zagier, Don: *Die ersten 50 Millionen Primzahlen.* Birkhäuser-Verlag, Basel-Boston-Berlin, 1977. – Beihefte zur Zeitschrift "Elemente der Mathematik". Beiheft No.15

[21] `http://archive.org/details/wassindundwasso00dedegoog`

Index