University of Stuttgart

Linare Algebra und analytische Geometrie I

Meinolf Geck
Assistenz: Eirini Chavli, Inga Paul

Lehrstuhl für Algebra

Wintersemester 2018/19

Ziele/Inhalt der Vorlesung

- **Lösen von linearen Gleichungssystemen:**

$$\begin{aligned} x_1 &+ 3x_2 - 2x_3 = 1 \\ 2x_1 &+ 2x_2 \quad\quad = 2 \\ 4x_1 &+ 6x_2 + x_3 = 8 \end{aligned}$$

  (Anwendungen in Natur- und Ingenieurwissenschaften, . . .)

- **Allgemeine Theorie der Vektorräume und linearen Abbildungen**
- **Hinführung auf neue Zahlsysteme und Strukturen:**
  Zum Beispiel "binäres" Zahlensystem $\{0, 1\}$ mit $1 + 1 = 0$ ($\rightsquigarrow$ Informatik).
- **Die ersten Kapitelüberschriften:**
  - Kapitel 0: Grundlagen.
  - Kapitel 1: Matrizen.
  - Kapitel 2: Vektorräume.

- **Modell für den axiomatischen Aufbau einer Theorie:**
  - Festlegung von grundlegenden Begriffen und Regeln (“Axiomen”), die als wahr vorausgesetzt werden.
  - Herleiten (“Beweisen”) von Aussagen aus den Axiomen sowie bereits bewiesenen Aussagen nach bestimmten logischen Regeln.
  - Präzises Formulieren und Argumentieren.
    (Anwendungen im Studium und in allen späteren Berufen!)

  (Obiges gilt genauso für die Vorlesung Analysis I.)

- **"Axiom" für diese Vorlesung:**
  - Das Zahlensystem der ganzen Zahlen, also der Zahlen $0, \pm 1, \pm 2, \pm 3, \ldots$, sowie das Rechnen mit diesen Zahlen (Addition, Multiplikation) werden als bekannt vorausgesetzt.
  - Mengentheoretische Sprechweisen und Grundlagen aus der mathematischen Logik werden schrittweise eingeführt wenn sie gebraucht werden.

Literatur

Besonders geeignet für diese Vorlesung:

- S. Axler, Linear Algebra done right. Undergraduate texts in mathematics, Springer-Verlag, 2015.
- G. Fischer, Lineare Algebra: Eine Einführung für Studienanfänger, Vieweg + Teubner Verlag; 17. Auflage 2010.
- B. Huppert und W. Willems, Lineare Algebra: Mit zahlreichen Anwendungen in Kryptographie, Codierungstheorie, Mathematischer Physik und Stochastischen Prozessen, Vieweg + Teubner Verlag, 2. Auflage 2010.
- M. Koecher, Lineare Algebra und analytische Geometrie, Grundwissen Mathematik, Springer-Verlag, 4. Auflage, 2002.
- D. Serre, Matrices: Theory and Applications. Graduate Texts in Mathematics 216, Springer-Verlag, 2. Auflage, 2010.

Weiterführende Texte:

- M. ARTIN, Algebra. Aus dem Englischen übersetzt von Annette A'Campo. Birkhäuser Verlag, 1993.
- N. BOURBAKI, Éléments de Mathématiques. Algèbre. Chap. 1 à 3, Masson, Paris, 1970; Chap. 4 à 7, Masson, Paris, 1981.
- S. H. FRIEDBERG, A. J. INSEL UND L. E. SPENCE, Linear Algebra, 4th ed., Pearson, 2002.
- P. R. HALMOS, Naive Mengenlehre, Vandenhoeck & Ruprecht, 5. Auflage, 1994.
- F. LORENZ, Lineare Algebra, 2 Bände. Spektrum Akademischer Verlag; 1. Band, 4. Auflage 2008; 2. Band, 3. Auflage, 1992.
- D. POOLE, Linear Algebra: A Modern Introduction. Brooks Cole Pub Co., 3. Auflage, 2010.

Zum Auffrischen von Schulwisssen und Grundlagen:

- T. GLOSAUSER, (Hoch)Schulmathematik, Ein Sprungbrett vom Gymnasium zur Uni. Springer-Spektrum, 2015.
- M. LIEBECK, A Concise Introduction to Pure Mathematics. Chapman Hall/CRC Mathematics Series, CRC Press, 3rd edition 2010.
- MINT Kolleg Baden-Württemberg, Mathematik-Vorkurs (Online), siehe `http://www.mint-kolleg.de/stuttgart/angebote/online_kurse/onlinemathematikvorkurs.html`.

Frei verfügbare software zum Ausprobieren und Experimentieren:

- GAP - Groups, Algorithms, and Programming, siehe `http://www.gap-system.org`.
- SageMath, siehe `https://www.sagemath.org`.

mathematik

Universität Stuttgart

Kapitel 0: Grundlagen (8 Vorlesungen)

§1 Mengen und Aussagen

Eine ***Menge*** ist für uns einfach eine Zusammenfassung von bestimmten Objekten, die als ***Elemente*** der Menge bezeichnet werden. Eine solche Zusammenfassung wird durch geschweifte Klammern $\{ \dots \}$ bezeichnet, zum Beispiel:

$$
\begin{aligned}
S &= \{ \text{ alle Einwohner von Stuttgart } \}, \\
\mathbb{N} &= \{1, 2, 3, 4, \dots\} \quad \text{die natürlichen Zahlen}, \\
\mathbb{N}_0 &= \{0, 1, 2, 3, 4, \dots\} \quad \text{die natürlichen Zahlen mit } 0, \\
\mathbb{Z} &= \{0, 1, -1, 2, -2, 3, -3, \dots\} \quad \text{die ganzen Zahlen}.
\end{aligned}
$$

Mengen können also nur eine bestimmte Anzahl von Elementen enthalten (wie im 1. Beispiel) oder auch unendlich viele Elemente (wie im 2., 3. und 4. Beispiel).

mathematik

Universität Stuttgart

Schreibweisen:

"$a \in A$" bedeutet: Das Objekt a ist ein Element der Menge A;
analog bedeutet "$a \notin A$", dass a nicht zu A gehört.

"$A \subseteq B$" bedeutet: Die Menge A ist eine Teilmenge der Menge B, und dies wiederum bedeutet, dass jedes Element von A auch ein Element von B ist.

"$A = B$" bedeutet: Die Menge A enthält die gleichen Elemente wie die Menge B, oder anders ausgedrückt: Es gilt $A \subseteq B$ und $B \subseteq A$.

Zum Beispiel gilt $-5 \notin \mathbb{N}$ und $\mathbb{N} \subseteq \mathbb{Z}$. Ist $A \subseteq B$ und $A \neq B$, so schreiben wir $A \subsetneq B$.

Das Symbol "$\varnothing$" steht für die ***leere Menge***, also die Menge, die überhaupt kein Element enthält. Wir können dies auch mit $\{\}$ bezeichnen. Es gilt $\varnothing \subseteq A$ für jede Menge A.

mathematik

Universität Stuttgart

Unter einer ***Aussage*** verstehen wir einen Satz (auf deutsch, englisch oder in sonst irgendeiner Zeichensprache), der entweder wahr oder falsch ist.

Beispiel: der Satz ”Der 17.10.2018 ist ein Mittwoch” ist eine wahre Aussage. Aber der Satz ”Bitte stellen Sie Fragen, wenn etwas nicht klar ist” ist keine Aussage.

Natürlich ist ein in der mathematischen Zeichensprache verfasster Satz wie ”$1 + 1 = 3$” eine Aussage, die in diesem Fall falsch ist.

Beachte: Es kann dabei sein, dass wir vielleicht nicht wissen, ob die fragliche Aussage nun wahr oder falsch ist, oder dass es extrem schwierig ist, die Antwort zu finden; es kommt nur darauf an, dass etwas gesagt wird, das entweder wahr oder falsch ist. – Beispiele:

- ”Es gibt Ausserirdische”.
- $2^{277232917} - 1$ (eine Zahl mit 23249425 Ziffern) ist eine Primzahl.

Mengenbildung mit Aussagen: Gegeben sei eine Menge A und, für jedes $a \in A$, eine Aussage $P(a)$.

Dann können wir die Menge aller derjenigen $a \in A$ bilden, für die $P(a)$ wahr ist, und dies ist eine Teilmenge von A; in Zeichen:

$$\{a \in A \mid P(a) \text{ ist wahr}\} \subseteq A.$$

BEISPIEL: Sei A die Menge aller Anwesenden in diesem Hörsaal. Für jedes $a \in A$ sei $P(a)$ die Aussage: ”a trägt einen blauen Pullover”.

Dann ist also $\{a \in A \mid P(a) \text{ ist wahr}\}$ genau die Menge der hier Anwesenden, die einen blauen Pullover tragen.

Hier sehen wir auch die Nützlichkeit der leeren Menge: Trägt nämlich niemand einen blauen Pullover, so ist $\{a \in A \mid P(a) \text{ ist wahr}\} = \varnothing$.

BEISPIEL: Sei $A = \mathbb{N}$ und $P(n)$ die Aussage: ”n ist eine gerade Zahl”. Dann ist also

$$\{n \in A \mid P(n) \text{ ist wahr}\} = \{2, 4, 6, 8, \ldots\}$$

die Menge der geraden Zahlen.

Beachten Sie: Es ist offenbar egal, ob wir $P(a)$ oder $P(n)$ schreiben, denn das Symbol ”a” bzw. ”n” ist hier ja nur ein Platzhalter, der auf ein Element von A verweist.

Sei nun $Q(n)$ die Aussage: ”$P(n)$ ist falsch”. Dann ist

$$\{n \in A \mid Q(n) \text{ ist wahr}\} = \{n \in A \mid P(n) \text{ ist falsch}\} = \{1, 3, 5, 7, \ldots\}$$

die Menge der ungeraden Zahlen.

Weitere Konstruktionen zum Bilden neuer Mengen: Sind A, B zwei Mengen, so ist

$$A \setminus B := \{x \in A \mid x \notin B\}$$

das ***Komplement*** von B in A (oft auch A^c geschrieben).

Hierbei steht der Doppelpunkt in ”:=” für eine Definition: Es wird keine Gleichheit behauptet, sondern das Symbol ”$A \setminus B$” ist lediglich ein Name für die Menge auf der rechten Seite.

Der ***Durchschnitt*** von A und B ist definiert durch

$$A \cap B := \{x \in A \mid x \in B\} = \{x \in B \mid x \in A\}.$$

Weiterhin können wir die ***Vereinigungsmenge*** $A \cup B$ bilden. Diese Menge ist dadurch bestimmt, dass $A \subseteq A \cup B$ und $B \subseteq A \cup B$ gelten, sowie $A \cup B$ keine weiteren Elemente enthält.

Schliesslich können wir zu jeder Menge A auch ihre ***Potenzmenge*** $\mathcal{P}(A)$ bilden, d.h., die Menge aller Teilmengen von A.

Zum Beispiel besteht die Potenzmenge von $A = \{1, 2, 3\}$ aus 8 Elementen:

$$\mathcal{P}(A) = \{\varnothing,\ \{1\},\ \{2\},\ \{3\},\ \{1,2\},\ \{1,3\},\ \{2,3\},\ \{1,2,3\}\}.$$

Hier gilt dann etwa $\{1,2\} \in \mathcal{P}(A)$ und $\{\varnothing, \{1\}\} \subseteq \mathcal{P}(A)$, d.h., Mengen können auch selbst wieder Elemente von anderen Mengen sein.

Letztendlich sind alle Objekte, die wir betrachten, stets Mengen; die Schreibweise "$A \in B$" macht also Sinn für beliebige Mengen A, B.

Weitere Literatur:
K. HRBACEK UND T. JECH, Introduction to set theory, third edition. Marcel Dekker Inc., 1999.

Man kann in logische Schwierigkeiten kommen, wenn man die obigen Mengenbildungsprinzipien verlässt.

Berühmtes Beispiel: Die ***Russel'sche Antinomie***
(siehe auch `https://en.wikipedia.org/wiki/Russell's_paradox`).

Nehmen wir an, wir könnten die Menge aller Mengen bilden; sei X diese Menge. Dann können wir auch die Menge $Y := \{A \in X \mid A \notin A\}$ bilden.

Frage: Gehört Y selbst zu Y oder nicht ? — Nun, wäre $Y \in Y$, so müsste nach Definition $Y \notin Y$ gelten; wäre $Y \notin Y$, so müsste $Y \in Y$ gelten.

D.h., in jedem Fall erhalten wir etwas, das zugleich wahr und falsch ist. Das Problem lag in der Annahme, dass wir X bilden können – diese Annahme ist allerdings auch durch keines der obigen Prinzipien erfasst.

Beachte: Auch in der Umgangssprache gibt es solche "Antinomien". Beispiele: "Ich lüge gerade" oder "Dieser Satz ist falsch".

"RICHTIGES" BEISPIEL:
Sei A eine nicht-leere Menge und B eine beliebige Teilmenge von $\mathcal{P}(A)$, d.h., B ist eine Menge von Teilmengen von A.

Dann können wir die Vereinigung aller $X \in B$ bilden.

Dazu betrachte für $a \in A$ die Aussage $P(a)$: "Es gibt ein $X \in B$ mit $a \in X$".

Dann ist $\displaystyle\bigcup_{X \in B} X := \{a \in A \mid \text{es gibt ein } X \in B \text{ mit } a \in X\}$

Konkretes Beispiel: $A =$ Menge aller Menschen auf der Erde.

$B = \Big\{\{\text{Menschen in Deutschland}\},\ \{\text{Menschen in Frankreich}\},$
$\{\text{Menschen in Polen}\},\ \ldots \text{usw. für alle (noch) 28 Länder der EU}\Big\}.$

Dann ist $\displaystyle\bigcup_{X \in B} X = \{\text{alle Menschen in der EU}\}.$

Verknüpfung von Aussagen:

Ist P eine Aussage, so wird mit $\neg P$ die Negation von P bezeichnet.

Beispiel: Ist P die Aussage "Heute ist Dienstag", so ist $\neg P$ die Aussage "Heute ist nicht Dienstag".

Sind P und Q Aussagen, so erhalten wir neue Aussagen durch folgende Verknüpfungen:

"$P \vee Q$" ist die Aussage: "P ist wahr oder Q ist wahr oder beide sind wahr."

"$P \wedge Q$" ist die Aussage: "P ist wahr und Q ist wahr."

"$P \Rightarrow Q$" ist die Aussage: "Aus P folgt Q" oder anders ausgedrückt: "Wann immer P wahr ist, so muss auch Q wahr sein."

Es ist manchmal nützlich, diese Verknüpfungen durch ***Wahrheitstabellen*** zu beschreiben, die angeben, welchen Wahrheitswert die Verknüpfung in Abhängigkeit von den möglichen Kombinationen der Wahrheitswerte von P und Q hat, also etwa:

P	$\neg P$
w	f
f	w

P	Q	$P \vee Q$	$P \wedge Q$	$P \Rightarrow Q$
w	w	w	w	w
w	f	w	f	f
f	w	w	f	w
f	f	f	f	w

Vielleicht kommt Ihnen die letzte Spalte etwas ungewohnt vor! Dazu beachten Sie, dass aus falschen Aussagen durchaus wahre Aussagen gefolgert werden können; es geht ja nur darum, dass die Folgerung als solche korrekt ist.

Beispiel: für $a, b \in \mathbb{Z}$ ist die folgende Verknüpfung eine wahre Aussage:

$$a = b \quad \Rightarrow \quad a^2 = b^2.$$

Beweis: Wenn $a = b$ gilt, so können wir im Produkt $a^2 = a \cdot a$ beide Faktoren durch b ersetzen und erhalten $b \cdot b = b^2$, also die rechte Seite.

Nehmen wir konkret $a = 2$ und $b = -2$, so ist "$a = b$" falsch, aber "$a^2 = b^2$" wahr; nehmen wir $a = 2$ und $b = 3$, so ist "$a = b$" falsch und auch "$a^2 = b^2$" falsch. Aber der obige Beweis ist natürlich immer richtig, egal in welcher Beziehung a und b zueinander stehen.
Das Beispiel $a = 2$ und $b = -2$ zeigt auch, dass die umgekehrte Folgerung

$$a^2 = b^2 \quad \Rightarrow \quad a = b$$

keine wahre Aussage ist.

Allgemein sagen wir, dass P und Q ***äquivalente Aussagen*** sind (in Zeichen: "$P \Leftrightarrow Q$"), wenn sowohl "$P \Rightarrow Q$" als auch "$Q \Rightarrow P$" wahr sind.

Wir drücken dies auch so aus, dass P genau dann gilt, wenn Q gilt. Mit Hilfe der Werte in den entsprechenden Wahrheitstabellen stellen Sie sofort fest:

- "$P \Leftrightarrow Q$" ist äquivalent zu: Entweder P, Q beide wahr oder beide falsch.
- "$P \Rightarrow Q$" ist äquivalent zu: "$(\neg P) \vee Q$".
- "$P \Rightarrow Q$" ist auch äquivalent zu: "$(\neg Q) \Rightarrow (\neg P)$".

Letztere Verknüpfung heißt ***Kontraposition***.

Quantoren: Dies sind die mathematischen Kurzzeichen $\exists$, welches für "es existiert" steht, und $\forall$, welches für "für alle" steht.

Beispiele:

- die Aussage "Es gibt eine natürliche Zahl n mit $n^3 = 8$" lässt sich kurz schreiben als: $\exists n \in \mathbb{N} : n^3 = 8$.
- Die Aussage "Das Quadrat einer beliebigen ganzen Zahl ist entweder 0 oder positiv" lässt sich kurz schreiben als: $\forall n \in \mathbb{Z} : n^2 \geqslant 0$.

Im Prinzip sollte man sämtliche mathematischen Aussagen in dieser Vorlesung in einer Formelsprache ausdrücken können, in denen nur Aussagen über Elemente in Mengen, Verknüpfungen von Aussagen und Quantoren vorkommen.

Aber bei komplizierteren Sachverhalten wird man der besseren Verständlichkeit halber stets versuchen, diese Sachverhalte so weit wie möglich in "normalen", möglichst einprägsamen, sprachlichen Sätzen auszudrücken.

§2 Beweistechniken und elementare Arithmetik

Wir stellen grundlegende Beweistechniken vor und illustrieren diese durch einige Beispiele, in denen wichtige Aussagen über ganze Zahlen (die zum Teil bereits aus der Schule vertraut sein mögen) mathematisch korrekt hergeleitet werden. Dabei setzen wir lediglich die Kenntnis der Grundrechenarten für natürliche und ganze (und später auch rationale) Zahlen voraus.

Definition 2.1

Seien $n, m \in \mathbb{Z}$. Wir schreiben $n \mid m$ und sagen "n teilt m" oder "m ist ein Vielfaches von n", wenn es ein $a \in \mathbb{Z}$ gibt mit $m = a \cdot n$.

Beispiele: $2 \mid 6$ (denn $6 = 3 \cdot 2$), $5 \mid 0$ (denn $0 = 0 \cdot 5$) und $3 \nmid 10$ (denn die positiven Vielfachen von 3 sind $3, 6, 9, 12, \ldots$).

Lemma 2.2 (oder auch "Hilfssatz")

(a) Seien $n, m, k \in \mathbb{Z}$. Gilt $n \mid m$ und $m \mid k$, so auch $n \mid k$.
(b) Seien $n, m, k \in \mathbb{Z}$ und $a, b \in \mathbb{Z}$. Gilt $n \mid m$ und $n \mid k$, so auch $n \mid (a \cdot m + b \cdot k)$.

Beweis. Dies ist ein Beispiel eines "Routine-Beweises", wo es darum geht, die Richtigkeit von vorgegebenen Formeln durch einfaches Nachrechnen zu bestätigen.

(a) Nach Voraussetzung gibt es $a, b \in \mathbb{Z}$ mit $m = a \cdot n$ und $k = b \cdot m$. Dann ist $k = b \cdot m = b \cdot (a \cdot n) = (b \cdot a) \cdot n$. (Hier haben wir benutzt, dass man Produkte von ganzen Zahlen beliebig klammern darf.) Setzen wir $c = b \cdot a \in \mathbb{Z}$, so gilt also $k = c \cdot n$ und damit $n \mid k$.

(b) Voraussetzung ist: $n \mid m$ und $n \mid k$. Also gibt es $u, v \in \mathbb{Z}$ mit $m = u \cdot n$ und $k = v \cdot n$. Dann ist

$$a \cdot m + b \cdot k = a \cdot (u \cdot n) + b \cdot (v \cdot n) = (a \cdot u) \cdot n + (b \cdot v) \cdot n = (a \cdot u + b \cdot v) \cdot n.$$

(Hier haben wir wiederum benutzt, dass man Produkte beliebig klammern darf; ausserdem haben wir eine Distributivregel verwendet, die besagt, dass man in einer Summe von zwei Produkten gemeinsame Faktoren ausklammern darf.) Setzen wir $c = a \cdot u + b \cdot v \in \mathbb{Z}$, so gilt also $a \cdot m + b \cdot k = c \cdot n$ und damit $n \mid (a \cdot m + b \cdot k)$. □

Wir benutzen das Symbol □, um das Ende eines Beweises anzuzeigen.
Im Folgenden werden wir nicht mehr explizit wie im obigen Beweis erwähnen, wenn wir eine der üblichen Regeln beim Rechnen mit ganzen Zahlen verwenden. Ausserdem lassen wir den Punkt bei der Multiplikation der besseren Lesbarkeit wegen einfach weg.

Lemma 2.3

(a) Ist $n \in \mathbb{N}_0$ ungerade, so ist auch n^2 ungerade.
(b) Ist $n \in \mathbb{N}_0$ so dass n^2 gerade ist, so ist auch n selbst gerade.

Beweis. (a) Da n ungerade ist, gilt $n = 2m + 1$ mit einem $m \in \mathbb{N}_0$. Damit erhalten wir $n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$. Setzen wir $k = 2m^2 + 2m \in \mathbb{N}_0$, so gilt also $n^2 = 2k + 1$, d.h., n^2 ist auch ungerade.

(b) Folgt sofort aus (a) durch "Kontraposition". Sei P die Aussage "n ist ungerade" und Q die Aussage "n^2 ist ungerade". In (a) wurde gezeigt, dass "$P \Rightarrow Q$" gilt. Kontraposition bedeutet, dass dann auch "$(\neg Q) \Rightarrow (\neg P)$" gilt, also genau die Aussage in (b). □

Lemma 2.4 (“Kürzungsregel”)

Seien $n, m \in \mathbb{Z}$ und $0 \neq k \in \mathbb{Z}$. Gilt $kn = km$, so folgt $n = m$.

Beweis. Wir betrachten die Aussagen P: “$kn = km$” und Q: “$n = m$”.
Um “$P \Rightarrow Q$” zu zeigen, können wir auch genauso gut “$(\neg Q) \Rightarrow (\neg P)$” zeigen.
Nehmen wir also an, es gelte $\neg Q$, d.h., es sei $n \neq m$. Dann ist $n - m \neq 0$ und $k(n-m) \neq 0$ (weil das Produkt von zwei ganzen Zahlen ungleich 0 wieder ungleich 0 ist). Nun ist $kn - km = k(n-m) \neq 0$ also folgt $kn \neq km$, d.h., $\neg P$. □

Beweise durch Kontraposition werden auch oft als “Widerspruchsbeweise” dargestellt. Man nimmt dazu an, dass die gewünschte Aussage falsch ist, und leitet dann daraus einen Widerspruch ab (d.h., eine Aussage, von der wir bereits wissen, dass sie falsch ist). Per Kontraposition ist damit die gewünschte Aussage wahr. — Mehr Beispiele später . . .

Satz 2.5

Sei $n \in \mathbb{N}$. Dann gilt $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1)$.

Beweis. Dies ist ein Beispiel eines Beweises, bei dem es nicht nur um routine-mässiges Nachrechnen geht, sondern irgendeine Idee oder ein Trick verwendet werden muss.
Zum Umgang mit Summen führen wir zunächst die allgemeine Summenschreibweise ein: Sind $a_1, \ldots, a_n$ ganze Zahlen, so schreiben wir

$$a_1 + a_2 + \ldots + a_n = \sum_{i=1}^{n} a_i.$$

Mit $a_i = i$ für $i = 1, \ldots, n$ wollen wir also eine Formel für folgende Summe finden:

$$S := 1 + 2 + \ldots + n = \sum_{i=1}^{n} i.$$

Der ”Trick” dieses Beweises besteht nun darin, auszunutzen, dass man die Reihenfolge in einer Summe von ganzen Zahlen beliebig ändern kann.
Also gilt auch $S = n + (n-1) + \ldots + 2 + 1$. Der i-te Term in dieser Summe ist gegeben durch $b_i = n + 1 - i$; damit erhalten wir

$$S = \sum_{i=1}^{n} b_i = \sum_{i=1}^{n} (n + 1 - i).$$

Nun bilden wir

$$\begin{aligned} 2S = S + S &= (a_1 + a_2 + \ldots + a_n) + (b_1 + b_2 + \ldots + b_n) \\ &= (a_1 + b_1) + (a_2 + b_2) + \ldots + (a_n + b_n) \qquad \text{(noch einmal der Trick!)} \\ &= \sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} \big(i + (n + 1 - i)\big) = \sum_{i=1}^{n} (n+1) = n(n+1). \end{aligned}$$

Damit ist $2S = n(n+1)$, also $S = \frac{1}{2}n(n+1)$, wie gewünscht. □

Zur Erinnerung: natürliche und ganze Zahlen sind angeordnet

$$\ldots < -4 < -3 < -2 < -1 < 0 < 1 < 2 < 3 < 4 < \ldots$$

Formal: Für $a, b \in \mathbb{Z}$ gilt $a \leqslant b$, wenn es ein $c \in \mathbb{N}_0$ gibt mit $b = a + c$.

Zum Beispiel gilt $kn \geqslant n$ für alle $k, n \in \mathbb{N}$.
(Denn: Ist $k \in \mathbb{N}$, so ist $k - 1 \geqslant 0$ und damit $kn = n + \underbrace{(k-1)n}_{\geqslant 0} \geqslant n$.)

Die folgende Eigenschaft erscheint intuitiv einsichtig; sie wird explizit als ”Axiom” formuliert, damit wir darauf verweisen und präzise damit argumentieren können.

Peano's Induktionsaxiom

Jede nicht-leere Teilmenge von $\mathbb{N}_0$ besitzt ein kleinstes Element. Oder, anders ausgedrückt mit Hilfe der Formelsprache in §1:

$$\forall\, A \in \mathcal{P}(\mathbb{N}_0): \quad A \neq \varnothing \quad \Rightarrow \quad \big(\exists\, a \in A: \quad \big(\forall\, b \in A: a \leqslant b\big)\big).$$

Als erste Anwendung dieses Axioms zeigen wir eine Aussage über die ***rationalen Zahlen*** $\mathbb{Q}$. Zur Erinnerung:

- Jedes $x \in \mathbb{Q}$ lässt sich schreiben als Bruch $x = n/m$ mit $n \in \mathbb{Z}$ und $m \in \mathbb{N}$.
- Zwei solche Brüche n/m und n'/m' sind gleich, wenn es ein $k \in \mathbb{N}$ gibt mit $n' = kn$ und $m' = km$, d.h., n/m entsteht aus n'/m', indem der Faktor k im Zähler und im Nenner gekürzt wird. (Beispiel: $x = 2/3 = 4/6 = 100/150$.)
- Sei $x \in \mathbb{Q}$. Wir schreiben $x \geqslant 0$, falls $x = n/m$ mit $n \in \mathbb{N}_0$ und $m \in \mathbb{N}$.
  Sind $x, y \in \mathbb{Q}$, so schreibe $x \leqslant y$ falls $y - x \geqslant 0$ $\rightsquigarrow$ Anordnung von $\mathbb{Q}$.

Lemma 2.6

Sei $x \in \mathbb{Q}$. Dann lässt sich x als ein Bruch $x = n/m$ (mit $n \in \mathbb{Z}$, $m \in \mathbb{N}$) schreiben, der gekürzt ist, d.h., es gibt keine natürliche Zahl $k > 1$ mit $k \mid n$ und $k \mid m$.

Im Beispiel oben ist $2/3$ gekürzt, $4/6$ und $100/150$ sind nicht gekürzt.

Beweis. Zu $x \in \mathbb{Q}$ definieren wir $A := \{m \in \mathbb{N} \mid mx \in \mathbb{Z}\} \subseteq \mathbb{N}_0$.
Dann ist $A \neq \varnothing$, denn schreiben wir $x = n'/m'$ mit $n' \in \mathbb{Z}$ und $m' \in \mathbb{N}$, so gilt $m'x = n'$, also ist $m' \in A$.
Nach Peano's Induktionsaxiom besitzt A ein kleinstes Element; sei dieses m_0.
Es gilt also $m_0 \leqslant m$ für alle $m \in A$, und m_0 gehört selbst zu A, d.h., setzen wir $n_0 := m_0 x$, so gilt $n_0 \in \mathbb{Z}$. Damit folgt zunächst $x = n_0/m_0$.
Wir behaupten nun, dass dieser Bruch $x = n_0/m_0$ gekürzt ist.

Sei also $k \in \mathbb{N}$ mit $k \mid n_0$ und $k \mid m_0$. Dann schreiben wir $n_0 = kn_1$ und $m_0 = km_1$, mit $n_1 \in \mathbb{Z}$ und $m_1 \in \mathbb{N}$. Nun ist $x = n_0/m_0 = (kn_1)/(km_1) = n_1/m_1$, also $m_1 x = n_1 \in \mathbb{Z}$ und damit $m_1 \in A$. Da m_0 das kleinste Element von A ist, gilt $m_0 \leqslant m_1$. Andererseits ist $m_0 = km_1$ und damit $m_0 \geqslant m_1$.
Also folgt $m_1 = m_0 = km_1$. Mit der Kürzungsregel (Lemma 2.4) folgt $k = 1$.
D.h., der Bruch n_0/m_0 ist gekürzt. □

Hier ist nun das klassische Beispiel eines Widerspruchsbeweises.

Satz 2.7 (Euklid, etwa 3. Jahrhundert v. Chr.)

Es gibt keine positive rationale Zahl $x \in \mathbb{Q}$ mit $x^2 = 2$.

Beweis. Nehmen wir an, es gibt doch ein $x \in \mathbb{Q}$ mit $x > 0$ und $x^2 = 2$. Wir versuchen, einen Widerspruch zu einer bekannten Aussage zu produzieren.

Nach Lemma 2.6 gibt es eine gekürzte Bruchdarstellung $x = n/m$ mit $n, m \in \mathbb{N}$. Dann ist $2 = x^2 = (n/m)^2 = n^2/m^2$. Multiplizieren auf beiden Seiten mit m^2 ergibt $2m^2 = n^2$. Nun ist $2m^2$ gerade, also auch n^2. Mit Lemma 2.3(b) folgt, dass n auch selbst gerade ist, also gilt $n = 2l$ mit einem $l \in \mathbb{N}$. Dann ist aber $2m^2 = n^2 = (2l)^2 = 4l^2$. Hier können wir eine 2 auf beiden Seiten kürzen (siehe Lemma 2.4) und erhalten $m^2 = 2l^2$. Wie vorher folgt, dass m^2 gerade und dann auch m selbst gerade ist. Also sind n und m gerade, d.h., durch $k = 2$ teilbar, im Widerspruch zur Annahme, dass $x = n/m$ gekürzt ist. □

Satz 2.8 (Teilen mit Rest)

Sei $n \in \mathbb{Z}$ und $m \in \mathbb{N}$. Dann gibt es $q, r \in \mathbb{Z}$ mit $n = qm + r$ und $0 \leqslant r < m$.
Hierbei sind q, r eindeutig bestimmt. (Ist $n \geqslant 0$, so ist auch $q \geqslant 0$.)

Beispiel. Für die Division von 17 mit Rest durch 5 erhalten wir:

$$17 = 3 \cdot 5 + 2, \qquad \text{also} \quad q = 3 \text{ und } r = 2.$$

(Dazu zieht man so lange 5 von 17 ab, bis noch etwas $\geqslant 0$ herauskommt.)
Für die Division von -17 mit Rest durch 5 erhalten wir:

$$-17 = (-4) \cdot 5 + 3, \qquad \text{also} \quad q = -4 \text{ und } r = 3.$$

(Dazu addiert man so lange 5 zu -17, bis man eine Zahl $\geqslant 0$ erhält.)

Bemerkung. Sei $n \in \mathbb{Z}$ und $m \in \mathbb{N}$. Ist $n = qm + r$ wie oben in Satz 2.8, so wird der "Rest" r auch mit $n \bmod m$ bezeichnet. Diese "$\bmod$" Funktion ist eine grundlegende arithmetische Operation; es gibt sie auch in den meisten modernen Programmierspachen, zum Beispiel `17 % 5` in Python oder C.

Jetzt der allgemeine **Beweis.** Sei zuerst $n \geqslant 0$. Dann betrachten wir die Menge

$$A := \{r \in \mathbb{N}_0 \mid \exists q \in \mathbb{N}_0 : \ r = n - qm\}.$$

Diese Menge ist nicht leer, denn z.B. können wir $q = 0$ setzen und erhalten $r = n - 0 \cdot m = n \in A$. Nach Peano besitzt A also ein kleinstes Element; sei dieses r_0. Dazu gibt es ein $q_0 \in \mathbb{N}$ mit $r_0 = n - q_0 m$. Es gilt also $n = q_0 m + r_0$ und $r_0 \geqslant 0$. Wir müssen noch zeigen, dass auch $r_0 < m$ gilt.

Annahme, es wäre $r_0 \geqslant m$. Dann ist aber

$$r := n - (q_0 + 1)m = n - q_0 m - m = r_0 - m \geqslant 0.$$

also auch $r \in A$. Aber $r = r_0 - m < r_0$, und damit haben wir einen Widerspruch dazu, dass r_0 das kleinste Element von A ist. Also war die Annahme falsch, d.h., es gilt $n = q_0 m + r_0$ mit $q_0, r_0 \in \mathbb{N}_0$ und $0 \leqslant r_0 < m$.

Sei nun $n < 0$. Dann ist $-n > 0$, also wissen wir bereits, dass es $q_1, r_1 \in \mathbb{Z}$ gibt mit $-n = q_1 m + r_1$ und $0 \leqslant r_1 < m$. Dann ist $n = (-q_1)m - r_1$. Ist $r_1 = 0$, so sind wir fertig (mit $q := -q_1$ und $r := r_1 = 0$). Ist $r_1 \geqslant 1$, so erhalten wir

$$n = (-q_1)m - r_1 = (-q_1)m - m + m - r_1 = (-q_1 - 1)m + (m - r_1).$$

Mit $q := -q_1 - 1$ und $r := m - r_1$ ist $n = qm + r$ und $1 \leqslant r < m$, wie gewünscht.

Also gibt es in jedem Fall eine Darstellung $n = qm + r$ mit $0 \leqslant r < m$.

Nur zur Eindeutigkeit von q, r: Es gelte also auch $n = q'm + r'$ mit $q', r' \in \mathbb{Z}$ und $0 \leqslant r' < m$. Behauptung: $q = q'$.
Annahme, dies wäre falsch, also $q \neq q'$, d.h., $q < q'$ oder $q > q'$. Sei zuerst $q < q'$. Dann ist $q' - q > 0$ und damit $(q' - q)m \geqslant m$. Mit $qm + r = n = q'm + r'$ folgt auch $r - r' = q'm - qm = (q' - q)m \geqslant m$. Andererseits ist $r - r' \leqslant r < m$, Widerspruch. Analog erhält man einen Widerspruch für $q > q'$. Also war die Annahme falsch, d.h., es gilt $q = q'$ und damit auch $r = n - qm = n - q'm = r'$. □

Eine Anwendung: Prüfziffern (Beispiel IBAN)

Deutsches Bankkonto
Konto-Nr. 0356843503
BLZ 37010050

$\rightsquigarrow$ IBAN: DE12 $\underbrace{37010050}_{\text{BLZ}}\underbrace{0356843503}_{\text{Konto-Nr.}}$

DE steht für das Land, die Prüfziffer 12 wird nach folgendem Verfahren berechnet:

- Schreibe BLZ, gefolgt von Konto-Nr., Land und 00: 370100500356843503DE00.
- Wandle Buchstaben in Zahlen um:

A	B	C	D	$\ldots$	Z
10	11	12	13	$\ldots$	35

- Berechne $370100500356843503131400 \bmod 97 = 86$; ziehe dies von 98 ab; Ergebnis ist 12. (Falls Ergebnis einstellig, ergänze führende Null.)

(Siehe `https://de.wikipedia.org/wiki/Internationale_Bankkontonummer`)

Umgekehrt: Validierung einer IBAN

DE12370100500356843503 $\rightsquigarrow$
370100500356843503DE12 $\rightsquigarrow$
370100500356843503131412 $\bmod 97 = 1$
Kommt als Ergebnis nicht 1 heraus, wird die IBAN nicht akzeptiert.

(Illustration mit GAP.)

Weiteres Beispiel: Formeln zur (relativ komplizierten!) Berechnung des Osterdatums $\rightsquigarrow$ Übung 2.

§3 Vollständige Induktion und Primzahlen

In der oben formulierten Fassung ist Peano's Induktionsaxiom oftmals etwas umständlich. Sehr nützlich ist folgende Variante.

Satz 3.1 (Vollständige Induktion)

Sei $n_0 \in \mathbb{N}_0$ fest und für jedes $n \in \mathbb{N}_0$ mit $n \geqslant n_0$ eine Aussage $P(n)$ gegeben. Die folgenden beiden Voraussetzungen seien erfüllt:

(I1) Induktionsanfang. $P(n_0)$ ist wahr.

(I2) Induktionsschritt. $\forall n \in \mathbb{N}_0 : (n \geqslant n_0$ und $P(n)$ wahr$) \Rightarrow P(n+1)$ wahr.

Dann ist $P(n)$ wahr für alle $n \in \mathbb{N}_0$ mit $n \geqslant n_0$.

Beweis. Wir zeigen dies wieder mit einem Widerspruchbeweis. Angenommen, es gäbe ein $n \in \mathbb{N}_0$ mit $n \geqslant n_0$ und so, dass $P(n)$ falsch ist. Dann ist

$$A := \{n \in \mathbb{N}_0 \mid n \geqslant n_0 \text{ und } P(n) \text{ ist falsch}\} \neq \varnothing.$$

Nach Peano's Induktionsaxiom besitzt A ein kleinstes Element; sei dieses k. Wegen (I1) ist $k > n_0$. Dann ist $k-1 \geqslant n_0$ und $k-1 \notin A$, d.h., $P(k-1)$ ist wahr. Wende (I2) auf $n = k-1$ an. Es folgt, dass auch $P(k)$ wahr ist, Widerspruch. □

Als Beispiel geben wir einen neuen Beweis von Satz 2.5, wobei wir für $n \in \mathbb{N}$ die folgende Aussage betrachten:

$$P(n): \quad 1+2+\ldots+n = \tfrac{1}{2}n(n+1).$$

Startwert ist hier $n_0 = 1$. Wir müssen nun nachweisen, dass die Voraussetzungen (I1) und (I2) erfüllt sind.

Zu (I1), Induktionsanfang: Ist $n = n_0 = 1$, so ist die linke Seite von $P(1)$ gleich 1 und die rechte Seite gleich $\frac{1}{2}(1+1) = 1$. Also ist $P(1)$ wahr.

Zu (I2), Induktionsschritt: Sei $n \in \mathbb{N}_0$ mit $n \geqslant n_0 = 1$ beliebig. Wir nehmen an, dass $P(n)$ wahr ist und müssen dann zeigen, dass auch $P(n+1)$ wahr ist.

Beginnen wir mit der linken Seite von $P(n+1)$ und formen diese um:

$$\begin{aligned} 1+2+\ldots+(n+1) &= (1+2+\ldots+n)+(n+1) \\ &= \tfrac{1}{2}n(n+1)+(n+1) \quad \text{(da } P(n) \text{ als wahr vorausgesetzt ist),} \\ &= \tfrac{1}{2}(n^2+n)+\tfrac{1}{2}(2n+2) = \tfrac{1}{2}(n^2+3n+2). \end{aligned}$$

Andererseits ist die rechte Seite von $P(n+1)$ gleich

$$\tfrac{1}{2}(n+1)\big((n+1)+1\big) = \tfrac{1}{2}(n+1)(n+2) = \tfrac{1}{2}(n^2+3n+2).$$

Also erhalten wir das gleiche Ergebnis wie voher; damit ist (I2) gezeigt. Mit Satz 3.1 folgt also, dass $P(n)$ für alle $n \geqslant 1$ wahr ist.

Bemerkung. Wir sehen hier gleichzeitig eine Stärke und eine Schwäche der vollständigen Induktion. Ist bereits bekannt, was man zeigen will, so ist vollständige Induktion eine sehr effiziente Beweismethode. Wenn man allerdings die Formel noch nicht kennt und erst herausfinden muss, so benötigt man in der Tat einen "Trick" – wie im ursprünglichen Beweis von Satz 2.5. Versuchen Sie etwa, Formeln für $1^2+2^2+\cdots+n^2$ und $1^3+2^3+\cdots+n^3$ zu finden.

Die folgende Variante der vollständigen Induktion ist ebenfalls sehr oft nützlich.

Satz 3.2 (Starke vollständige Induktion)

Sei $n_0 \in \mathbb{N}_0$ fest und für jedes $n \in \mathbb{N}_0$ mit $n \geqslant n_0$ eine Aussage $P(n)$ gegeben. Die folgenden beiden Voraussetzungen seien erfüllt:

(SI1) $P(n_0)$ ist wahr.

(SI2) $\forall n \in \mathbb{N}_0 : (P(m)$ wahr für $n_0 \leqslant m < n) \Rightarrow P(n)$ wahr.

Dann ist $P(n)$ wahr für alle $n \in \mathbb{N}_0$ mit $n \geqslant n_0$.

Beweis. Wir brauchen nur den obigen Beweis von Satz 3.1 etwas zu modifizieren. Nehmen wir wieder an, es wäre

$$A := \{n \in \mathbb{N}_0 \mid n \geqslant n_0 \text{ und } P(n) \text{ ist falsch}\} \neq \varnothing.$$

Nach Peano besitzt A ein kleinstes Element; sei dieses k. Wegen (SI1) ist $k > n_0$. Sei nun $m \in \{n_0, n_0+1, \ldots, k-1\}$. Dann ist $m \notin A$, d.h., $P(m)$ ist wahr. Mit (SI2) angewandt auf $n = k$ folgt, dass auch $P(k)$ wahr ist, Widerspruch. □

Definition 3.3

Sei $n \in \mathbb{N}$, $n \geqslant 2$. Dann heißt n eine ***Primzahl***, wenn n nur durch 1 und sich selbst teilbar ist.

Zum Beispiel sind $2, 3, 5, 7, 11$ Primzahlen, aber 1 und 12 sind keine Primzahlen.

Satz 3.4

Sei $n \in \mathbb{N}$, $n \geqslant 2$. Dann lässt sich n als Produkt von Primzahlen schreiben; es gibt also $r \geqslant 1$ Primzahlen $p_1, p_2, \ldots, p_r$ mit $n = p_1 p_2 \cdots p_r$ und $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_r$.

Eine solche Produktdarstellung nennen wir eine ***Primfaktorzerlegung*** von n.

Beweis. (Starke Induktion mit $n_0 = 2$.) Für $n \geqslant 2$ betrachten wir die Aussage:

$P(n)$: "n ist Produkt von Primzahlen".

Wir müssen zeigen, dass die Voraussetzungen (SI1) und (SI2) erfüllt sind.

Zu (SI1): Sei also $n = n_0 = 2$. Da 2 eine Primzahl ist, ist $n = 2$ offenbar auch ein Produkt von Primzahlen (mit nur einem Faktor).

Zu (SI2): Sei $n > 2$ und vorausgesetzt, dass $P(m)$ wahr ist für $m = 2, 3, \ldots, n-1$. Wir müssen dann zeigen, dass $P(n)$ wahr ist. Dazu unterscheiden wir zwei Fälle.

1. Fall: n ist selbst eine Primzahl. Dann ist (siehe oben) n offenbar auch ein Produkt von Primzahlen (mit nur einem Faktor), also die Behauptung gezeigt.

2. Fall: n ist keine Primzahl. Nach Definition einer Primzahl bedeutet dies, dass $n = ab$ gilt mit $a, b \in \mathbb{N}$ und $2 \leqslant a, b \leqslant n-1$. Nach Voraussetzung sind $P(a)$ und $P(b)$ wahr, also sind a und b Produkte von Primzahlen. Wir schreiben $a = p_1 p_2 \cdots p_r$ und $b = q_1 q_2 \cdots q_s$ mit $r, s \geqslant 1$ und Primzahlen p_i, q_j.
Dann ist aber auch $n = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$ ein Produkt von Primzahlen (mit $r + s$ Faktoren).

Schließlich sortieren wir noch im Endprodukt die Faktoren so um, dass sie der Größe nach geordnet sind. □

Satz 3.5 (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis. Dies ist wieder ein klassisches Beispiel eines Widerspruchsbeweises.
Angenommen, es gäbe nur endlich viele Primzahlen; seien diese $p_1, p_2, \ldots, p_r$.
Damit bilden wir $N := p_1 p_2 \cdots p_r + 1 \in \mathbb{N}$. (Dies ist der Trick des Beweises.)
Es gilt sicherlich $N \geqslant 2$, also besitzt N nach Satz 3.4 eine Primfaktorzerlegung.
In dieser können aber nur die Primzahlen $p_1, \ldots, p_r$ vorkommen, und mindestens eine kommt vor. Es gibt also ein $i \in \{1, \ldots, r\}$ mit $p_i \mid N$.
Andererseits ist $N - 1 = p_1 p_2 \cdots p_r$, also gilt $p_i \mid N - 1$. Mit Lemma 2.2(b) folgt dann aber auch $p_i \mid N - (N-1) = 1$, also $p_i = 1$, Widerspruch. □

Bemerkung. Für $n \in \mathbb{N}$ sei p_n die n-te Primzahl. Zum Beispiel $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, …, $p_{100} = 541$, … Es ist keine allgemeine Formel bekannt, mit der man zu beliebigem n die entsprechende Primzahl p_n berechnen könnte.
PIERRE DE FERMAT vermutete um 1640, dass

$$F_n := 2^{2^n} + 1 \quad \text{eine Primzahl ist für alle } n \in \mathbb{N}_0.$$

n	F_n	
0	3	ok
1	5	ok
2	17	ok
3	257	ok
4	65537	ok
5	$2^{32} + 1 = 4294967297$	nicht ok: $641 \cdot 6700417$ (LEONHARD EULER 1732)

Es ist bekannt, dass $F_5, \ldots, F_{32}$ keine Primzahlen sind.
Für größere Werte von n ist nicht bekannt, ob F_n eine Primzahl ist oder nicht.

Lemma 3.6 (“Lemma von Euklid”)

Sei $p \in \mathbb{N}$ eine Primzahl und seien $a, b \in \mathbb{N}$. Gilt $p \mid ab$, so folgt $p \mid a$ oder $p \mid b$.

Das Lemma von Euklid kommt in nahezu jeder Argumentation mit Primzahlen vor; es ist genau das “richtige” technische Hilfsmittel.

Beispiel. In Lemma 2.3 haben wir gezeigt: “n ungerade $\Rightarrow n^2$ ungerade” und dann mit Kontraposition geschlossen: “n^2 gerade $\Rightarrow n$ gerade”. Mit dem Lemma von Euklid folgt dies auch direkt: Ist n^2 gerade, so gilt $2 \mid n^2 = nn$, also folgt $2 \mid n$.

Beweis. Seien $a, b \in \mathbb{N}$ gegeben mit $p \mid ab$. Nehmen wir an, es gilt $p \nmid a$. Dann müssen wir $p \mid b$ zeigen. Da p nur die Teiler 1 und p hat, ist $\mathrm{ggT}(p, a) = 1$ oder p. Also $\mathrm{ggT}(p, a) = 1$ wegen $p \nmid a$. Nach dem Lemma von Bézout (siehe Ü2) gibt es $r, s \in \mathbb{Z}$ mit $1 = rp + sa$. Multiplikation mit b ergibt $b = rpb + sab$. Wegen $p \mid rpb$ und $p \mid sab$ folgt mit Lemma 2.2, dass auch $p \mid rpb + sab = b$ gilt. □

Folgerung 3.7

Sei $p \in \mathbb{N}$ eine Primzahl, $n \in \mathbb{N}$ und seien $c_1, \ldots, c_n \in \mathbb{N}$.
Gilt $p \mid c_1 c_2 \cdots c_n$, so gibt es ein $i \in \{1, \ldots, n\}$ mit $p \mid c_i$.

Beweis. (Vollständige Induktion über n mit Startwert $n_0 = 1$.)
Induktionsanfang. Sei $n = 1$, also ist nur eine Zahl c_1 gegeben mit $p \mid c_1$. Dann gilt die Aussage. (Es ist nichts zu zeigen.)
Induktionsschritt. Sei $n \geqslant 1$ und angenommen, dass die Aussage bereits für n Zahlen gilt. Dann müssen wir zeigen, dass sie auch für $n+1$ Zahlen gilt. Gegeben seien also $c_1, \ldots, c_{n+1} \in \mathbb{N}$ mit $p \mid c_1 c_2 \ldots c_{n+1}$. Setze nun $a := c_1 c_2 \cdots c_n$. Dann ist $c_1 c_2 \cdots c_{n+1} = a c_{n+1}$ und $p \mid a c_{n+1}$. Nach Lemma 3.6 folgt also $p \mid a$ oder $p \mid c_{n+1}$. Im 2. Fall sind wir fertig. Im 1. Fall gilt $p \mid c_1 \cdots c_n$, also gibt es nach Induktionsannahme ein $i \in \{1, \ldots, n\}$ mit $p \mid c_i$, und wir sind wieder fertig. □

Satz 3.8 (Hauptsatz der elementaren Arithmetik)

Die Primfaktorzerlegung einer natürlichen Zahl $n \geqslant 2$ (siehe Satz 3.4) ist eindeutig.

Beweis. (Starke Induktion mit Startwert $n_0 = 2$.) Für $n \in \mathbb{N}$, $n \geqslant 2$, ist folgende Aussage $P(n)$ zu beweisen:
“Gegeben seien Primzahlen $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_r$ und $q_1 \leqslant q_2 \leqslant \ldots \leqslant q_s$ (wobei $r, s \geqslant 1$) mit $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$. Dann gilt $r = s$ und $p_i = q_i$ für $1 \leqslant i \leqslant r$.”

Induktionsanfang. Sei $n = 2$. Dann ist n selbst eine Primzahl, und die Aussage ist klar nach Definition einer Primzahl.

Induktionsschritt. Sei $n > 2$ und angenommen, dass $P(m)$ bereits gilt für alle m mit $2 \leqslant m < n$. Dann müssen wir zeigen, dass auch $P(n)$ gilt. Ist n selbst eine Primzahl, so ist die Aussage wieder klar nach Definition einer Primzahl. Sei also nun n keine Primzahl und betrachten wir zwei Faktorisierungen wie oben:

$$(*) \qquad n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \qquad (\text{mit } r, s \geqslant 2).$$

Wir unterscheiden jetzt 3 Fälle.

1. Fall: $p_1 = q_1$. Dann können wir p_1 auf beiden Seiten kürzen und erhalten $m := p_2 \cdots p_r = q_2 \cdots q_s$. Wegen $2 \leqslant m < n$ ist $P(m)$ nach Induktionsannahme wahr, also $r = s$ und $p_i = q_i$ für $2 \leqslant i \leqslant r$. Da auch $p_1 = q_1$ gilt, ist also $P(n)$ wahr.

2. Fall: $p_1 < q_1$. Nun ist $p_1 \mid p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, also gibt es nach Folgerung 3.7 ein $i \in \{1, \ldots, s\}$ mit $p_1 \mid q_i$. Aber p_1 und q_i sind Primzahlen, also muss $p_1 = q_i$ gelten. Andererseits ist $p_1 < q_1 \leqslant q_2 \leqslant \ldots \leqslant q_i$, also $p_1 < q_i$, Widerspruch.

3. Fall: $p_1 > q_1$. Dies führt völlig analog zum 2. Fall auf einen Widerspruch. (Es ist $q_1 \mid p_1 \cdots p_r$ usw.)

Also treten der 2. und 3. Fall gar nicht auf. □

§4 Relationen und Restklassen

Wir führen eine weitere grundlegende mengentheoretische Konstruktion ein. Das ***kartesische Produkt*** von zwei nicht-leeren A und B wird mit $A \times B$ bezeichnet. Dies ist eine Menge, die aus allen Paaren (a, b) mit $a \in A$ und $b \in B$ besteht:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Für zwei solche Paare (a, b) und (a', b') gilt $(a, b) = (a', b')$ genau dann, wenn $a = a'$ und $b = b'$ gelten. (Formal korrekt wird das Paar (a, b) als die Menge $\{a, \{a, b\}\}$ definiert.) Zum Beispiel ist

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

Beachten Sie, dass die Reihenfolge wichtig ist: $(2, 4)$ ist nicht das Gleiche wie $(4, 2)$. Sie sind vermutlich vertraut mit dem kartesischen Produkt $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, das man sich üblicherweise als Ebene mit 2 Koordinatenachsen vorstellt.

Definition 4.1

Sind A, B nicht-leere Mengen, so heißt eine Teilmenge $R \subseteq A \times B$ eine ***Relation*** auf A und B. Für $a \in A$ und $b \in B$ schreiben wir $a \sim b$, wenn $(a, b) \in R$ gilt (und sagen: "a steht in Relation zu b"). Ist $A = B$, so heißt R eine Relation auf A.

Beispiel 4.2

(a) Sei A die Menge aller Punkte der Ebene und B die Menge aller Geraden in der Ebene. Die Eigenschaft, dass ein Punkt auf einer Geraden liegt, definiert eine Relation: $R = \{(a, b) \in A \times B \mid \text{Der Punkt } a \text{ liegt auf der Geraden } b\}$.

(b) Hier sind Beispiele von Relationen auf $A = B = \mathbb{Z}$:

$$R_1 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n < m\},$$
$$R_2 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n \text{ teilt } m\},$$
$$R_3 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n = m \text{ oder } n + m \geqslant 0\}.$$

Beispiel 4.3

Sei wieder $A = B = \mathbb{Z}$. Für festes $m \in \mathbb{N}$ definieren wir die Relation

$$R_m := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \bmod m = b \bmod m\}.$$

Es gilt hier also $a \sim b$ genau dann, wenn a und b den gleichen Rest bei Division durch m haben. Wir behaupten, dass diese Relation auch wie folgt charakterisiert werden kann:

$$(a, b) \in R_m \quad \Leftrightarrow \quad m \mid b - a. \qquad (*)$$

Beweis von $(*)$: Seien $a, b \in \mathbb{Z}$. Es gibt $q, q', r, r' \in \mathbb{Z}$ mit $a = qm + r$, $b = q'm + r'$ und $0 \leqslant r, r' < m$. Zu zeigen: $r = r' \Leftrightarrow m \mid b - a$.

"$\Rightarrow$" Ist $r = r'$, so folgt $a - qm = r = r' = b - q'm$ und damit $b - a = (q' - q)m$. Also ist $m \mid b - a$.

"$\Leftarrow$" Ist $m \mid b - a$, so gilt $b - a = cm$ mit $c \in \mathbb{Z}$, also $b = cm + a = cm + qm + r = (c + q)m + r$. Aus der Eindeutigkeit des Restes folgt also $r = r'$. □

Anstelle von $(n, n') \in R_m$ schreiben wir künftig $n \equiv n' \pmod m$.
Dies wird gelesen als: "n und n' sind ***kongruent modulo*** m."
Ist etwa $m = 2$ und $n \in \mathbb{Z}$ beliebig, so ist der Rest $n \bmod 2$ entweder 0 oder 1. Also:

$$n \bmod 2 = 0 \quad \Leftrightarrow \quad n \equiv 0 \pmod 2 \quad \Leftrightarrow \quad n \text{ ist gerade},$$
$$n \bmod 2 = 1 \quad \Leftrightarrow \quad n \equiv 1 \pmod 2 \quad \Leftrightarrow \quad n \text{ ist ungerade}.$$

Definition 4.4

Sei A eine nicht-leere Menge und $R \subseteq A \times A$ eine Relation auf A, geschrieben $a \sim b$ für $a, b \in A$. Die Relation R heißt:

- ***reflexiv***, wenn $a \sim a$ für alle $a \in A$ gilt;
- ***symmetrisch***, wenn für $a, b \in A$ aus $a \sim b$ stets $b \sim a$ folgt;
- ***transitiv***, wenn für $a, b, c \in A$ aus $a \sim b$ und $b \sim c$ stets $a \sim c$ folgt.

Ist R reflexiv, symmetrisch und transitiv, so heißt R eine ***Äquivalenzrelation***.

Beispiel 4.5

(a) Sei $A = \mathbb{Z}$ und betrachte die Relationen R_1, R_2, R_3 in Beispiel 4.2(b).
$R_1 = \{(n,m) \in \mathbb{Z} \times \mathbb{Z} \mid n < m\}$ ist transitiv, aber weder reflexiv noch symmetrisch;
$R_2 = \{(n,m) \in \mathbb{Z} \times \mathbb{Z} \mid \ n$ teilt $m\}$ ist transitiv, reflexiv aber nicht symmetrisch;
$R_3 = \{(n,m) \in \mathbb{Z} \times \mathbb{Z} \mid \ n = m$ oder $n + m \geqslant 0\}$ ist reflexiv, symmetrisch, aber nicht transitiv (denn z.B. $(-1,2) \in R_3$, $(2,0) \in R_3$, aber $(-1,0) \notin R_3$).

(b) Sei $A = \mathbb{Z}$ und $m \in \mathbb{N}$ fest. Die Kongruenz-Relation R_m in Beispiel 4.3 ist

- reflexiv, denn $m \mid a - a = 0$, also $a \sim a$;
- symmetrisch, denn aus $a \sim b$ folgt $m \mid b - a$ und damit auch $m \mid -(b-a) = a - b$ (siehe Lemma 2.2(b)), also $b \sim a$;
- transitiv, denn aus $a \sim b$ und $b \sim c$ folgt $m \mid b - a$ und $m \mid c - b$; also auch $m \mid (c-b) - (b-a) = c - a$ (siehe Lemma 2.2(b)) und damit $a \sim c$.

Also ist R_m eine Äquivalenzrelation.

Definition 4.6

Sei $R \subseteq A \times A$ eine Äquivalenzrelation. Für $a \in A$ heißt dann
$$K(a,R) := \{b \in A \mid (a,b) \in R\}$$
die ***Äquivalenzklasse*** von a. Dies ist also eine Teilmenge von A, d.h., ein Element von $\mathcal{P}(A)$. Sei $\mathcal{K}(A,R)$ die Menge aller Äquivalenzklassen von Elementen in A, d.h., $\mathcal{K}(A,R) = \{S \in \mathcal{P}(A) \mid \exists a \in A : S = K(a,R)\}$

Sei zum Beispiel A die Menge aller Menschen auf dem Planeten Erde und
$$R = \{(a,b) \in A \times A \mid a \text{ und } b \text{ leben im gleichen Land}\}.$$
Sie überprüfen leicht, dass dies eine Äquivalenzrelation ist. Eine Äquivalenzklasse besteht genau aus allen Menschen, die in einem Land leben. Die Menge der Äquivalenzklassen entspricht also den verschiedenen Ländern.
In Beispiel 4.3 mit $m = 2$ ist $K(0,R_2) =$ Menge aller geraden Zahlen und $K(1,R_2) =$ Menge aller ungeraden Zahlen. Also $\mathcal{K}(\mathbb{Z},R_2) = \{K(0,R_2), K(1,R_2)\}$.

Satz 4.7

Sei $R \subseteq A \times A$ eine Äquivalenzrelation. Dann gilt:
(a) Jedes $a \in A$ liegt in einer Äquivalenzklasse.
(b) Zwei Äquivalenzklassen sind entweder gleich oder disjunkt.
("disjunkt" bedeutet: der Durchschnitt ist leer).

Beweis. (a) Sei $a \in A$. Da R reflexiv ist, gilt $a \sim a$ also $a \in K(a,R)$.
(b) Seien a, b und $K_a = K(a,R)$, $K_b = K(b,R)$. Nehmen wir an, es ist $K_a \cap K_b \neq \varnothing$. Dann müssen wir zeigen, dass $K_a = K_b$ gilt. Sei dazu $d \in K_a \cap K_b$. Ist $c \in K_a$ beliebig, so gilt $a \sim c$. Wegen $d \in K_a$ ist $a \sim d$ und wegen der Symmetrie dann auch $d \sim a$. Mit der Transitivität folgt $d \sim c$. Wegen $d \in K_b$ gilt $b \sim d$, also folgt mit der Transitivität schliesslich $b \sim c$, d.h., $c \in K_b$. Damit ist gezeigt, dass $K_a \subseteq K_b$ gilt. Auf völlig analoge Weise wird $K_b \subseteq K_a$ gezeigt. Also gilt $K_a = K_b$, wie behauptet. □

Für $a \in A$ sei $K_a = K(a,R) = \{b \in A \mid (a,b) \in R\}$ die Äquivalenzklasse von a.
Der letzte Satz zeigt: A ist Vereinigung aller Äquivalenzklassen.
Außerdem: In dieser Vereinigung sind im Allgemeinen viele Terme gleich.
Sind $a, b \in A$, so gilt $K_a = K_b$ genau dann, wenn $b \in K_a$.

Definition 4.8

Sei $R \subseteq A \times A$ eine Äquivalenzrelation. Eine Teilmenge $B \subseteq A$ heißt ***Repräsentantensystem der Äquivalenzklassen***, wenn es zu jedem $a \in A$ genau ein $b \in B$ gibt mit $(b,a) \in R$. Oder anders ausgedrückt:
$$A = \bigcup_{b \in B} K(b,R), \quad \text{und in dieser Vereinigung sind die Terme alle disjunkt.}$$

Beispiel 4.9 (Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$)

Sei $A = \mathbb{Z} \times \mathbb{N}$ und betrachte folgende Relation:
$$R := \{((n,m),(n',m')) \in A \times A \mid nm' = n'm\}.$$
Nach Ü3 ist dies eine Äquivalenzrelation.

Für $(n,m) \in A$ schreiben wir anstelle von $K((n,m),R)$ einfach kurz n/m.
Genauso wie in Lemma 2.6 zeigt man, dass jede Äquivalenzklasse ein *gekürztes* Paar (n,m) enthält, d.h., es gibt keine natürliche Zahl $k > 1$ mit $k \mid n$ und $k \mid m$.
Nach Ü3 ist ein Repräsentantensystem der Äquivalenzklassen gegeben durch

$$B := \{(n,m) \in A \mid (n,m) \text{ ist gekürzt}\},$$

d.h., die Äquivalenzklassen entspechen genau den ***rationalen Zahlen*** !
Auf diese Weise erhält man in der Tat eine mathematisch korrekte Konstruktion:

Man definiert $\quad \mathbb{Q} := K(A,R).$

Eine Gleichheit wie $2/3 = 4/6 = 100/150$ entspricht dann einfach der Tatsache, dass die Paare $(2,3)$, $(4,6)$, $(100,150)$ zur gleichen Äquivalenzklasse gehören.
Ist $n \in \mathbb{Z}$, so schreiben wir einfach n anstelle von $n/1$. Vermöge dieser Identifizierung ist dann $\mathbb{Z} \subseteq \mathbb{Q}$. (Überlegen Sie sich selbst, wie man auf ähnliche Weise auch $\mathbb{Z}$ aus $\mathbb{N}$ konstruieren kann.)

Beispiel 4.10

Sei $A = \mathbb{Z}$ und $m \in \mathbb{N}$. Die Äquivalenzklassen bezüglich der Äquivalenzrelation R_m (siehe Beispiel 4.3) werden auch als ***Restklassen*** (modulo m) bezeichnet.
Sofern m fest vorgegeben ist, werden wir die Restklasse von $n \in \mathbb{Z}$ einfach mit $\overline{n}$ bezeichnen, also $\quad \overline{n} = \{a \in \mathbb{Z} \mid m \text{ teilt } n-a\} = \{a \in \mathbb{Z} \mid a \bmod m = n \bmod m\}$.

Repräsentantensystem ? Ein solches ist gegeben durch $B = \{0,1,2,\ldots,m-1\}$, denn bei der Division mit Rest durch m kommen nur die Reste $0,1,2,\ldots,m-1$ vor (und der Rest ist eindeutig bestimmt). Anders formuliert: Für jedes $n \in \mathbb{Z}$ gibt es genau ein $r \in B$ mit $n \bmod m = r$, also $n \in \overline{r}$ und $\overline{n} = \overline{r}$. Es gilt also

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \ldots \cup \overline{(m-1)} \qquad \text{(disjunkte Vereinigung)}.$$

Ist etwa $m = 5$, so gilt $\quad \mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}$.
Es ist $\quad -17 \in \overline{3} \quad$ und $\quad 38 \in \overline{3} \quad$ (weil -17 und 38 den Rest 3 modulo 5 haben).

Genauso, wie man Brüche (also letztlich gewisse Äquivalenzklassen) addieren und multiplizieren kann, werden wir sehen, dass man auch Restklassen modulo m addieren und multiplizieren kann. Grundlage dafür ist:

Lemma 4.11

Sei $m \in \mathbb{N}$. Wie oben bezeichnen wir die Restklasse (modulo m) von $n \in \mathbb{Z}$ mit $\overline{n}$.
Es seien nun beliebige $a,b,c,d \in \mathbb{Z}$ gegeben.
Gilt $\quad \overline{a} = \overline{c} \quad$ und $\quad \overline{b} = \overline{d}, \quad$ so folgt $\quad \overline{a+b} = \overline{c+d} \quad$ und $\quad \overline{ab} = \overline{cd}$.

Beweis. Sei $\overline{a} = \overline{c}$ und $\overline{b} = \overline{d}$, also $m \mid c-a$ und $m \mid d-b$. Seien $r,s \in \mathbb{Z}$ mit $c - a = rm$ und $d - b = sm$, also $c = a + rm$ und $d = b + sm$. Damit erhalten wir

$$(c+d) - (a+b) = (a+rm) + (b+sm) - a - b = rm + sm = (r+s)m,$$

also $m \mid (c+d) - (a+b)$, d.h., $\overline{a+b} = \overline{c+d}$. Ausserdem ist

$$\begin{aligned} cd - ab &= (a+rm)(b+sm) - ab = (ab + asm + rmb + rmsm) - ab \\ &= asm + rmb + rmsm = (as + rb + rsm)m, \end{aligned}$$

also $m \mid cd - ab$, d.h., $\overline{ab} = \overline{cd}$. □

Beispiel. Sei $m = 6$. Wir wollen $(17 \cdot 14) \bmod 6$ berechnen.
Dazu: Es gilt $17 \bmod 6 = 5$ und $14 \bmod 6 = 2$, also $\overline{17} = \overline{5}$ und $\overline{14} = \overline{2}$. Damit

$$\overline{17 \cdot 14} = \overline{5 \cdot 2} = \overline{10} = \overline{4}$$

wobei wir Lemma 4.11 für die 1. Gleichheit benutzt haben.
Also gilt $(17 \cdot 14) \bmod 6 = 4$.

Beispiel. Ist 7513 durch 3 teilbar ? Nach der (vielleicht bekannten) ***Dreierregel*** müssten wir uns dazu nur die Quersumme von 7513 anschauen:
Diese ist $\quad 7+5+1+3 = 16, \quad$ und wegen $\quad 3 \nmid 16 \quad$ folgt auch $\quad 3 \nmid 7513$.
Begründung: Sei $m = 3$ und betrachte $\overline{7513} = \overline{7 \cdot 1000 + 5 \cdot 100 + 1 \cdot 10 + 3}$.
Nun ist $\quad 10 \bmod 3 = 1, \quad$ also $\quad \overline{10} = \overline{1}$. $\quad$ Mit Lemma 4.11 folgt daher auch $\overline{100} = \overline{10 \cdot 10} = \overline{1 \cdot 1} = \overline{1}$. Genauso $\overline{1000} = \overline{10 \cdot 100} = \overline{1 \cdot 1} = \overline{1}$, und damit

$$\overline{7513} = \overline{7 \cdot 1000 + 5 \cdot 100 + 1 \cdot 10 + 3} = \overline{7 \cdot 1 + 5 \cdot 1 + 1 \cdot 1 + 3} = \overline{7+5+1+3} = \overline{16}.$$

D.h., die Zahl 7513 hat den gleichen Rest (modulo 3) wie ihre Quersumme.

§5 Abbildungen und die Mächtigkeit von Mengen

Definition 5.1

Seien A, B nicht-leere Mengen. Eine ***Abbildung*** f von A nach B ist eine Zuordnung, die jedem Element von A genau ein Element von B zuordnet.
Wir schreiben dies als $\quad f\colon A \to B, \qquad a \mapsto f(a).$

Das ***Bild*** von f ist definiert als $\mathrm{Bild}(f) := \{b \in B \mid \exists a \in A : f(a) = b\}$.
Für eine beliebige Teilmenge $A' \subseteq A$ sei $f(A') := \{b \in B \mid \exists a \in A' : f(a) = b\}$.
Damit ist also $\mathrm{Bild}(f) = f(A)$. Die Abbildung f heißt

- ***surjektiv***, wenn $f(A) = B$ gilt;
- ***injektiv***, wenn für alle $a, a' \in A$ gilt: Aus $f(a) = f(a')$ folgt $a = a'$.
  (Oder umgekehrt: Gilt $a \neq a'$, so auch $f(a) \neq f(a')$.)
- ***bijektiv***, wenn sie injektiv und surjektiv ist.

Bemerkung 5.2

(a) Implizit haben wir bereits Abbildungen betrachtet.
Zum Beispiel ist die Addition in $\mathbb{N}$ eine Abbildung $\alpha\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(n, n') \mapsto n + n'$.

(b) Ist $f\colon A \to B$ eine Abbildung, so heißt $\quad \mathcal{G}(f) := \{(a, f(a)) \mid a \in A\} \subseteq A \times B$ der ***Graph*** von f. Dies ist also eine Relation auf $A \times B$.

(c) Umgekehrt: Formal korrekt ist eine Abbildung $f\colon A \to B$ durch eine Relation $R \subseteq A \times B$ gegeben, welche folgende Bedingungen erfüllt:

(i) Zu jedem $a \in A$ gibt es ein $b \in B$ mit $(a, b) \in R$;

(ii) sind $a \in A$ und $b, b' \in B$ mit $(a, b) \in R$ und $(a, b') \in R$ gegeben, so folgt $b = b'$.

Diese beiden Bedingungen besagen gerade, dass zu jedem $a \in A$ genau ein $b \in B$ gehört, und dieses b wird dann mit $f(a)$ bezeichnet. Dann ist $R = \mathcal{G}(f)$.

Also: Eine Abbildung $f\colon A \to B$ ist eine Relation mit speziellen Eigenschaften.

Beispiel 5.3

(a) Die Abbildung $f\colon \mathbb{Z} \to \mathbb{Z}$, $n \mapsto n^2$, ist weder injektiv noch surjektiv, denn es gilt zum Beispiel $f(1) = 1 = f(-1)$ und $2 \notin f(\mathbb{Z})$.

(b) Sei $A = \{n \in \mathbb{Z} \mid n \text{ gerade}\}$ und $B = \{n \in \mathbb{Z} \mid n \text{ ungerade}\}$. Dann erhalten wir eine Abbildung $f\colon A \to B$, $n \mapsto n + 1$. Diese Abbildung ist bijektiv.
Injektivität: Seien $a, a' \in A$ mit $f(a) = f(a')$. Dann gilt also $a + 1 = a' + 1$ und damit $a = a'$. Surjektivität: Sei $b \in B$, also b ungerade. Dann ist $b - 1$ gerade, also $b - 1 \in A$. Es gilt $f(b - 1) = b$, also $b \in f(A)$.

(c) Die Abbildung $f\colon \mathbb{N}_0 \to \mathbb{N}_0$, $n \mapsto 2n$, ist injektiv aber nicht surjektiv.

(d) Seien $k, n \in \mathbb{N}_0$. Dann ist $2^k(2n + 1) \geqslant 1$, also $2^k(2n + 1) - 1 \in \mathbb{N}_0$. Damit erhalten wir eine Abbildung
$$f\colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0, \qquad (k, n) \mapsto 2^k(2n + 1) - 1.$$
Wir überlassen es als Übung zu zeigen, dass diese Abbildung bijektiv ist.

Definition 5.4

Seien A, B nicht-leere Mengen und $f\colon A \to B$ eine Abbildung.
Für $b \in B$ heißt $f^{-1}(b) := \{a \in A \mid f(a) = b\}$ das ***Urbild*** von b. Allgemeiner:
Ist $B' \subseteq B$ eine Teilmenge, so ist $f^{-1}(B') := \{a \in A \mid f(a) \in B'\}$ das Urbild von B'.

- Sei $b \in B$. Dann gilt: $\quad f^{-1}(b) \neq \varnothing \quad \Leftrightarrow \quad b \in f(A)$.
  Beispiel: Für $f\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto 2n$, gilt $f^{-1}(3) = \varnothing$.
- Ist f injektiv und $b \in f(A)$, so gilt $|f^{-1}(b)| = 1$.
- Seien $b, b' \in B$ und $b \neq b'$. Dann ist $f^{-1}(b) \cap f^{-1}(b') = \varnothing$.
- Sei f surjektiv. Dann ist $f^{-1}(b) \neq \varnothing$ für alle $b \in B$ und
  $$A = \bigcup\nolimits_{b \in B} f^{-1}(b) \qquad \text{(disjunkte Vereinigung).}$$
  Beispiel: $f\colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$, $(n, m) \mapsto n + m$, ist surjektiv und
  $f^{-1}(0) = \{(0, 0)\}$, $\quad f^{-1}(2) = \{(2, 0), (1, 1), (0, 2)\}$, $\quad f^{-1}(\{\text{gerade Zahlen}\}) = \{(n, m) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid n, m \text{ beide gerade oder } n, m \text{ beide ungerade}\}$.

Definition 5.5

Seien A, B, C nicht-leere Mengen und $f\colon A \to B$, $g\colon B \to C$ Abbildungen. Durch ***Hintereinanderausführung*** erhalten wir auch eine Abbildung

$$g \circ f\colon A \to C, \qquad a \mapsto g\big(f(a)\big).$$

Schliesslich bezeichnen wir mit $\mathrm{id}_A\colon A \to A$ die ***identische Abbildung***, d.h., es gilt $\mathrm{id}_A(a) = a$ für alle $a \in A$.

Lemma 5.6

Sei $f\colon A \to B$ eine Abbildung. Dann gilt:

(a) Gibt es eine Abbildung $g\colon B \to A$ mit $g \circ f = \mathrm{id}_A$, so ist f injektiv.

(b) Gibt es eine Abbildung $g\colon B \to A$ mit $f \circ g = \mathrm{id}_B$, so ist f surjektiv.

(c) f ist bijektiv $\quad\Leftrightarrow\quad$ es gibt eine Abbildung $g\colon B \to A$ mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$.

In diesem Fall heißt g die ***Umkehrabbildung*** von f.

Beweis. (a) Sei also angenommen, dass es $g\colon B \to A$ gibt mit $g \circ f = \mathrm{id}_A$. Wir wollen zeigen, dass f injektiv ist. Seien $a, a' \in A$ mit $f(a) = f(a')$. Dann folgt

$$a = \mathrm{id}_A(a) = (g \circ f)(a) = g\big(f(a)\big) = g\big(f(a')\big) = (g \circ f)(a') = \mathrm{id}_A(a') = a'.$$

(b) Sei nun angenommen, dass es $g\colon B \to A$ gibt mit $f \circ g = \mathrm{id}_B$. Wir wollen zeigen, dass f surjektiv ist. Sei also $b \in B$ und setze $a := g(b) \in A$. Dann gilt

$$f(a) = f\big(g(b)\big) = (f \circ g)(b) = \mathrm{id}_B(b) = b.$$

(c) Wir müssen die beiden Richtungen der Äquivalenz zeigen. Nehmen wir zuerst an, dass es $g\colon B \to A$ gibt mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$. Also erfüllt g die Bedingungen in (a) und (b). Dann ist f injektiv und surjektiv, also bijektiv.
Umgekehrt: Nehmen wir jetzt an, dass f bijektiv ist. Wir müssen zeigen, dass es $g\colon B \to A$ gibt mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$. Wir definieren g wie folgt.
Sei $b \in B$. Da f surjektiv ist, gibt es ein $a \in A$ mit $f(a) = b$. Da f injektiv ist, gibt es nur eine Möglichkeit für dieses Element a; wir setzen $g(b) := a$. Dann folgt sofort $g\big(f(a)\big) = a$ für alle $a \in A$ und $f\big(g(b)\big) = b$ für alle $b \in B$. □

Für jedes $n \in \mathbb{N}$ können wir die Menge $\{k \in \mathbb{N} \mid k \leqslant n\} = \{1, 2, \ldots, n\}$ bilden, diese hat offenbar genau n Elemente. Allgemein definieren wir:

Definition 5.7

(a) Seien A, B nicht leere Mengen. Dann heißen A, B ***gleichmächtig***, wenn es eine bijektive Abbildung $f\colon A \to B$ gibt. Wir schreiben in diesem Fall $|A| = |B|$.
(b) Gibt es ein $n \in \mathbb{N}$, so dass A gleichmächtig zu $\{1, \ldots, n\}$ ist, so schreiben wir einfach $|A| = n$ und sagen, dass A eine ***endliche Menge*** ist. Es gibt dann also eine bijektive Abbildung $f\colon \{1, \ldots, n\} \to A$, und A besteht genau aus den n Elementen $f(1), \ldots, f(n)$.
(c) Wenn es kein n wie in (b) gibt, so schreiben wir $|A| = \infty$. In diesem Fall hat A unendlich viele Elemente. Schließlich: Ist $A = \varnothing$, so setzen wir $|A| = 0$.

Zum Beispiel ist $\mathbb{N} \subsetneq \mathbb{N}_0$, aber dennoch $|\mathbb{N}| = |\mathbb{N}_0|$, denn $f\colon \mathbb{N}_0 \to \mathbb{N}$, $n \mapsto n + 1$, ist eine Bijektion ($\rightsquigarrow$ “Hilberts Hotel”). Bleiben wir zuerst bei endlichen Mengen.

Bemerkung 5.8

Seien A und B nicht-leere endliche Mengen. Dann ist auch $A \cup B$ endlich.
(a) Gilt $A \cap B = \varnothing$, so folgt $|A \cup B| = |A| + |B|$.
(b) Im Allgemeinen ist $|A \cup B| = |A| + |B| - |A \cap B|$.

Beweis. (a) Sei $n \in \mathbb{N}$ so, dass es eine bijektive Abbildung $f\colon \{1, \ldots, n\} \to A$ gibt. Sei $m \in \mathbb{N}$ so, dass es eine bijektive Abbildung $g\colon \{1, \ldots, n\} \to B$ gibt.
Definiere dann $h\colon \{1, \ldots, n+m\} \to A \cup B$ durch

$$h(i) := \begin{cases} f(i) & \text{falls } 1 \leqslant i \leqslant n, \\ g(i-n) & \text{falls } n < i \leqslant n+m. \end{cases}$$

Dann prüft man sofort nach, dass h eine bijektive Abbildung ist.
(b) Sei $A' := A \setminus (A \cap B)$. Dann gilt $A = A' \cup (A \cap B)$, und die Vereinigung ist disjunkt. Mit (a) folgt $|A| = |A'| + |A \cap B|$. Außerdem ist $A \cup B = A' \cup B$, und die Vereinigung ist disjunkt. Damit $|A \cup B| = |A'| + |B| = |A| - |A \cap B| + |B|$. □

Lemma 5.9

Seien A, B nicht-leere, endliche Mengen und $f\colon A \to B$ eine Abbildung.

(a) Ist f injektiv, so gilt $|A| \leqslant |B|$.

(b) Ist f surjektiv, so gilt $|A| \geqslant |B|$.

(c) Es gelte $|A| = |B|$. Ist f injektiv oder surjektiv, so ist f bijektiv.

Beweis. Sei $|A| = n \in \mathbb{N}$ und $|B| = m \in \mathbb{N}$.
Also ist $A = \{a_1, \ldots, a_n\}$ und $B = \{b_1, \ldots, b_m\}$.
(a) Ist f injektiv, so sind $f(a_1), \ldots, f(a_n)$ alle verschieden, also ist $|f(A)| = n$.
Wegen $f(A) \subseteq B$ folgt $|A| = n = |f(A)| \leqslant |B|$.
(b) Ist f surjektiv, so wähle zu jedem $j \in \{1, \ldots, m\}$ ein $i_j \in \{1, \ldots, n\}$ mit $f(a_{i_j}) = b_j$. Dann sind $a_{i_1}, \ldots, a_{i_m} \in A$ alle verschieden, also $|A| \geqslant m = |B|$.
(c) Sei $|A| = |B|$. Ist f injektiv, so ist wie oben $|A| = |f(A)|$. Wegen $|A| = |B|$ folgt also $|f(A)| = |B|$, und damit $f(A) = B$, d.h., f ist auch surjektiv.

Noch einmal die Voraussetzungen: $|A| = |B| = m$ und $B = \{b_1, \ldots, b_m\}$.
Ist f surjektiv, so folgt $A = f^{-1}(b_1) \cup \ldots \cup f^{-1}(b_m)$, wobei jedes $f^{-1}(b_j)$ nicht leer ist und die Vereinigung disjunkt ist. Damit $m = |A| = |f^{-1}(b_1)| + \ldots + |f^{-1}(b_m)|$ (siehe Bemerkung 5.8), wobei jeder Summand $\geqslant 1$ ist. Da die ganze Summe gleich m ist, muss jeder Summand gleich 1 sein, also f injektiv. □

Im Folgenden bestimmen wir nun noch die Mächtigkeiten von endlichen Mengen bei einigen weiteren Konstruktionen.

Beispiel 5.10

Seien A, B nicht-leere Mengen. Mit $\mathrm{Abb}(A, B)$ bezeichnen wir die Menge aller Abbildungen $f\colon A \to B$. Seien nun A, B endlich. Dann gilt $|\mathrm{Abb}(A, B)| = |B|^{|A|}$.

Denn: Seien $|A| = n$ und $|B| = m$; sei $A = \{a_1, \ldots, a_n\}$. Um $f\colon A \to B$ zu definieren, haben wir für $f(a_1)$ genau m Möglichkeiten (nämlich eines der m Elemente von B), ebenso für $f(a_2)$ und so fort. Also insgesamt m^n Möglichkeiten.

Beispiel 5.11

Seien A, B nicht-leere, endliche Mengen. Dann gilt $|A \times B| = |A| \cdot |B|$.
Denn: Seien $|A| = n$ und $|B| = m$. Für $(a, b) \in A \times B$ gibt es n Möglichkeiten für die erste Komponente $a \in A$, und für jede Wahl von $a \in A$ dann jeweils m Möglichkeiten für die zweite Komponente, also ingesamt nm Möglichkeiten.

Beispiel 5.12

Seien A_1, A_2, A_3 nicht-leere Mengen. Dann definieren wir $A_1 \times A_2 \times A_3 := (A_1 \times A_2) \times A_3$, und schreiben $\big((a_1, a_2), a_3\big)$ einfach als (a_1, a_2, a_3). Die Elemente von $A_1 \times A_2 \times A_3$ sind damit Tripel (a_1, a_2, a_3) mit $a_1 \in A_1$, $a_2 \in A_2$, $a_3 \in A_3$. Allgemeiner: Ist $n \geqslant 2$ und sind $A_1, A_2, \ldots, A_n$ nicht-leere Mengen, so definieren wir rekursiv $A_1 \times A_2 \times \ldots \times A_n := (A_1 \times \ldots \times A_{n-1}) \times A_n$. Die Elemente von $A_1 \times \ldots \times A_n$ schreiben wir als $(a_1, \ldots, a_n)$ mit $a_i \in A_i$ für $1 \leqslant i \leqslant n$; diese Elemente heißen n***-Tupel***. Mit einer einfachen vollständigen Induktion nach n folgt: Sind $A_1, \ldots, A_n$ endlich, so gilt $|A_1 \times \ldots \times A_n| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_n|$.

Bemerkung 5.13

Sei $n \in \mathbb{N}$ und seien $A_1, \ldots, A_n$ nicht-leere Mengen. Rekursiv haben wir oben $A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \mid a_i \in A_i \text{ für } 1 \leqslant i \leqslant n\}$ definiert. Wir sehen nun: Sei $A := A_1 \cup \ldots \cup A_n$. Dann können wir ein n-Tupel $(a_1, \ldots, a_n)$ auch als Abbildung $f\colon \{1, \ldots, n\} \to A$ auffassen, mit $a_i = f(i) \in A_i$ für $1 \leqslant i \leqslant n$.
Mit dieser Identifizierung können wir auch definieren:

$$A_1 \times A_2 \times \ldots \times A_n := \{f \in \mathrm{Abb}(\{1, 2, \ldots, n\}, A) \mid f(i) \in A_i \text{ for } 1 \leqslant i \leqslant n\}.$$

Definition 5.14

Seien $n \in \mathbb{N}$ und $k \in \mathbb{N}_0$. Dann bezeichnen wir mit dem Symbol $\binom{n}{k}$ die Anzahl der Teilmengen von $\{1, \ldots, n\}$ mit genau k Elementen. Für $n = 0$ setzen wir $\binom{0}{0} = 1$, und $\binom{0}{k} = 0$ falls $k \geqslant 1$. Die Symbole $\binom{n}{k}$ heissen ***Binomialkoeffizienten***.

Beispiele: $\binom{n}{0} = 1 = \binom{n}{n}$ für alle $n \in \mathbb{N}_0$. Es gilt $\binom{4}{2} = 6$, denn es gibt 6 Teilmengen von $\{1, 2, 3, 4\}$ mit 2 Elementen, nämlich $\{1, 2\}$, $\{1, 3\}$, $\{1, 4\}$, $\{2, 3\}$, $\{2, 4\}$, $\{3, 4\}$.

Satz 5.15 (Formel von Pascal, um 1655)

Für alle $n, k \in \mathbb{N}$ gilt $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Beweis. Ist $n = 1$, so gilt $\binom{1}{0} = \binom{1}{1} = 1$ und die Formel folgt mit den obigen Konventionen für $\binom{0}{k}$. Wir führen folgende Bezeichnungen ein:

$T(n,k) :=$ Menge der Teilmengen von $\{1,\dots,n\}$ mit genau k Elementen,
$T_1(n,k) := \{S \in T(n,k) \mid n \in S\}$.
$T_0(n,k) := \{S \in T(n,k) \mid n \notin S\} = T(n-1,k)$ (für $n \geqslant 2$).

Sei nun $n \geqslant 2$. Es ist offenbar $T(n,k) = T_1(n,k) \cup T_0(n,k)$ und die Vereinigung ist disjunkt. Mit Bemerkung 5.8 erhalten wir

$$\begin{aligned}\binom{n}{k} = |T(n,k)| &= |T_1(n,k)| + |T_0(n,k)| \\ &= |T_1(n,k)| + |T(n-1,k)| = |T_1(n,k)| + \binom{n-1}{k}.\end{aligned}$$

Wir müssen jetzt nur noch zeigen, dass $|T_1(n,k)| = \binom{n-1}{k-1}$ gilt. Nun ist die rechte Seite gleich $|T(n-1,k-1)|$, also müssen wir $|T_1(n,k)| = |T(n-1,k-1)|$ zeigen.

Noch einmal:

$T(n,k) :=$ Menge der Teilmengen von $\{1,\dots,n\}$ mit genau k Elementen,
$T_1(n,k) =$ Menge aller $S \in T(n,k)$ mit $n \in S$.

Wir wollen zeigen: $|T_1(n,k)| = |T(n-1,k-1)|$. Dazu definieren wir Abbildungen:

$$\begin{aligned} f\colon\ & T(n-1,k-1) \to T_1(n,k), & S &\mapsto S \cup \{n\}, \\ g\colon\ & T_1(n,k) \to T(n-1,k-1), & S' &\mapsto S' \setminus \{n\}. \end{aligned}$$

Dann sind $f \circ g$ und $g \circ f$ jeweils die identischen Abbildungen, also ist f bijektiv (siehe Lemma 5.6(c)) und damit $|T_1(n,k)| = |T(n-1,k-1)| = \binom{n-1}{k-1}$. □

Für $m \in \mathbb{N}$ heißt $m! := 1 \cdot 2 \cdot \ldots \cdot m$ die ***Fakultät*** von m; Konvention: $0! := 1$.

Folgerung 5.16

Für alle $n, k \in \mathbb{N}_0$ mit $0 \leqslant k \leqslant n$ gilt $\displaystyle\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Beweis. Für $0 \leqslant k \leqslant n$ definiere $\displaystyle\beta(n,k) := \frac{n!}{k! \cdot (n-k)!} \in \mathbb{Q}$.

Nach Ü3 erfüllen diese $\beta(n,k)$ folgende Bedingungen:

- $\beta(n,0) = \beta(n,n) = 1$ für alle $n \in \mathbb{N}_0$ und
- $\beta(n,k) = \beta(n-1,k-1) + \beta(n-1,k)$ für alle $n, k \in \mathbb{N}_0$ mit $1 \leqslant k \leqslant n-1$.

Aber die Binomialkoeffizienten $\binom{n}{k}$ erfüllen ebenfalls diese Bedingungen, siehe Formel von Pascal.
Also folgt mit Ü3, dass $\beta(n,k) = \binom{n}{k}$ für alle $n, k \in \mathbb{N}_0$ mit $0 \leqslant k \leqslant n$ gilt. □

Die Fakultät $n!$ selbst hat ebenfalls eine mengentheoretische Interpretation.

Lemma 5.17

Sei $n \in \mathbb{N}$. Dann ist $n! = |\{f\colon \{1,\dots,n\} \to \{1,\dots,n\} \mid f \text{ bijektiv }\}|$.

Beweis. Um eine injektive Abbildung $f\colon \{1,\dots,n\} \to \{1,\dots,n\}$ zu definieren, gibt es zunächst n Möglichkeiten für $f(1)$ (nämlich irgendeine der Zahlen $1,\dots,n$).

Damit f injektiv wird, gibt es dann noch $n-1$ Möglichkeiten für $f(2)$ (nämlich irgendeine der Zahlen $1,\dots,n$ außer $f(1)$).

Für $f(3)$ gibt es dann noch $n-2$ Möglichkeiten (alle Zahlen außer $f(1), f(2)$).

Nach $n-1$ Schritten sind dann bereits $n-1$ Zahlen für die Werte $f(1),\dots,f(n-1)$ verbraucht, also bleibt für $f(n)$ noch genau eine Möglichkeit übrig.

Damit hat man also insgesamt $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1 = n!$ Möglichkeiten für f.

Mit Satz 5.9 ist jedes solche injektive f automatisch bijektiv. □

Siehe auch `https://de.wikipedia.org/wiki/Abzählende_Kombinatorik`.

§6 Unendliche Mengen

Definition 6.1

Eine nicht-leere, unendliche Menge A, die gleichmächtig zu $\mathbb{N}$ ist (oder zu $\mathbb{N}_0$), heißt ***abzählbar unendlich***. Sonst heißt A ***überabzählbar***.
Ist A abzählbar, so gibt es also eine Bijektion $f\colon \mathbb{N} \to A$. Setzen wir $a_n := f(n)$ für alle $n \in \mathbb{N}$, so ist also $A = \{a_1, a_2, a_3, \ldots\}$ eine "Aufzählung" der Elemente von A.

- $\mathbb{Z}$ ist abzählbar unendlich, denn wir können eine bijektive Abbildung $f\colon \mathbb{Z} \to \mathbb{N}$ zum Beispiel wie folgt definieren:
$$f(n) = \begin{cases} 2n+1 & \text{falls } n \geqslant 0, \\ -2n & \text{falls } n < 0. \end{cases}$$
- $\mathbb{N}_0 \times \mathbb{N}_0$ ist abzählbar, siehe Beispiel 5.3(d).
- $\mathbb{Q}$ ist ebenfalls abzählbar (siehe Übungen).

In der Analysis wird gezeigt, dass $\mathbb{R}$ überabzählbar ist. Weiteres Beispiel:

Satz 6.2 (Georg Cantor, um 1880)

Ist A eine nicht-leere Menge, so gibt es keine surjektive Abbildung $f\colon A \to \mathcal{P}(A)$. Also kann A auch nicht gleichmächtig zu $\mathcal{P}(A)$ sein.
Beispiel: Die Potenzmenge $\mathcal{P}(\mathbb{N})$ ist überabzählbar.

Beweis. Annahme, es gibt eine surjektive Abbildung $f\colon A \to \mathcal{P}(A)$. Betrachte dann die Menge $B := \{x \in A \mid x \notin f(x)\} \in \mathcal{P}(A)$. Da f surjektiv ist, gibt es ein $a \in A$ mit $B = f(a)$. Nun gilt aber: $\quad a \in f(a) \quad \Leftrightarrow \quad a \in B \quad \Leftrightarrow \quad a \notin f(a)$.
Also erhalten wir einen Widerspruch. Nun betrachte das Beispiel $A = \mathbb{N}$.
Die Abbildung $f\colon \mathbb{N} \to \mathcal{P}(\mathbb{N})$, $n \mapsto \{n\}$, ist injektiv, also ist $\mathcal{P}(\mathbb{N})$ unendlich. Da $\mathbb{N}$ nicht gleichmächtig zu $\mathcal{P}(\mathbb{N})$ ist, folgt also, dass $\mathcal{P}(\mathbb{N})$ überabzählbar ist. □
Die Frage, ob $\mathcal{P}(\mathbb{N})$ gleichmächtig zu $\mathbb{R}$ ist, wird als ***Kontinuumshypothese*** bezeichnet, siehe `https://de.wikipedia.org/wiki/Kontinuumshypothese`.

Satz 6.3

Sei A eine unendliche Menge. Dann gibt es eine injektive Abbildung $f\colon \mathbb{N}_0 \to A$, d.h., setzt man $a_n := f(n)$ für $n \in \mathbb{N}_0$, so erhält man eine unendliche Folge von paarweise verschiedenen Elementen $a_0, a_1, a_2, \ldots$ in A.

Idee des Beweises: Zuerst wähle irgendeinen Startwert $a_0 \in A$.

- Jetzt betrachte $A_1 := A \setminus \{a_0\}$. Dann ist immer noch $|A_1| = \infty$, also $A_1 \neq \varnothing$. Wähle irgendein $a_1 \in A_1$; dann ist auch $a_1 \neq a_0$.
- Jetzt betrachte $A_2 := A_1 \setminus \{a_1\} = A \setminus \{a_0, a_1\}$. Dann ist immer noch $|A_2| = \infty$, also $A_2 \neq \varnothing$. Wähle irgendein $a_2 \in A_2$; dann ist auch $a_2 \neq a_0$ und $a_2 \neq a_1$.
- Jetzt betrachte $A_3 := A_2 \setminus \{a_2\} = A \setminus \{a_0, a_1, a_2\}$, … usw. usw.

Aber das Problem ist hier das "usw. usw." ! Wie macht man so etwas präzise ?
Dazu brauchen wir zwei Hilfsmittel (auf die wir aber nur kurz eingehen werden).

Satz 6.4 (Rekursionssatz)

Sei A eine nicht-leere Menge, und $a_0 \in A$. Außerdem sei für jedes $n \in \mathbb{N}_0$ eine Abbildung $h_n\colon A \to A$ gegeben. Dann gibt es genau eine Abbildung $F\colon \mathbb{N}_0 \to A$ mit $\quad F(0) = a_0 \quad$ und $\quad F(n+1) = h_n\big(F(n)\big) \quad$ für alle $n \in \mathbb{N}_0$.

Dies ist die theoretische Grundlage für die ***rekursive Definition*** von Folgen.
Sei zum Beispiel $A = \mathbb{Q}_{>0} := \{x \in \mathbb{Q} \mid x > 0\}$ und $h\colon \mathbb{Q}_{>0} \to \mathbb{Q}_{>0}$ gegeben durch
$$h(x) = \tfrac{1}{2}\big(x + \tfrac{2}{x}\big) \qquad \text{für alle } x \in \mathbb{Q},\ x > 0.$$
Sei $a_0 = 2$ und $h_n = h$ für $n \in \mathbb{N}_0$. Sei F die zugehörige Abbildung aus Satz 6.4.
Setze $a_n := F(n)$ für $n \in \mathbb{N}$. Dann ist $(a_n)_{n\in\mathbb{N}_0}$ eine Folge mit $a_0 = 2$ und
$$a_{n+1} = F(n+1) = h(F(n)) = h(a_n) = \tfrac{1}{2}(a_n + \tfrac{2}{a_n}) \qquad \text{für alle } n \geqslant 0.$$
(Diese Folge kennen Sie vermutlich aus der Analysis: sie konvergiert gegen $\sqrt{2}$.)

Die Abbildungen h_n sind also Vorschriften, mit denen man das jeweils nächste Folgenglied aus dem vorherigen berechnet. Aber dass man damit eine auf ganz $\mathbb{N}_0$ definierte Abbildung erhält, ist zunächst — und überhaupt — nicht klar.

Beweisidee (nicht in der Vorlesung). Um die Existenz von F zu zeigen, erinnern wir uns daran, dass eine Abbildung $\mathbb{N}_0 \to A$ eine Relation $R \subseteq \mathbb{N}_0 \times A$ mit speziellen Eigenschaften ist; siehe Bemerkung 5.2(c). Sei $\mathcal{R}$ die Menge aller Teilmengen $R \subseteq \mathbb{N}_0 \times A$, die folgende Eigenschaften erfüllen:

$(*)$ $\quad (0, a_0) \in R \quad$ und $\quad \forall n \in \mathbb{N}_0\colon (n, a) \in R \Rightarrow (n+1, h_n(a)) \in R.$

Die ganze Menge $R = \mathbb{N}_0 \times A$ erfüllt $(*)$, also ist $\mathcal{R}$ eine nicht-leere Teilmenge von $\mathcal{P}(\mathbb{N}_0 \times A)$. Dann setze $\quad R_0 := \bigcap_{R \in \mathcal{R}} R.$

Wegen $(0, a_0) \in R$ für alle $R \in \mathcal{R}$ folgt auch $(0, a_0) \in R_0$, also ist $R_0 \neq \varnothing$. Weil die zweite Bedigung in $(*)$ für alle $R \in \mathcal{R}$ gilt, gilt sie auch für R_0. Also erfüllt R_0 selbst auch $(*)$. Wir müssen noch zeigen, dass R_0 eine Abbildung definiert, d.h.,

(a) Zu jedem $n \in \mathbb{N}_0$ gibt es ein $a \in A$ mit $(n, a) \in R_0$.

(b) Sind $(n, a) \in R_0$ und $(n, a') \in R_0$, so folgt $a = a'$.

Dazu wird wiederum vollständige Induktion nach n benutzt. Versuchen Sie es selbst, sonst siehe §12 im Buch von Halmos für die weiteren Details. □

Beispiel 6.5 (siehe auch `https://de.wikipedia.org/wiki/Fibonacci-Folge`)

Sei $(f_n)_{n \in \mathbb{N}_0}$ die von Leonardo Fibonacci (um 1202 !) rekursiv definierte Folge mit

$f_0 := 1, \quad f_1 := 1 \quad$ und $\quad f_{n+1} := f_n + f_{n-1} \quad$ für alle $n \geqslant 1$.

Also $\quad 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots, 12586269025\ (n = 50), \ldots$

Hier braucht mal also jeweils zwei vorhergehende Folgenglieder, um ein neues Folgenglied auszurechnen. — Wie passt dies in den Rekursionssatz?

Dazu sei $A := \mathbb{N}_0 \times \mathbb{N}_0$; definiere $h\colon A \to A$ durch

$$h(i, j) := (j, i + j) \qquad \text{für alle } (i, j) \in \mathbb{N}_0 \times \mathbb{N}_0.$$

Nach dem Rekursionssatz gibt es eine Abbildung $F\colon \mathbb{N}_0 \to A$ mit $F(0) = (0, 1)$ und $F(n+1) = h(F(n))$ für alle $n \geqslant 0$. Dann:

$$F(1) = h(F(0)) = h(0, 1) = (1, 1), \quad F(2) = h(F(1)) = h(1, 1) = (1, 2),$$
$$F(3) = h(F(2)) = h(1, 2) = (2, 3), \quad F(4) = h(F(3)) = h(2, 3) = (3, 5), \quad \ldots$$

Schreibe $F(n) = (a_n, b_n)$ für alle $n \in \mathbb{N}_0$. Übung: $b_n = a_{n+1} = a_n + a_{n-1}$ für $n \geqslant 1$. (Vollständige Induktion nach n). Also ist $(a_n)_{n \in \mathbb{N}_0}$ die Fibonacci–Folge.

Das zweite Hilfsmittel ist ein weiteres (berühmtes) Axiom der Mengenlehre.

Auswahlaxiom (Ernst Zermelo 1904)

Sei A eine nicht-leere Menge und $\mathcal{P}(A)^\natural := \mathcal{P}(A) \setminus \{\varnothing\}$. Dann gibt es eine Abbildung $\alpha\colon \mathcal{P}(A)^\natural \to A$ mit $\alpha(B) \in B$ für alle nicht-leeren Teilmengen $B \subseteq A$.

Eine solche Abbildung heißt ***Auswahlfunktion***, denn sie "wählt" aus jeder nicht-leeren Teilmenge $B \subseteq A$ ein Element $\alpha(B) \in B$ aus.

Beispiel. Sei $A = \mathbb{N}$. Eine Auswahlfunktion $\alpha\colon \mathcal{P}(\mathbb{N})^\natural \to \mathbb{N}$ ist durch Peano's Induktionsaxiom gegeben: $\alpha(B) = \min(B)$ für jede nicht-leere Teilmenge $B \subseteq \mathbb{N}$.

Hier sehen wir jetzt, wo das Problem liegt: Versuchen Sie, eine Auswahlfunktion für $A = \mathbb{R}$ hinzuschreiben — Das ist bisher noch niemandem gelungen !
Das Auswahlaxiom garantiert also die Existenz von Etwas, das man in vielen Fällen gar nicht konkret hinschreiben kann. Für eine weitere Diskussion siehe

`https://de.wikipedia.org/wiki/Auswahlaxiom`

Nun zum **Beweis** von Satz 6.3. Sei $A \neq \varnothing$ und $|A| = \infty$. Zu zeigen: Es gibt eine injektive Abbildung $f\colon \mathbb{N}_0 \to A$. Dazu sei $\alpha\colon \mathcal{P}(A)^\natural \to A$ eine Auswahlfunktion. Sei $a_0 := \alpha(A)$. Dann definieren wir rekursiv eine Folge $(a_n)_{n \in \mathbb{N}_0}$ mit

$$(*) \quad a_{n+1} = \alpha(A \setminus \{a_0, a_1, \ldots, a_n\}) \qquad \text{für alle } n \geqslant 0.$$

Beachte: Wegen $|A| = \infty$ ist $(A \setminus B) \neq \varnothing$ für jede endliche Teilmenge $B \subseteq A$, also können wir $\alpha(A \setminus \{a_0, a_1, \ldots, a_n\})$ bilden. Aus $(*)$ folgt $a_{n+1} \notin \{a_0, a_1, \ldots, a_n\}$ für alle $n \geqslant 0$, also sind $a_0, a_1, a_2, \ldots$ alle verschieden. Damit ist $f\colon \mathbb{N}_0 \to A$, $n \mapsto a_n$, die gesuchte injektive Abbildung.

Noch einmal (zum letzten Mal!): wie rechtfertigt man $(*)$ mit dem Rekursionssatz? Wir brauchen eine Menge X und eine Abbildung $h\colon X \to X$. Wir setzen

$$X := \big\{(B, a) \in \mathcal{P}(A) \times A \mid B \text{ endlich und } a \notin B\big\}.$$

Dann ist $X \neq \varnothing$ (zum Beispiel $(\varnothing, a) \in X$ für $a \in A$). Definiere $h\colon X \to X$ durch

$$h(B, a) := \big(B \cup \{a\},\ \alpha(A \setminus (B \cup \{a\}))\big) \qquad \text{für alle } (B, a) \in X.$$

Mit dem Rekursionssatz erhalten wir $F\colon \mathbb{N}_0 \to X$ mit $F(0) = (\varnothing, a_0)$ und $F(n+1) = h(F(n))$ für alle $n \in \mathbb{N}_0$. Schreibe $F(n) = (B_n, a_n)$ für alle $n \in \mathbb{N}_0$.
Dann zeigt man für alle $n \in \mathbb{N}_0$:

$$B_{n+1} = \{a_0, a_1, \ldots, a_n\} \quad \text{und} \quad a_{n+1} = \alpha(A \setminus \{a_0, a_1, \ldots, a_n\}).$$

(Dies ist eine leichte vollständige Induktion nach n, ähnlich wie vorher bei Fibonacci.) Damit ist obige rekursive Definition gerechtfertigt. □

Folgerung 6.6

(a) Sei $A \subseteq \mathbb{N}_0$ nicht-leer und unendlich. Dann ist auch A abzählbar unendlich.
(b) Sei A eine nicht-leere, unendliche Menge und $g\colon \mathbb{N}_0 \to A$ eine surjektive Abbildung. Dann ist auch A abzählbar unendlich.

Damit lassen sich bereits viele Beweise zu abzählbar unendlichen Mengen führen; Beispiele in den Übungen.

Beweis (nur kurz in der Vorlesung). Zu (a): Für $A \subseteq \mathbb{N}_0$ ist eine Auswahlfunktion $\alpha\colon \mathcal{P}(A)^\natural \to A$ gegeben durch $\alpha(B) = \min(B)$ für alle $B \in \mathcal{P}(A)^\natural$. Wie im obigen Beweis erhalten wir eine injektive Abbildung $f\colon \mathbb{N}_0 \to A$ mit $f(0) = \min(A)$ und

$$f(n+1) = \min(A \setminus \{f(0), f(1), \ldots, f(n)\}) \in A \qquad \text{für alle } n \geqslant 0.$$

Dann folgt leicht: $A = f(\mathbb{N}_0)$, also ist f bijektiv und damit $|A| = |\mathbb{N}_0|$.
Denn für gegebenes $n_0 \in A$ ist die Menge $B := \{k \in \mathbb{N}_0 \mid n_0 \leqslant f(k)\}$ nicht leer und dann $n_0 = f(m_0)$, wobei $m_0 := \min(B)$ (überzeugen Sie sich davon).

Zu (b): Da $g\colon \mathbb{N}_0 \to A$ surjektiv ist, gilt $\mathbb{N}_0 = \bigcup_{a \in A} g^{-1}(a)$ mit $g^{-1}(a) \neq \varnothing$ für alle $a \in A$. Für $a \in A$ sei $n_a := \min\big(g^{-1}(a)\big) \in \mathbb{N}_0$; damit erhalten wir eine Abbildung $f\colon A \to \mathbb{N}_0$, $a \mapsto n_a$. Es gilt $(g \circ f)(a) = g\big(f(a)\big) = g(n_a) = a$ für alle $a \in A$.
Also ist $g \circ f = \mathrm{id}_A$ und damit ist f injektiv, siehe Lemma 5.6(a).
Setze $B := f(A) = \{n_a \mid a \in A\} \subseteq \mathbb{N}_0$. Dann ist $f\colon A \to B$ eine bijektive Abbildung, also $|A| = |B|$. Nun ist B eine unendliche Teilmenge von $\mathbb{N}_0$, also nach (a) selbst abzählbar unendlich. Also ist auch A abzählbar unendlich. □

Folgerung 6.7 (Richard Dedekind, um 1888)

Sei A eine nicht-leere Menge. Dann ist A unendlich genau dann, wenn es eine echte Teilmenge $B \subsetneqq A$ gibt mit $|A| = |B|$.

Dies ist eine Charakterisierung von "unendlich", die nicht Bezug auf $\mathbb{N}$ nimmt !

Beweis. Sei zuerst angenommen, dass es eine Teilmenge $B \subsetneqq A$ mit $|B| = |A|$ gibt. Dann ist $f\colon B \to A$, $b \mapsto b$, injektiv. Wäre A endlich, so müsste f auch surjektiv sein (siehe Satz 5.9(c)), Widerspruch. Also ist A unendlich. Umgekehrt: Sei A unendlich. Nach Satz 6.3 gibt es eine injektive Abbildung $f\colon \mathbb{N}_0 \to A$. Sei $a_n := f(n)$ für alle $n \in \mathbb{N}_0$, und $A' := f(\mathbb{N}_0) = \{a_0, a_1, a_2, \ldots\} \subseteq A$.
Setze nun $B := A \setminus \{a_0\}$. Wir definieren eine Abbildung $g\colon A \to B$ durch

$$g(a) := \begin{cases} a & \text{falls } a \notin A', \\ a_{n+1} & \text{falls } a \in A' \text{ und } a = a_n. \end{cases}$$

Man sieht sofort, dass g injektiv und surjektiv ist. Also $|A| = |B|$ aber $B \subsetneqq A$. □

§7 Verknüpfungen und algebraische Strukturen

Definition 7.1

Sei A eine nicht-leere Menge. Eine Abbildung $A \times A \to A$, $(a, b) \mapsto a \star b$, heißt eine ***Verknüpfung*** auf A. Eine solche Verknüpfung heißt:

- ***assoziativ***, wenn $a \star (b \star c) = (a \star b) \star c$ für alle $a, b, c \in A$ gilt;
- ***kommutativ***, wenn $a \star b = b \star a$ für alle $a, b \in A$ gilt.

Ein Element $e \in A$ heißt ***neutrales Element*** bezüglich dieser Verknüpfung, wenn $a \star e = e \star a = a$ für alle $a \in A$ gilt. Gibt es ein solches neutrales Element e und ist $a \in A$, so heißt ein Element $b \in A$ ein ***Inverses*** zu a, wenn $a \star b = b \star a = e$ gilt.

Zum Beispiel ist die Addition auf $\mathbb{Z}$ assoziativ und kommutativ; $0 \in \mathbb{Z}$ ist das neutrale Element bezüglich "+" und jedes $n \in \mathbb{Z}$ besitzt ein Inverses, nämlich $-n$. In $\mathbb{N}$ gibt es weder ein neutrales Element noch inverse Elemente bezüglich "+".

Bemerkung 7.2

(a) Gibt es ein neutrales Element, so ist dieses eindeutig bestimmt. Denn sind $e, e' \in A$ neutrale Elemente, so gilt $e' = e \star e' = e$, wobei die erste Gleichheit gilt, weil e ein neutrales Element ist, und die zweite, weil e' ein neutrales Element ist.
(b) Nehmen wir an, dass $\star$ assoziativ ist und es ein neutrales Element $e \in A$ gibt. Gibt es zu $a \in A$ ein inverses Element $b \in B$, so ist dieses eindeutig bestimmt. Denn ist auch $c \in A$ invers zu a, so folgt $c = c \star e = c \star (a \star b) = (c \star a) \star b = e \star b = b$. Das Inverse zu a werde nun mit a' bezeichnet.
(c) Die Voraussetzungen seien wie in (b). Seien $a, b \in A$ und es gebe inverse Elemente $a' \in A$, $b' \in A$. Dann ist $b' \star a'$ das Inverse zu $a \star b$, d.h., $(a \star b)' = b' \star a'$. Denn es gilt

$$(a \star b) \star (b' \star a') = \big(a \star (b \star b')\big) \star a' = (a \star e) \star a' = a \star a' = e,$$

und genauso $(b' \star a') \star (a \star b) = e$.

Definition 7.3

Sei A eine nicht-leere Menge und $\star\colon A \times A \to A$ eine Verknüpfung. Dann heißt $(A, \star)$ eine ***Gruppe***, wenn $\star$ assoziativ ist, es ein neutrales Element $e \in A$ gibt und jedes $a \in A$ ein Inverses besitzt. Eine Gruppe heißt ***abelsch*** (zu Ehren von H. N. Abels), wenn die Verknüpfung kommutativ ist.

Zum Beispiel sind $(\mathbb{Z}, +)$ und $(\mathbb{Q} \setminus \{0\}, \cdot)$ abelsche Gruppen. Gruppen, die nicht abelsch sind, werden wir im nächsten Kapitel kennen lernen.

Definition 7.4

Sei A eine abelsche Gruppe; die Verknüpfung werde dabei mit "$+$" bezeichnet, das neutrale Element mit 0 und das Inverse von $a \in A$ mit $-a$. Es sei eine weitere Verknüpfung $\cdot\colon A \times A \to A$ gegeben. Dann heißt $(A, +, \cdot)$ ein ***Ring***, wenn "$\cdot$" assoziativ ist und die Distributivregeln gelten, d.h.:

$a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$ für alle $a, b, c \in A$.

Sei $(A, +, \cdot)$ ein Ring. Gibt es ein neutrales Element $1 \in A$ bezüglich "$\cdot$", so heißt A ein ***Ring mit*** 1. Ist "$\cdot$" kommutativ, so heißt A ein ***kommutativer Ring***.
Ein kommutativer Ring mit 1, in dem $1 \neq 0$ gilt und jedes Element $0 \neq a \in A$ ein Inverses bezüglich "$\cdot$" besitzt, heißt ein ***Körper***.

Zum Beispiel ist $(\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit 1, aber kein Körper; $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper. Die Menge der geraden Zahlen $2\mathbb{Z} := \{2n \mid n \in \mathbb{Z}\}$ ist mit der üblichen Addition und Multiplikation ein kommutativer Ring, aber ohne 1.

Bemerkung 7.5

Sei $(A, +, \cdot)$ ein Ring. Dann gilt $0 \cdot a = a \cdot 0 = 0$ für alle $a \in A$. Denn

$$0 = 0 \cdot a - (0 \cdot a) = (0 + 0) \cdot a - (0 \cdot a) = (0 \cdot a + 0 \cdot a) - (0 \cdot a) = 0 \cdot a$$

und genauso $a \cdot 0 = 0$. Sei nun A ein Ring mit 1. In der Definition wurde nicht ausgeschlossen, dass $1 = 0$ gilt. Ist dies der Fall, so folgt aber $a = a \cdot 1 = a \cdot 0 = 0$ für alle $a \in A$, also gilt $A = \{0\}$.

Ist K ein Körper und $0 \neq a \in K$, so wird das Inverse von a bezüglich der Multiplikation meist mit a^{-1} bezeichnet (manchmal auch $1/a$).

Lemma 7.6 (Nullteilerfreiheit)

Sei $(K, +, \cdot)$ ein Körper und seien $a, b \in K$. Gilt $a \cdot b = 0$, so folgt $a = 0$ oder $b = 0$. Umgekehrt: Ist $a \neq 0$ und $b \neq 0$, so folgt $a \cdot b \neq 0$. Noch einmal anders ausgedrückt: Für festes $0 \neq a \in K$ ist die Abbildung $f\colon K \to K, \quad x \mapsto a \cdot x,$ injektiv.

Beweis. Es gelte $a \cdot b = 0$. Nehmen wir an, es ist auch $a \neq 0$. Dann müssen wir zeigen, dass $b = 0$ gilt. Dazu: Wegen $a \neq 0$ gibt es ein Inverses $a^{-1} \in K$.
Dann folgt $b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0,$ wobei die letzte Gleichheit aus Bemerkung 7.5 folgt. Sei schließlich $0 \neq a \in K$ fest. Seien $x, y \in K$ mit $f(x) = f(y)$. Aus $a \cdot x = f(x) = f(y) = a \cdot y$ folgt $a \cdot (x - y) = a \cdot x - a \cdot y = 0$, also $x - y = 0$ (weil $a \neq 0$) und damit $x = y$. Also ist f injektiv. □

Körper bilden eine grundlegende Struktur für die gesamte Lineare Algebra.
In der Analysis sind die wichtigsten Körper $\mathbb{R}$ und $\mathbb{C}$ (die komplexen Zahlen).

Nach all unseren Vorbereitungen über den “mod” Operator, Kongruenzen usw. können wir hier nun eine neue Klasse von Ringen und Körpern einführen.

Zur Erinnerung: Sei $m \in \mathbb{N}$ fest. Für $n \in \mathbb{Z}$ sei $\overline{n}$ die Restklasse von n (modulo m), also $\overline{n} = \{a \in \mathbb{Z} \mid m \text{ teilt } n-a\} = \{a \in \mathbb{Z} \mid a \mod m = n \mod m\}$. Wie in Beispiel 4.10 ist $B = \{0, 1, \ldots, m-1\}$ ein Repräsentantensystem der Restklassen. Die Menge der Restklassen bezeichnen wir nun mit $\mathbb{Z}/m\mathbb{Z} := \{\overline{0}, \overline{1}, \ldots, \overline{(m-1)}\}$.

Satz 7.7

Mit obigen Bezeichnungen können wir für alle $a, b \in \mathbb{Z}$ wie folgt eine Addition und eine Multiplikation für die zugehörigen Restklassen definieren:

$$\overline{a} + \overline{b} := \overline{a+b} \qquad \text{und} \qquad \overline{a} \cdot \overline{b} := \overline{ab}.$$

Mit diesen Verknüpfungen erhalten wir:

(a) $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins-Element $\overline{1}$.

(b) Sei $m \geqslant 2$. Dann gilt: $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper $\Leftrightarrow$ m ist eine Primzahl.

Beweis. Seien $a, b \in \mathbb{Z}$. Dann können wir $\overline{a+b}$ und $\overline{ab}$ bilden. Sind auch $c, d \in \mathbb{Z}$ mit $\overline{a} = \overline{c}$ und $\overline{b} = \overline{d}$ gegeben, so können wir entsprechend $\overline{c+d}$ und $\overline{cd}$ bilden. Damit es überhaupt Sinn macht, die Restklassen selbst zu addieren und zu multiplizieren, muss sichergestellt sein, dass bei den obigen beiden Rechnungen jeweils das gleiche Ergebnis herauskommt; aber dies ist gerade die Aussage von Lemma 4.11. Damit haben wir also “wohl-definierte” Verknüpfungen

$$+ : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \qquad \text{und} \qquad \cdot : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}.$$

($\rightsquigarrow$ Hinweis auf “Topfrechnen”)

(a) Zu den Ringaxiomem: Aufgrund der obigen Definition ist klar, dass $\overline{0}$ neutrales Element bezüglich ”+” und $\overline{1}$ neutrales Element bezüglich ”$\cdot$” ist. Jedes $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ hat ein Inverses bezüglich ”+”, nämlich $\overline{-a}$ (wegen $\overline{a} + \overline{(-a)} = \overline{a-a} = \overline{0}$).

Nun müssen noch die weiteren Regeln gezeigt werden, also für alle $a, b, c \in \mathbb{Z}$:

$$\overline{a} + \overline{b} = \overline{b} + \overline{a}, \qquad (\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c}),$$
$$\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}, \qquad (\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c}),$$
$$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}.$$

Diese Regeln folgen aber unmittelbar aus den entsprechenden Regeln für $\mathbb{Z}$; zum Beispiel:

$$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{(b+c)} = \overline{a(b+c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c},$$

wobei beim 3. Gleichheitszeichen die Regel $a(b+c) = ab + ac$ für $a, b, c \in \mathbb{Z}$ verwendet wurde. Der Beweis der anderen Regeln verläuft analog und sei als Übung überlassen. Damit ist $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit 1.

(b) Sei nun $m \geqslant 2$. Dann ist jedenfalls $\overline{0} \neq \overline{1}$.

Sei zuerst angenommen, dass $\mathbb{Z}/m\mathbb{Z}$ ein Körper ist. Dann müssen wir zeigen, dass m eine Primzahl ist. Nehmen wir an, m ist keine Primzahl, d.h., $m = ab$ mit $2 \leqslant a, b < m$. Dann gilt $\overline{a} \neq \overline{0}$ und $\overline{b} \neq \overline{0}$, aber auch $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{m} = \overline{0}$, Widerspruch zu Lemma 7.6. Also war die Annahme falsch, d.h., m ist eine Primzahl.

Zum Beispiel gilt für $m = 4$: $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$, oder für $m = 6$: $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$.

Umgekehrt sei nun $m = p$ eine Primzahl und $\overline{0} \neq \overline{a} \in \mathbb{Z}/p\mathbb{Z}$. Wir müssen zeigen: Es gibt ein Inverses zu $\overline{a}$ (bezüglich der Multiplikation).

Dazu: Wegen $\overline{a} \neq \overline{0}$ ist $p \nmid a$, also $\text{ggT}(p, a) = 1$. Nach dem Lemma von Bézout (siehe Ü2) gibt es $r, s \in \mathbb{Z}$ mit $1 = rp + sa$. Dann ist aber

$$\overline{1} = \overline{rp + sa} = \overline{r} \cdot \overline{p} + \overline{s} \cdot \overline{a} = \overline{r} \cdot \overline{0} + \overline{s} \cdot \overline{a} = \overline{s} \cdot \overline{a},$$

also ist $\overline{s} = \overline{a}^{-1}$ das gesuchte Inverse. □

Definition 7.8

Ist $m = p \in \mathbb{N}$ eine Primzahl, so wird $\mathbb{Z}/p\mathbb{Z}$ auch mit $\mathbb{F}_p = \{\overline{0}, \overline{1}, \ldots, \overline{(p-1)}\}$ bezeichnet und heißt der ***endliche Körper mit p Elementen***.

Zum Beispiel ist $\mathbb{F}_2 = \{\overline{0}, \overline{1}\}$ mit Verknüpfungstabellen:

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

und

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Dieser spielt in der Informatik und in der Kodierungstheorie eine wichtige Rolle.

Beispiel 7.9

(a) Für $m = 1$ ist $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$ und natürlich $\overline{0} + \overline{0} = \overline{0} = \overline{0} \cdot \overline{0}$.

(b) Für $m = 3, 4$ sind die Verknüpfungstabellen wie folgt gegeben:

$m = 3$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

(also $\overline{2}^{-1} = \overline{2}$)

$m = 4$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

(kein Körper)

(c) In $\mathbb{F}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ gilt: $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{3}$, $\overline{3}^{-1} = \overline{2}$, $\overline{4}^{-1} = \overline{4}$.

Folgerung 7.10 (Kleiner Satz von Fermat; um 1640)

Ist p eine Primzahl, so gilt $a^p \equiv a \pmod p$ für alle $a \in \mathbb{Z}$.

Beweis. (Vergleiche mit Beweis auf Blatt 3 der Analysis–Vorlesung.) Zu zeigen:

$\overline{a} = \overline{a^p} = \overline{a}^p$ für alle $a \in \mathbb{Z}$, wobei wir Restklassen modulo p betrachten.

Ist $\overline{a} = 0$, so ist die Aussage klar. Sei nun $\overline{a} \neq \overline{0}$ und betrachte die Abbildung $f\colon \mathbb{F}_p \to \mathbb{F}_p,\ \overline{x} \mapsto \overline{a} \cdot \overline{x}$. Diese ist injektiv nach Lemma 7.6 und Satz 7.7(b) ($\mathbb{F}_p$ ist Körper weil p Primzahl). Also ist f bijektiv nach Lemma 5.9(c), d.h.,

$$\{\overline{0},\ \overline{1},\ \overline{2},\ \ldots,\ \overline{(p-1)}\} = f(\mathbb{F}_p) = \{\overline{a} \cdot \overline{0},\ \overline{a} \cdot \overline{1},\ \overline{a} \cdot \overline{2}, \ldots,\ \overline{a} \cdot \overline{(p-1)}\}.$$

Auf beiden Seiten kommt $\overline{0} = \overline{a} \cdot \overline{0}$ vor (siehe Bemerkung 7.5), also ist auch

$$\{\overline{1},\ \overline{2},\ \ldots,\ \overline{(p-1)}\} = \{\overline{a} \cdot \overline{1},\ \overline{a} \cdot \overline{2},\ \ldots,\ \overline{a} \cdot \overline{(p-1)}\}.$$

Bilde das Produkt aller dieser Elemente:

$$\overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{(p-1)} = (\overline{a} \cdot \overline{1}) \cdot (\overline{a} \cdot \overline{2}) \cdot \ldots \cdot (\overline{a} \cdot \overline{(p-1)}) = \overline{a}^{p-1} \cdot (\overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{(p-1)}).$$

Wegen $\overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{(p-1)} \neq \overline{0}$ (Lemma 7.6) können wir diesen Faktor auf beiden Seiten kürzen (noch einmal Lemma 7.6) und erhalten $\overline{1} = \overline{a}^{p-1}$, also $\overline{a} = \overline{a}^p$. □

Zum Abschluss dieses Kapitels nun noch ein paar Ergänzungen.

Satz 7.11 (Binomischer Lehrsatz)

Sei R ein Ring mit 1. Seien $a, b \in R$ mit $a \cdot b = b \cdot a$. Dann gilt für alle $n \in \mathbb{N}_0$:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k} \qquad \text{(Konvention: } r^0 = 1 \text{ für alle } r \in R\text{)}.$$

Außerdem benutzen wir hier folgende Konvention, bezüglich des Produkts von $\binom{n}{k} \in \mathbb{N}_0$ und $a, b \in R$. Seien $m \in \mathbb{N}_0$ und $r \in R$. Dann setze $mr := 0$ falls $m = 0$; ist $m \geqslant 1$, so setze $mr := r + \ldots + r$, mit m Summanden.

Beweis. (Vollständige Induktion mit Startwert $n_0 = 0$.)

• Induktionsanfang. Sei $n = 0$. Dann ist die linke Seite $(a+b)^0$; die Summe auf der rechten Seite hat nur einen Term, nämlich $\binom{0}{0} a^0 b^0$. Beides Mal erhalten wir 1 als Ergebnis (mit unseren Konventionen zu $\binom{0}{0}$ und r^0).

• Induktionsschritt. Sei $n \geqslant 0$ und angenommen, die Formel gilt bereits für $(a+b)^n$.

Nun $(a+b)^{n+1} = (a+b)^n \cdot (a+b) = \left(\sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k}\right) \cdot (a+b)$

$$= \left(\sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k} \cdot a\right) + \left(\sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k} \cdot b\right) = A + B,$$

wobei $A = \sum_{k=0}^{n} \binom{n}{k} a^{k+1} \cdot b^{n-k}$ und $B = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n+1-k}$.

Jetzt machen wir in A die Variablensubstitution $l = k+1$. Dann ist $k = l-1$, $n-k = n+1-l$. Und nun läuft l von 1 bis $n+1$. Damit erhalten wir :

$$A = \sum_{l=1}^{n+1} \binom{n}{l-1} a^l \cdot b^{n+1-l} = \sum_{k=1}^{n+1} \binom{n}{k-1} a^k \cdot b^{n+1-k}.$$

Jetzt sehen die Terme, über die summiert wird, in A genauso aus wie in B, im neuen A läuft k von 1 bis $n+1$, in B weiterhin von 0 bis n.

Also $A = \sum_{k=1}^{n+1} \binom{n}{k-1} a^k \cdot b^{n+1-k} = \left(\sum_{k=1}^{n} \binom{n}{k-1} a^k \cdot b^{n+1-k}\right) + \binom{n}{n} a^{n+1}$,

$$B = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n+1-k} = \binom{n}{0} b^{n+1} + \left(\sum_{k=1}^{n} \binom{n}{k} a^k \cdot b^{n+1-k}\right).$$

Damit erhalten wir

$$A + B = \binom{n}{0} b^{n+1} + \left(\sum_{k=1}^{n} \Big(\underbrace{\binom{n}{k-1} + \binom{n}{k}}_{= \binom{n+1}{k} \text{ nach Pascal 5.15}} \Big) a^k \cdot b^{n+1-k}\right) + \binom{n}{n} a^{n+1},$$

$$= b^{n+1} + \left(\sum_{k=1}^{n} \binom{n+1}{k} a^k \cdot b^{n+1-k}\right) + a^{n+1}$$

$$= \binom{n+1}{0} b^{n+1} + \left(\sum_{k=1}^{n} \binom{n+1}{k} a^k \cdot b^{n+1-k}\right) + \binom{n+1}{n+1} a^{n+1}$$

und dies ist genau die gewünschte Summe auf der rechten Seite. □

Beispiel 7.12

Sei A eine nicht-leere, endliche Menge mit $|A| = n \in \mathbb{N}$. Dann gilt $|\mathcal{P}(A)| = 2^n$.

Dazu: Wegen $|A| = n$ ist $A = \{a_1, a_2, \ldots, a_n\}$. Die Teilmengen von A entsprechen dann genau den Teilmengen von $\{1, 2, \ldots, n\}$, also gilt $|\mathcal{P}(A)| = |\mathcal{P}(\{1, 2, \ldots, n\})|$. Wir brauchen also nur den Fall $A = \{1, 2, \ldots, n\}$ zu behandeln.
Wie im Beweis von Satz 5.15 (Formel von Pascal) sei

$$T(n, k) := \text{Menge der Teilmengen von } \{1, \ldots, n\} \text{ mit genau } k \text{ Elementen,}$$

für $0 \leqslant k \leqslant n$. Dann ist $\mathcal{P}(\{1, 2, \ldots, n\}) = T(n, 0) \cup T(n, 1) \cup \ldots \cup T(n, n)$,
und diese Vereinigung ist disjunkt. Also folgt

$$|\mathcal{P}(\{1, 2, \ldots, n\})| = |T(n, 0)| + |T(n, 1)| + \ldots + |T(n, n)|$$
$$= \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = (1+1)^n = 2^n,$$

wobei wir den Binomischen Lehrsatz mit $R = \mathbb{Z}$ und $a = b = 1$ verwenden.