# Mathematik I für inf, swt, msv

## Vorlesung Wintersemester 2021/22

Prof. Meinolf Geck, Lehrstuhl für Algebra, Universität Stuttgart
https://pnp.mathematik.uni-stuttgart.de/idsr/idsr1/geckmf

Dies ist das Skript zur Vorlesung Mathematik I (für inf, swt, msv) im Wintersemester 2021/22 (V4Ü2, 15 Wochen). Eines der Hauptziele ist natürlich die Vermittlung von Grundwissen und Rechenfertigkeiten in der Mathematik. Etwas genereller geht es auch um die Vermittlung einer mathematischen Denkweise für Studierende, deren erstes Fach nicht Mathematik selbst ist aber wo diese Denkweisen dennoch eine wichtige Rolle spielen.

Dazu gehört es zu lernen, wie man mathematische Sachverhalte formal korrekt aufschreibt und diese beweist, also ihre Richtigkeit nach logischen Prinzipien herleitet. Dies sind übrigens Fähigkeiten, die sich auch beim Programmieren (und in diversen anderen Situationen) als sehr hilfreich erweisen! Außerdem sollen natürlich Beispiele für die Nützlichkeit von mathematischen Konzepten in Anwendungen gegeben werden.

Die Gebiete, die in diesem Skript behandelt werden, umfassen Lineare Algebra (Matrix-Theorie), die ersten Grundlagen zur Analysis (reelle und komplexe Zahlen), sowie diskrete algebraische Strukturen (zum Beispiel das "binäre" Zahlensystem $\{0, 1\}$ mit $1 + 1 = 0$). Ganz am Anfang gibt es zunächst eine kurze Einführung in die Mengenlehre und mathematische Logik. Bei der Auswahl des konkreten Stoffes habe ich mich an den Skripten von Herrn Künzer und Herrn Lesky aus früheren Semestern orientiert und auch explizit weite Teile daraus übernommen. Allerdings gibt es hier und da Änderungen in der Präsentation.

Im Durchschnitt werden pro Woche etwa 7 Seiten dieses Skriptes behandelt. (In den einführenden Abschnitten am Anfang etwas mehr.)

Mein Dank an Herrn Rainer Häußling für die regelmäßigen Listen mit Druckfehlern und Verbesserungsvorschlägen.

***Kommentare sehr willkommen!*** (Insbesondere weitere Druckfehler, sonstige Unklarheiten, Verbesserungsvorschläge etc.)

*Stuttgart, Oktober 2021*

# Literatur

**Besonders geeignet für diese Vorlesung:**


- G. Teschl und S. Teschl, Mathematik für Informatiker. Band 1: Diskrete Mathematik und Lineare Algebra, 4. Auflage, Springer Vieweg, 2013.
- G. Teschl und S. Teschl, Mathematik für Informatiker. Band 2: Analysis und Stochastik, 3. Auflage, Springer Vieweg, 2014.


**Skripte aus früheren Durchgängen an der Uni Stuttgart:**


- P. Lesky, Mathematik I für inf, swt, msv. Skript zur Vorlesung im WiSe 2018/19; siehe `http://info.mathematik.uni-stuttgart.de/Mathe1InfWS1819`.
- M. Künzer, Mathematik I für inf, swt, msv, dsc. Skript zum WiSe 2020/21; siehe `https://info.mathematik.uni-stuttgart.de/Mathe-1-Inf-WiSe20`.


**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`


**Frei verfügbare mathematische Software zum Ausprobieren/Experimentieren:**

- GAP - Groups, Algorithms, and Programming, siehe `http://www.gap-system.org/` (Exaktes Rechnen mit Zahlen und diskreten algebraischen Strukturen.)
- SageMath, siehe `https://www.sagemath.org/` (Basiert auf der Programmiersprache Python; siehe `https://www.python.org/`)

**Einige weiterführende Texte (wird laufend ergänzt):**


- S. Axler, Linear Algebra done right. Undergraduate Texts in Mathematics, Springer-Verlag, 2015.
- N. L. Biggs, Discrete Mathematics, 2nd Edition. Oxford University Press, 2002.
- H. D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel und R. Remmert, Zahlen. Grundwissen Mathematik, vol. 1, Springer-Verlag, Berlin, 1983.

- R. L. Graham, D. E. Knuth and O. Patashnik, Concrete Mathematics: A foundation for Computer Science, 2nd edition, Addison–Wesley 1994.
- R. Haggarty, Principles of Mathematical Analysis, 2nd Edition. Prentice Hall, Addison–Wesley, 1993.
- P. R. Halmos, Naive Mengenlehre, Vandenhoeck & Ruprecht, 5. Auflage, 1994.
- 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 (Neuauflage überarbeitet, aktualisiert und ergänzt), Grundwissen Mathematik, Springer–Verlag, 1985.
- D. Serre, Matrices: Theory and Applications. Graduate Texts in Mathematics 216, Springer-Verlag, 2. Auflage, 2010.

*Inhaltsverzeichnis*

# Kapitel I: Grundlagen

Mathematik beruht auf den Grundpfeilern Mengenlehre und Logik. Wir können und wollen hier keine formale Einführung in die abstrakte Mengenlehre und mathematische Logik geben. (Dazu wäre eine eigene Vorlesung nötig, die auch in einem Mathematik-Studium oft erst später angeboten wird, wenn überhaupt.) Für den Anfang und die meisten Zwecke genügt es, sich auf einige grundlegende Sprech- und Schreibweisen zu verständigen, mit denen wir im weiteren Verlauf mathematische Sachverhalte präzise formulieren und beweisen können.

## 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 $\{\ldots\}$ bezeichnet, zum Beispiel:

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

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).

**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 $A$.

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 19.10.2021 ist ein Dienstag" 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 im Hörsaal V47.01. 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 (also so etwas wie eine lokale Variable beim Programmieren), 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.

**Verknüpfung von Aussagen.**

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

Beispiel: Ist $P$ : "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:

| $P$ | $\neg P$ |
|---|---|
| 1 | 0 |
| 0 | 1 |

| $P$ | $Q$ | $P \vee Q$ | $P \wedge Q$ | $P \Rightarrow Q$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 1 |

(wobei 1 für "wahr" steht und 0 für "falsch"). 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 $a = 2$, $b = -2$ zeigt auch, dass die Umkehrung "$a^2 = b^2 \Rightarrow a = b$" falsch 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***.

**Weitere Konstruktionen zum Bilden neuer Mengen:** Seien $A$, $B$ zwei Teilmengen einer Menge $M$. Dann ist die ***Durchschnittsmenge*** von $A$ und $B$ ist definiert durch

$$A \cap B := \{x \in M \mid x \in A \wedge x \in B\};$$

dieser besteht also genau aus den Elementen, die sowohl in $A$ als auch in $B$ enthalten sind.

Hierbei (und auch sonst in diesem Skript) steht der Doppelpunkt in ":=" für eine Definition: Es wird keine Gleichheit behauptet, sondern das Symbol "$A \cap B$" ist lediglich ein Name für die Menge auf der rechten Seite.

Die ***Vereinigungsmenge*** von $A$ und $B$ ist definiert als

$$A \cup B := \{x \in M \mid x \in A \vee x \in B\};$$

diese besteht also genau aus den Elementen, die in $A$ oder in $B$ enthalten sind (oder sowohl in $A$ als auch in $B$). Das ***Komplement*** von $B$ in $A$ bezeichnet ist definiert als

$$A \setminus B := \{x \in A \mid x \notin B\} \qquad \text{(oft auch } A^c \text{ geschrieben)}.$$

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.

Ein etwas komplexeres 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.

Dies wird mit obigen Mengenbildungsprinzipien wie folgt begründet. 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.

$$B = \Big\{ \{\text{Menschen in Deutschland}\},\ \{\text{Menschen in Frankreich}\},$$
$$\{\text{Menschen in Polen}\},\ \ldots \text{usw. für alle (nur noch) 27 Länder der EU} \Big\}.$$

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

**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: $\forall n \in \mathbb{Z} : n^2 \geqslant 0$.

Etwas formaler: Gegeben sei eine Menge $A$ und, für jedes $a \in A$, eine Aussage $P(a)$.

"$\forall a \in A : P(a)$" bedeutet, dass die Aussage $P(a)$ für alle $a \in A$ wahr ist.

"$\exists a \in A : P(a)$" bedeutet, dass es (mindestens) ein $a \in A$ gibt, für welches $P(a)$ wahr ist.

Für die Negation von Aussagen mit Quantoren gilt:

$$\neg\big(\forall a \in A : P(a)\big) \ \Leftrightarrow\ \exists\, a \in A : \neg P(a) \qquad \text{und} \qquad \neg\big(\exists\, a \in A : P(a)\big) \ \Leftrightarrow\ \forall a \in A : \neg P(a)$$

---

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 Sätzen auszudrücken.

Schließlich erwähnen wir hier nur, dass man in logische Schwierigkeiten geraten kann, wenn man die obigen Mengenbildungsprinzipien verlässt. Berühmtes Beispiel ist die ***Russell'sche Antinomie***; siehe dazu `https://en.wikipedia.org/wiki/Russell's_paradox`. Man kann so etwas auch in der Umgangssprache formulieren:

"*Definieren wir einen Barbier als jemanden, der all jene und nur jene rasiert, die sich nicht selbst rasieren. Frage: Rasiert der Barbier sich selbst?*"

Nimmt man an, er rasiert sich selbst, so erhält man einen Widerspruch; aber ebenso, wenn man annimmt, er rasiert sich nicht selbst ...

## 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 $n \mid (a \cdot m + b \cdot k)$. $\square$ ($\leftarrow$ zeigt Ende des Beweises an)

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* $n, m, k \in \mathbb{Z}$*. Gilt* $k \neq 0$ *und* $kn = km$*, 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. □

**Ab hier Woche 2**

Die folgende Eigenschaft von $\mathbb{N}_0$ erscheint intuitiv einsichtig; sie wird explizit als "Axiom" formuliert, damit wir darauf verweisen und präzise damit argumentieren können.

**Axiom 2.6** (***Peano's Induktionsaxiom***)**.** *Jede nicht-leere Teilmenge von* $\mathbb{N}_0$ *besitzt ein kleinstes Element. Oder, anders ausgedrückt mit Hilfe der Formelsprache in §1:*

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

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 $kn = n + \underbrace{(k-1)n}_{\geqslant 0} \geqslant n$.)

Als erste Anwendung des obigen Axioms zeigen wir folgende Aussage:

**Satz 2.7** (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* $0 \leqslant r < m$*. Hier sind* $q, r$ *eindeutig bestimmt. (Ist* $n \geqslant 0$*, so auch* $q \geqslant 0$*.)*

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

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

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

(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:

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

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

Dieses "so lange ... bis" scheint intuitiv klar. Typischerweise benötigt man allerdings das Peano Axiom für einen formalen Beweis. Wir führen dies hier einmal explizit aus.

*Beweis von Satz 2.7.* 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 $q_0 \in \mathbb{N}_0$ 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

$$r := n - (q_0 + 1)m = n - q_0 m - m = r_0 - m \geqslant 0, \qquad \text{also auch } r \in A.$$

Aber $r = r_0 - m < r_0$, und damit 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.

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 $r = n - qm = n - q'm = r'$. □

**Beispiel 2.8.** Eine Anwendung: Prüfziffern bei IBAN

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

(Deutsche) Konto-Nr. 0356843503
Bankleitzahl (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 | ... | Z |
|---|---|---|---|---|---|
| 10 | 11 | 12 | 13 | ... | 35 |

- Berechne $370100500356843503\underline{131400} \bmod 97 = 86$; ziehe dies von 98 ab; Ergebnis ist 12. (Falls Ergebnis einstellig, ergänze führende Null.)

Weiteres Beispiel: Formeln zur Berechnung des Osterdatums $\rightsquigarrow$ Übung 2.

Zurück zur allgemeinen Theorie. Seien $d, n \in \mathbb{Z}$ gegeben mit $d \neq 0$ und $n \neq 0$. Gilt $d \mid n$, so folgt natürlich auch $(-d) \mid n$. Um alle Teiler $d$ von $n$ zu bestimmen, brauchen wir also nur den Fall $d > 0$ zu betrachten. Sei nun $d > 0$. Aus $d \mid n$ folgt offenbar auch $d \leqslant |n|$ (= Absolutbetrag von $n$); also hat $n$ nur endlich viele Teiler. Sind $n, m \in \mathbb{Z}$ mit $n \neq 0$ oder $m \neq 0$ gegeben, so definieren wir

$$\mathrm{ggT}(n, m) := \max\{a \in \mathbb{N} \mid a \text{ teilt } n \text{ und } a \text{ teilt } m\} \quad \text{"}\textbf{\textit{größter gemeinsamer Teiler}}\text{"}.$$

Gilt $\mathrm{ggT}(n, m) = 1$, so bezeichnen wir $m$ und $n$ als ***teilerfremd***.

**Lemma 2.9** (Lemma von Bézout). *Gegeben seien* $n, m \in \mathbb{Z}$ *mit* $n \neq 0$ *oder* $m \neq 0$. *Dann gibt es* $a, b \in \mathbb{Z}$ *mit* $\mathrm{ggT}(n, m) = an + bm$. *Ist auch* $d' \in \mathbb{Z}$ *ein gemeinsamer Teiler von* $n$ *und* $m$, *so folgt* $d' \mid \mathrm{ggT}(n, m)$.

*Beweis.* Ist $n = 0$ oder $m = 0$, so ist die Aussage sehr einfach zu sehen. (Ist z.B. $n = 0$ und $m < 0$, so ist $-m = \mathrm{ggT}(n, m) = 0 \cdot n + (-1) \cdot m$.) Sei also jetzt $n \neq 0$ und $m \neq 0$. Wir beschreiben einen Algorithmus, genannt (erweiterter) ***Euklidischer Algorithmus***, zur Bestimmung von $\mathrm{ggT}(n, m)$ und $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(n, m) = an + bm$. Dazu berechnen wir rekursiv eine endliche Folge von Tripeln $(r_k, a_k, b_k)$ für $k = 0, 1, 2, 3, \ldots$, wie folgt. Ist $n > 0$ und $m > 0$, so initialisieren wir $r_0 := n,\ a_0 := 1,\ b_0 := 0$ und $r_1 := m,\ a_1 := 0,\ b_1 := 1$. (Ist $n < 0$, so setze $r_0 := -n, a_0 := -1, b_0 := 0$; ist $m < 0$, so setze $r_1 := -m$, $a_1 := 0$, $b_1 := -1$.) In jedem Fall gilt dann $r_0 = a_0 n + b_0 m \geqslant 1$ und $r_1 = a_1 n + b_1 m \geqslant 1$. Sei nun $k \geqslant 1$ und $r_i, a_i, b_i$ bereits konstruiert für $0 \leqslant i \leqslant k$, wobei jeweils $r_i = a_i n + b_i m \geqslant 1$ gelte. Division mit Rest liefert

$$r_{k-1} = q_k r_k + r_{k+1} \qquad \text{mit} \qquad q_k, r_{k+1} \in \mathbb{Z} \quad \text{und} \quad 0 \leqslant r_{k+1} < r_k;$$

dies definiert $r_{k+1}$; dann setze $a_{k+1} := a_{k-1} - q_k a_k$ und $b_{k+1} := b_{k-1} - q_k b_k$. Damit gilt wieder

$$r_{k+1} = r_{k-1} - q_k r_k = (a_{k-1} n + b_{k-1} m) - q_k (a_k n + b_k m) = a_{k+1} n + b_{k+1} m.$$

Dieses Verfahren wird so lange fortgesetzt, bis $r_{k+1} = 0$ gilt. (Wegen $r_1 > r_2 > \ldots \geqslant 0$ muss es ein solches $k$ geben. Hier ist wieder ein solcher Fall von "so lange ... bis"; überlegen Sie sich selbst, wie man dies hier mit Hilfe des Peano Axioms formal rechtfertigt.) Dann ist $r_k > 0$ und $r_{k-1} = q_k r_k$. Im vorherigen Schritt ist $r_{k-2} = q_{k-1} r_{k-1} + r_k$; wegen $r_k \mid r_{k-1}$ folgt also auch $r_k \mid r_{k-2}$. Dies setzt sich entsprechend in alle vorherigen Schritte fort, also gilt $r_k \mid r_i$ für $0 \leqslant i \leqslant k-1$. Insbesondere ist $r_k \mid n = \pm r_0$ und $r_k \mid m = \pm r_1$, also $r_k \leqslant \mathrm{ggT}(n, m)$. Wegen $r_k = a_k n + b_k m$ folgt aber auch $d \mid r_k$ für jeden gemeinsamen Teiler $d$ von $n$ und $m$. Also ist $\mathrm{ggT}(n, m) = r_k = a_k n + b_k m$. (Für mehr Details siehe `https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm`). □

Sei zum Beispiel $n = 1071$ und $m = 462$. Dann initialisieren wir $r_0 = 1071$, $a_0 = 1$, $b_0 = 0$ und $r_1 = 462$, $a_1 = 0$, $b_1 = 1$. Das obige Verfahren liefert nun nacheinander:

$$\begin{aligned}
r_0 &= 1071 = 2 \cdot 462 + 147 = q_1 r_1 + r_2, && \text{also } q_1 = 2,\ r_2 = 147 \text{ und } a_2 = 1,\ b_2 = -2,\\
r_1 &= \ \ 462 = 3 \cdot 147 + 21 \ \ = q_2 r_2 + r_3, && \text{also } q_2 = 3,\ r_3 = 21 \ \ \text{und } a_3 = -3,\ b_3 = 7,\\
r_2 &= \ \ 147 = 7 \cdot 21 + 0 \ \ \ \ = q_3 r_3 + r_4, && \text{also } q_3 = 7,\ r_4 = 0.
\end{aligned}$$

Damit bricht das Verfahren bei $k = 3$ mit $r_3 = 21$, $a_3 = -3$, $b_3 = 7$ ab und wir erhalten $21 = \mathrm{ggT}(1071, 462) = (-3) \cdot 1071 + 7 \cdot 462$. Versuchen Sie, dieses Verfahren möglichst effizient zu programmieren (in Python oder einer beliebigen anderen Programmiersprache).

Als nächstes betrachten wir 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: $x = 2/3 = 4/6 = 100/150$.)
- Ist $x = n/m \in \mathbb{Q}$ und teilt man den Zähler und Nenner durch $\mathrm{ggT}(n, m)$, so erhält man einen "gekürzten" Bruch $x = n'/m'$ mit $n' \in \mathbb{Z}$, $m' \in \mathbb{N}$ und $\mathrm{ggT}(n', m') = 1$. (Im Beispiel oben ist $2/3$ gekürzt, $4/6$ und $100/150$ sind nicht gekürzt.)
- 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 $y - x \geqslant 0$ $\quad\rightsquigarrow\quad$ Anordnung von $\mathbb{Q}$.

Hier ist nun das klassische Beispiel eines Widerspruchsbeweises.

**Satz 2.10** (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.

Wir nehmen 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., beide durch $k = 2$ teilbar, im Widerspruch zur Annahme, dass $x = n/m$ gekürzt ist. □

## 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 (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 3.2.** Wir sehen hier gleichzeitig eine Stärke und eine Schwäche der vollständigen Induktion. Ist bereits bekannt, was man zeigen will, so ist dies 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. (Siehe dazu auch `https://de.wikipedia.org/wiki/Faulhabersche_Formel`)

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

**Satz 3.3** (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 Beweis von Satz 3.1 etwas zu verändern. Angenommen, 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 3.4.** 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 3.5** (Primfaktorzerlegung in $\mathbb{N}$)**.** *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 $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_r$.*

*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 die Faktoren im Endprodukt der Größe nach um. □

**Satz 3.6** (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 3.5 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 3.7.** 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 $F_n := 2^{2^n}+1$ 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 3.8** ("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 von Lemma 3.8.* 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*** 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 3.9.** *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 3.8 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 3.10** (Hauptsatz der elementaren Arithmetik)**.** *Die Primfaktorzerlegung einer natürlichen Zahl* $n \geqslant 2$ *(siehe Satz 3.5) 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:

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

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 3.9 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: $p_1 > q_1$. Man erhält Widerspruch völlig analog zum 2. Fall. (Es ist $q_1 \mid p_1 \cdots p_r$ usw.)

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

**Ab hier Woche 3**

## 4. *Relationen und Restklassen*

Wir führen eine weitere grundlegende mengentheoretische Konstruktion ein. Das ***kartesische Produkt*** von zwei nicht-leeren Mengen $A$ 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 Paare $(a, b)$ und $(a', b')$ gilt $(a, b) = (a', b')$ genau dann, wenn $a = a'$ und $b = b'$. (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:

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

*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 $0 \leqslant r, r' < m$. Sei zuerst $(a, b) \in R_m$, d.h., $r = r'$. Dann folgt $a - qm = r = r' = b - q'm$ und damit $b - a = (q' - q)m$; also ist $m \mid b - a$. Sei umgekehrt $m \mid b - a$, also $b - a = cm$ mit $c \in \mathbb{Z}$, also $b = cm + a = cm + qm + r = (c + q)m + r$. Aus der Eindeutigkeit des Restes folgt also $r = r'$ und damit $(a, b) \in R_m$. □

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;
- ***anti-symmetrisch***, wenn für $a, b \in A$ aus $a \sim b$ und $b \sim a$ stets $a = b$ 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***.
Ist $R$ reflexiv, anti-symmetrisch und transitiv, so heißt $R$ eine ***Ordnungsrelation***.

**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) Die übliche Relation "$\leqslant$" auf $A = \mathbb{Z}$ ist eine Ordnungsrelation.

(c) Sei $A = \mathbb{Z}$ und $m \in \mathbb{N}$ fest. Wir behaupten, dass die Kongruenz-Relation $R_m$ in Beispiel 4.3 eine Äquivalenzrelation ist. Prüfen wir dies nach. Die Relation 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 $a \sim c$.

**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 $a, b \in A$ 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. In dieser Vereinigung sind im Allgemeinen viele Terme gleich. Sind $a, b \in A$, so gilt $K_a = K_b \Leftrightarrow b \in K_a$.

**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:

$$R := \big\{\big((n, m), (n', m')\big) \in A \times A \mid nm' = n'm\big\}.$$

(Nach Übung 3 ist dies eine Äquivalenzrelation.) Für $(n, m) \in A$ schreiben wir anstelle von $K((n, m), R)$ einfach kurz $n/m$. Mit Hilfe des ggT sieht man leicht, 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 Übung 3 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* $\mathbb{Q} := \mathcal{K}(A, R)$.

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 $\mathbb{Z}$ aus $\mathbb{N}$ konstruiert.)

**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 $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}$.
Es ist $-17 \in \overline{3}$ und $38 \in \overline{3}$ (weil $-17$ und $38$ beide 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 $\overline{n}$. Seien $a, b, c, d \in \mathbb{Z}$. Gilt $\overline{a} = \overline{c}$ und $\overline{b} = \overline{d}$, so folgt $\overline{a+b} = \overline{c+d}$ und $\overline{ab} = \overline{cd}$.*

*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., $\overline{ab} = \overline{cd}$. □

Sei zum Beispiel $m = 6$. 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 $(17 \cdot 14) \bmod 6 = 4$. (Man muss also nicht erst $17 \cdot 14$ ausrechnen und dann mit Rest durch 6 teilen.)

**Beispiel 4.12.** Ist 7513 durch 3 teilbar? Nach der (vielleicht bekannten) ***Dreierregel*** müssten wir uns dazu nur die Quersumme von 7513 anschauen:
Diese ist $7 + 5 + 1 + 3 = 16$, und wegen $3 \nmid 16$ folgt auch $3 \nmid 7513$.

Begründung: Sei $m = 3$ und betrachte $\overline{7513} = \overline{7 \cdot 1000 + 5 \cdot 100 + 1 \cdot 10 + 3}$.
Nun ist $10 \bmod 3 = 1$, also $\overline{10} = \overline{1}$. 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*

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. In Zeichen $f\colon A \to B$, $a \mapsto f(a)$.

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.
Die Abbildung $f$ heißt ***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 $f(a) \neq f(a')$.)
Die Abbildung heißt ***bijektiv***, wenn sie sowohl injektiv als auch surjektiv ist.

Ist $A = \mathbb{N}$, so bezeichnet man $f$ auch als ***Folge*** und schreibt vereinfachend $f = (a_n)_{n\in\mathbb{N}}$, wobei $a_n = f(n)$ für alle $n \in \mathbb{N}$. (Analog für $A = \mathbb{N}_0$.)

**Bemerkung 5.1.** (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 5.2.** (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 (wie Sie selbst leicht zeigen).

(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 $\quad f\colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0, \qquad (k, n) \mapsto 2^k(2n + 1) - 1$.
Wir überlassen es als Übung zu zeigen, dass diese Abbildung bijektiv ist.

**Definition 5.3.** 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 $A = \bigcup_{b \in B} f^{-1}(b)$.
Beispiel: $f\colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$, $(n, m) \mapsto n + m$, ist surjektiv. Es gilt
$f^{-1}(0) = \{(0,0)\}$, $f^{-1}(2) = \{(2,0), (1,1), (0,2)\}$,
$f^{-1}(\{\text{gerade Zahlen}\}) = \{(n, m) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid n, m \text{ beide gerade oder } n, m \text{ beide ungerade}\}$.

**Definition 5.4.** 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

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

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

**Lemma 5.5.** *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 $\Leftrightarrow$ 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) Es gebe $g\colon B \to A$ mit $f \circ g = \mathrm{id}_B$. Wir wollen zeigen, dass $f$ surjektiv ist. Sei dazu $b \in B$ 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 sei nun $f$ als bijektiv angenommen. 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 $a$; wir setzen $g(b) := a$. Dann folgt $g\big(f(a)\big) = a$ 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 5.6.** (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 $\mathbb{N} \subsetneqq \mathbb{N}_0$, 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 zunächst bei endlichen Mengen.

**Bemerkung 5.7.** 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 $f\colon \{1, \dots, n\} \to A$ gibt. Sei $m \in \mathbb{N}$ so, dass es eine bijektive Abbildung $g\colon \{1, \dots, m\} \to B$ gibt. Definiere dann die Abbildung $h\colon \{1, \dots, n+m\} \to A \cup B$ durch $h(i) := \begin{cases} f(i) & \text{falls } 1 \leqslant i \leqslant n, \\ g(i-n) & \text{falls } n < i \leqslant n+m. \end{cases}$
Man prüft 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 Vereingung 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 5.8.** *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 $A = \{a_1, \dots, a_n\}$ und $B = \{b_1, \dots, b_m\}$.

(a) Ist $f$ injektiv, so sind $f(a_1), \dots, f(a_n)$ 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 $j \in \{1, \dots, m\}$ ein $i_j \in \{1, \dots, n\}$ mit $f(a_{i_j}) = b_j$. Dann sind $a_{i_1}, \dots, a_{i_m} \in A$ 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. 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 5.7), 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 5.9.** 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 5.10.** 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 insgesamt $nm$ Möglichkeiten.

**Beispiel 5.11.** 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 5.12.** 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:

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

**Ab hier Woche 4**

**Definition 5.13.** 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 $n \in \mathbb{N}_0$. Ist $k > n$, so gilt offenbar $\binom{n}{k} = 0$.
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 5.14** (***Pascal–Dreieck***, um 1655)**.** *Für alle* $n, k \in \mathbb{N}$ *gilt* $\displaystyle\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

*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:

$$\begin{aligned}
T(n, k) &:= \text{Menge der Teilmengen von } \{1, \ldots, n\} \text{ mit genau } k \text{ Elementen},\\
T_1(n, k) &:= \{S \in T(n, k) \mid n \in S\}.\\
T_0(n, k) &:= \{S \in T(n, k) \mid n \notin S\} = T(n-1, k) \qquad (\text{für } n \geqslant 2).
\end{aligned}$$

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 5.7 erhalten wir

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

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

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

Dann sind $f \circ g$ und $g \circ f$ jeweils die identischen Abbildungen, also ist $f$ bijektiv (siehe Lemma 5.5(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 5.15.** *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.* (Vollständige Induktion über $n$ mit Startwert $n_0 = 1$.) Induktionsanfang: Für $n = 1$ $\binom{1}{1} = 1!/(1!0!)$ und $\binom{1}{0} = 1!/(0!1!)$. Induktionsschritt: Sei nun $n \geqslant 2$ und die Behauptung bereits für $n-1$ bewiesen. Sei $0 \leqslant k \leqslant n$. Ist $k = n$, so gilt $\binom{n}{n} = 1 = n!/(n!0!)$, also die Behauptung. Sei nun $0 \leqslant k \leqslant n-1$. Nach Induktion und mit Satz 5.14 erhält man

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!((n-1)-(k-1))!} + \frac{(n-1)!}{k!(n-1-k)!}.$$

Mit einer einfachen Rechnung sieht man, dass die rechte Seite gleich $n!/(k!(n-k)!)$ ist. □

**Lemma 5.16.** *Sei* $n \in \mathbb{N}$. *Dann ist* $n! = |\{f\colon \{1,\ldots,n\} \to \{1,\ldots,n\} \mid f \text{ bijektiv }\}|$.

*Beweis.* Um eine injektive Abbildung $f\colon \{1,\ldots,n\} \to \{1,\ldots,n\}$ zu definieren, gibt es zunächst $n$ Möglichkeiten für $f(1)$ (nämlich irgendeine der Zahlen $1,\ldots,n$).
Damit $f$ injektiv wird, gibt es dann noch $n-1$ Möglichkeiten für $f(2)$ (nämlich irgendeine der Zahlen $1,\ldots,n$ 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 $f(1),\ldots,f(n-1)$ 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 Lemma 5.8 ist jedes solche injektive $f$ automatisch bijektiv. □

Für mehr dazu siehe auch `https://de.wikipedia.org/wiki/Abzählende_Kombinatorik`.

## 6. *Unendliche Mengen*

In diesem (kurzen) Abschnitt stellen wir einige Aussagen und Beispiele zu Mengen mit unendlich vielen Elementen zusammen, die teilweise ziemlich verblüffend sind. Zunächst gibt es zwei Arten von "Unendlichkeit". 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 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 5.2(d);
- $\mathbb{Q}$ ist ebenfalls abzählbar (siehe Übungen).

Wir werden im nächsten Kapitel sehen, dass $\mathbb{R}$ überabzählbar ist. Weiteres Beispiel (das wirklich Erstaunliche am folgenden Satz ist der genial einfache Beweis):

**Satz 6.1** (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.*
*Insbesondere ist die Potenzmenge $\mathcal{P}(\mathbb{N})$ 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: $a \in f(a) \Leftrightarrow a \in B \Leftrightarrow a \notin f(a)$. Also erhalten wir einen Widerspruch.

Nun betrachte $A = \mathbb{N}$. 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 6.2.** *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 $A_3 := A_2 \setminus \{a_2\} = A \setminus \{a_0, a_1, a_2\}, \ldots$ 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).

Das erste dieser Hilfsmittel hat mit ***rekursiven Definitionen*** zu tun, mit denen Sie vermutlich vertraut sind. Als Beispiel betrachten wir die Folge $(a_n)_{n\in\mathbb{N}}$ von natürlichen Zahlen, die nach folgendem Schema gebildet wird. Sei $a_1 \in \mathbb{N}$ ein fest gewählter Startwert und dann

$$a_{n+1} = \begin{cases} 3a_n + 1 & \text{falls } a_n \text{ ungerade,} \\ a_n/2 & \text{falls } a_n \text{ gerade.} \end{cases}$$

Mit $a_1 = 19$ erhält man z.B. die Folge $19, 58, 29, 88, 44, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, 4, 2, 1, \ldots$ (Übrigens: Versuchen Sie das Gleiche mit einem anderen $a_1$; fällt Ihnen etwas auf? Siehe dazu auch `https://de.wikipedia.org/wiki/Collatz-Problem`.)

Wenn man sich eine solche "Definition" genauer anschaut, so haben wir streng genommen lediglich eine Vorschrift, mit der man das jeweils nächste Folgenglied aus dem vorherigen berechnet. Dass man damit eine auf ganz $\mathbb{N}$ definierte Abbildung erhält, ist zunächst — und überhaupt — nicht klar. Die formale Begründung wird durch folgenden Satz geliefert.

**Satz 6.3** (Rekursionssatz)**.** *Sei* $A$ *eine nicht-leere Menge,* $a_0 \in A$ *fest. Für jedes* $n \in \mathbb{N}_0$ *sei eine Abbildung* $h_n \colon A \to A$ *gegeben. Dann gibt es genau eine Abbildung* $F \colon \mathbb{N}_0 \to A$ *mit*

$$F(0) = a_0 \qquad \textit{und} \qquad F(n+1) = h_n\big(F(n)\big) \quad \textit{für alle } n \in \mathbb{N}_0.$$

(Für einen formalen Beweis siehe §12 im Buch von Halmos.) Weiteres Beispiel:
Sei $A = \mathbb{Q}_{>0} := \{x \in \mathbb{Q} \mid x > 0\}$ 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 6.3. 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

$$a_{n+1} = F(n+1) = h(F(n)) = h(a_n) = \frac{1}{2}\Big(a_n + \frac{2}{a_n}\Big) \quad \text{für alle } n \geqslant 0.$$

Diese Folge kommt Ihnen vielleicht bekannt vor: Sie konvergiert gegen $\sqrt{2}$. (Mehr zu Grenzwerten folgt im 2. Semester.)
Die Abbildungen $h_n$ sind also die Vorschriften, mit denen man das jeweils nächste Folgenglied aus dem vorherigen berechnet; diese Abbildungen können sogar selbst von $n$ abhängen.

**Beispiel 6.4** (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

$$f_0 := 0, \qquad f_1 := 1 \qquad \text{und} \qquad f_{n+1} := f_n + f_{n-1} \quad \text{für alle } n \geqslant 1.$$

Also $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots, 12586269025\ (n = 50), \ldots$
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 $h(i,j) := (j, i+j)$ 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 erhält man:

$$F(1) = h(F(0)) = h(0,1) = (1,1), \qquad F(2) = h(F(1)) = h(1,1) = (1,2),$$
$$F(3) = h(F(2)) = h(1,2) = (2,3), \qquad F(4) = h(F(3)) = h(2,3) = (3,5), \qquad \dots$$

Schreibe nun $F(n) = (x_n, y_n)$ für alle $n \in \mathbb{N}_0$. Dann ist $x_0 = 0$, $y_0 = 1$ und $y_n = x_{n+1} = x_n + x_{n-1}$ für alle $n \geqslant 1$. Also ist $f_n = x_n$ für alle $n \in \mathbb{N}_0$.

Das zweite Hilfsmittel ist ein weiteres, berühmtes Axiom der Mengenlehre.

**Axiom 6.5** (***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 $\alpha$ heißt ***Auswahlfunktion***, denn sie "wählt" aus jeder nicht-leeren Teilmenge $B \subseteq A$ ein Element $\alpha(B) \in B$ aus.

**Beispiel.** Sei $A = \mathbb{N}$. Hier ist eine Auswahlfunktion $\alpha\colon \mathcal{P}(\mathbb{N})^\natural \to \mathbb{N}$ 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 (vor allem wenn man mit unendlichen Mengen zu tun) gar nicht konkret hinschreiben oder mit einer expliziten Formel bestimmen kann. Für eine weitere Diskussion siehe

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

Skizzieren wir kurz, wie man damit Satz 6.2 beweist. Sei also $A \neq \varnothing$ und $|A| = \infty$. Zu zeigen: Es gibt eine injektive Abbildung $f\colon \mathbb{N}_0 \to A$. Nun, nach dem Auswahlaxiom gibt es eine Auswahlfunktion $\alpha\colon \mathcal{P}(A)^\natural \to A$. Sei $a_0 := \alpha(A)$. Mit Hilfe des Rekursionssatzes können wir dann eine Folge $(a_n)_{n\in\mathbb{N}_0}$ definieren mit

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

Dann gilt $a_{n+1} \notin \{a_0, a_1, \dots, a_n\}$ für alle $n \geqslant 0$, also sind die Elemente $a_0, a_1, a_2, \dots$ in $A$ alle verschieden. Damit ist $f\colon \mathbb{N}_0 \to A$, $n \mapsto a_n$, die gesuchte injektive Abbildung. □

Zum Schluss noch eine weitere verblüffende Eigenschaft von unendlichen Mengen:

**Folgerung 6.6** (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 $|A| = |B|$.*

*Beweis.* Sei zuerst angenommen, dass es eine Teilmenge $B \subsetneq A$ 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 $A$ als unendlich angenommen. Nach Satz 6.2 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 ist $|A| = |B|$ aber $B \subsetneq A$. □

# Kapitel II: Zahlensysteme

## 7. *Verknüpfungen*

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 7.1.** (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 $b \in A$, 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 7.2.** 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. Abel), 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 7.3.** 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.:

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

Sei $(A, +, \cdot)$ ein Ring. Gibt es ein neutrales Element $1 \in A$ bezüglich "$\cdot$", so heißt $A$ ein ***Ring mit*** $1$. Ist die Multiplikation "$\cdot$" kommutativ, so heißt $A$ ein ***kommutativer Ring***.

Ein kommutativer Ring $A$ mit $1$, in dem $1 \neq 0$ gilt und jedes Element $0 \neq a \in A$ ein Inverses bezüglich "$\cdot$" besitzt, heißt ein ***Körper***. In diesem Fall wird das Inverse von $a \neq 0$ bezüglich der Multiplikation meist mit $a^{-1}$ bezeichnet (manchmal auch $1/a$).

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 7.4.** Sei $(R, +, \cdot)$ ein Ring. Dann gilt $0 \cdot r = r \cdot 0 = 0$ für alle $r \in R$. Denn

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

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

**Lemma 7.5** (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* $f\colon K \to K, \quad x \mapsto a \cdot x, \quad$ *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 7.4 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. □

Sie kennen vermutlich schon die Formel im folgenden Satz (für reelle Zahlen $a, b$); nachdem die obigen Begriffe eingeführt sind, können wir diese für beliebige Ringe mit $1$ beweisen.

**Satz 7.6** (***Binomischer Lehrsatz***)**.** *Sei* $R$ *ein Ring mit* $1$*. Seien* $a, b \in R$ *mit* $a \cdot b = b \cdot a$*. Dann gilt für alle* $n \in \mathbb{N}_0$*:*

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

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

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

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

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

(Hier haben wir benutzt, dass $a$ und $b$ miteinander vertauschbar sind.) 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

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

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

Damit erhalten wir

$$A + B = \binom{n}{0} b^{n+1} + \Big(\sum_{k=1}^{n} \Big( \underbrace{\binom{n}{k-1} + \binom{n}{k}}_{= \binom{n+1}{k} \text{ Pascal–Dreieck}} \Big) a^k \cdot b^{n+1-k}\Big) + \binom{n}{n} a^{n+1}$$

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

Wegen $\binom{n+1}{0} = \binom{n+1}{n+1} = 1$ ist dies genau die gewünschte Summe auf der rechten Seite. □

**Ab hier Woche 5**

**Beispiel 7.7.** Sei $A$ eine 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 5.14 (***Pascal–Dreieck***) sei $T(n, k) :=$ Menge der Teilmengen von $\{1, \ldots, n\}$ mit genau $k$ 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. □

**Folgerung 7.8** (***Kleiner Satz von Fermat***; um 1640)**.**
*Sei $p$ eine Primzahl. Dann gilt $n^p \equiv n \pmod{p}$ für alle $n \in \mathbb{Z}$.*

*Beweis.* Sei zuerst $n \geqslant 0$. Dann zeigen wir die Aussage mit vollständiger Induktion nach $n$. Für $n = 0$ ist dies klar. Sei nun $n \geqslant 0$ beliebig und angenommen, die Aussage gelte bereits für $n$. Dann müssen wir $n + 1$ betrachten. Mit dem Binomischen Lehrsatz erhalten wir:

$$(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k = 1 + \Big(\sum_{k=1}^{p-1} \binom{p}{k} n^k\Big) + n^p.$$

Betrachte nun $\binom{p}{k} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{1 \cdot 2 \cdot \ldots \cdot k} \in \mathbb{N}$ für $k \in \{1, \ldots, p-1\}$. Der Zähler dieses Bruches ist durch $p$ teilbar, aber wegen $1 \leqslant k \leqslant p-1$ ist der Nenner nicht durch $p$ teilbar. Also folgt $p \mid \binom{p}{k}$ für alle diese $k$ und die geklammerte Summe in obiger Formel ist $\equiv 0 \bmod p$. Nach Induktion ist $n^p \equiv n \bmod p$. Damit folgt $(n+1)^p \equiv 1 + n^p \equiv 1 + n \bmod p$, wie gewünscht.

Sei nun $n < 0$. Dann ist $-n > 0$, also wissen wir bereits, dass $(-1)^p n^p \equiv (-n)^p \equiv -n \bmod p$ gilt. Schließlich ist $(-1)^p \equiv -1 \bmod p$ für alle Primzahlen $p$ (unterscheide die Fälle $p = 2$ und $p > 2$), also folgt auch hier $n^p \equiv n \bmod p$. □

## 8. *Die ganzen und rationalen Zahlen und die Ringe* $\mathbb{Z}/m\mathbb{Z}$

Wir haben bereits oben festgehalten, dass $\mathbb{Z}$ ein kommutativer Ring mit $1$ und $\mathbb{Q}$ ein Körper ist, jeweils mit der üblichen Addition und Multiplikation; außerdem ist natürlich $\mathbb{Z} \subseteq \mathbb{Q}$ (indem wir $n \in \mathbb{Z}$ mit dem Bruch $n/1 \in \mathbb{Q}$ identifizieren).

In den meisten modernen Programmiersprachen kann man mit beliebig großen ganzen Zahlen exakt rechnen. Für rationale Zahlen ist dies auch möglich, indem man jedes $x \in \mathbb{Q}$ als gekürzten Bruch darstellt, also $x = n/m$ mit $n \in \mathbb{Z}$, $m \in \mathbb{N}$ und $\mathrm{ggT}(n, m) = 1$. Kommt in

einer Zwischenrechnung ein ungekürzter Bruch vor, so teilt man Zähler und Nenner durch ihren ggT und erhält wiederum einen gekürzten Bruch. Zum Beispiel:

$$3/22 + 9/10 = (3 \cdot 10 + 9 \cdot 22)/(22 \cdot 10) = (30 + 198)/220 = 228/220 = \ldots = 57/55.$$

In Python muss dazu ein extra-Paket geladen werden:

```
Python 3.9.7 (default, Aug 30 2021, 00:00:00)
>>> from fractions import Fraction
>>> Fraction(3,22)+Fraction(9,10)
Fraction(57, 55)
```

In GAP ist dies bereits eingebaut:

```
GAP 4.11.1 of 2021-03-02
gap> 3/22+9/10;
57/55
gap> Factorial(50);
30414093201713378043612608166064768844377641568960512000000000000
```

Wir sind daran gewohnt, natürliche Zahlen im üblichen Dezimalsystem darzustellen, also zum Beispiel: $53072 = 5 \cdot 10^4 + 3 \cdot 10^3 + 0 \cdot 10^2 + 7 \cdot 10 + 2$. Es handelt sich hier um ein ***Stellenwertsystem*** zur Basis 10. Genauso gut kann man auch andere Basen verwenden; vor allem in der Informatik ist die Basis 2 relevant. Die Grundlage dafür ist folgender Satz.

**Satz 8.1.** *Sei* $g \in \mathbb{N}$, $g \geqslant 2$, *fest. Dann lässt sich jede natürliche Zahl* $n \in \mathbb{N}$ *darstellen als*

$$n = a_d g^d + a_{d-1} g^{d-1} + \ldots + a_1 g + a_0 \text{ mit } d \in \mathbb{N}_0,\ a_0, \ldots, a_d \in \{0, 1, 2, \ldots, g-1\} \text{ und } a_d \neq 0.$$

*Hier sind* $d$ *und die "Ziffern"* $a_0, a_1, \ldots, a_d$ *eindeutig bestimmt.*

Man bezeichnet dies dann als "$g$-***adische Entwicklung***" $n = (a_d, \ldots, a_1, a_0)_g$. Zum Beispiel für $g = 2$ heißt dies ***Binärdarstellung***; für $g = 16$ die ***Hexadezimaldarstellung***.

*Beweis.* Zuerst einige Bezeichnungen. Für $d \in \mathbb{N}_0$ sei $I_d$ die Menge aller $(d+1)$-Tupel $(a_0, a_1, \ldots, a_d)$ mit $a_0, a_1, \ldots, a_d \in \{0, 1, 2, \ldots, g-1\}$ und $a_d \neq 0$. Wir erhalten dann eine Abbildung $f_d \colon I_d \to \mathbb{N}$ mit $f_d(a_0, a_1, \ldots, a_d) := a_d g^d + a_{d-1} g^{d-1} + \ldots + a_1 g + a_0$. Also besitzt $n \in \mathbb{N}$ eine $g$-adische Entwicklung, wenn es ein $d \in \mathbb{N}_0$ und $(a_0, a_1, \ldots, a_d) \in I_d$ gibt mit $n = f_d(a_0, a_1, \ldots, a_d)$. Insgesamt erhalten wir eine Abbildung

$$f \colon \bigcup_{d \in \mathbb{N}_0} I_d \to \mathbb{N}, \qquad (a_0, a_1, \ldots, a_d) \mapsto f_d(a_0, a_1, \ldots, a_d).$$

Zu beweisen ist dann, dass $f$ bijektiv ist. Zuerst zeigen wir mit Induktion nach $n$, dass $f$ surjektiv ist. Für $n = 1$ ist $n = f_0(1)$ im Bild von $f$. Sei nun $n \geqslant 2$ und bereits gezeigt, dass alle natürlichen Zahlen $< n$ im Bild von $f$ sind. Für $n$ selbst ergibt Teilen mit Rest durch $g$ dann $n = n'g + a_0$ mit $n', a_0 \in \mathbb{N}_0$ und $0 \leqslant a_0 < g$. Ist $n' = 0$, so ist $n = f_0(a_0)$

bereits im Bild von $f$. Sei nun $n' > 0$. Wegen $g \geqslant 2$ ist $n' < n$, also gilt nach Induktion $n' = f_{d'}(b_0, b_1, \ldots, b_{d'})$ mit einem $d' \in \mathbb{N}_0$ und $(b_0, b_1, \ldots, b_{d'}) \in I_{d'}$. Dann ist aber

$$\begin{aligned} n &= n'g + a_0 = (b_{d'}g^{d'} + b_{d'-1}g^{d'-1} + \ldots + b_1 g + b_0)g + a_0 \\ &= b_{d'}g^{d'+1} + b_{d'-1}g^{d'} + \ldots + b_1 g^2 + b_0 g + a_0 = f_{d'+1}(a_0, b_0, b_1, \ldots, b_{d'}). \end{aligned}$$

Also besitzt auch $n$ eine $g$-adische Entwicklung. Damit ist gezeigt, dass $f$ surjektiv ist. Betrachten wir nun genauer das Bild von $f_d$. Wegen $a_i \geqslant 0$ für alle $i$ und $a_d \geqslant 1$ gilt $f_d(a_0, a_1, \ldots, a_d) \geqslant a_d g^d \geqslant g^d$. Andererseits gilt wegen $a_i \leqslant g-1$ auch

$$\begin{aligned} f_d(a_0, a_1, \ldots, a_d) &\leqslant (g-1)g^d + (g-1)g^{d-1} + \ldots + (g-1)g + (g-1) \\ &= (g-1)(g^d + g^{d-1} + \ldots + g + 1) = g^{d+1} - 1, \end{aligned}$$

wobei wir die (hoffentlich) bekannte Formel für die geometrische Reihe $g^d + g^{d-1} + \ldots + g + 1 = (g^{d+1} - 1)/(g-1)$ benutzt haben. Also ist $f_d(a_0, a_1, \ldots, a_d)$ eine natürliche Zahl zwischen $g^d$ und $g^{d+1} - 1$, d.h.,

$$f_d(I_d) \subseteq I'_d \qquad \text{wobei} \qquad I'_d := \{g^d,\ g^d + 1,\ g^d + 2,\ \ldots,\ g^{d+1} - 1\} \subseteq \mathbb{N}.$$

Nun ist $\mathbb{N}$ die disjunkte Vereinigung aller $I'_d$. Da obiges $f$ surjektiv ist, so muss auch jedes $f_d \colon I_d \to I'_d$ surjektiv sein. Hier haben wir es nun mit endlichen Mengen zu tun. Man sieht sofort dass $|I_d| = g^d(g-1)$ und $|I'_d| = g^{d+1} - g^d = g^d(g-1) = |I_d|$ gilt. Also folgt mit Lemma 5.8(c), dass $f_d$ automatisch auch injektiv ist. Aber dann ist auch $f$ ingesamt injektiv, also die $g$-adische Zerlegung eindeutig. □

**Beispiel 8.2.** Der obige Beweis liefert ein Verfahren, wie man die $g$-adische Entwicklung bestimmt. Sei etwa $n = 2021$ und $g = 4$. Wiederholtes Teilen mit Rest durch 4 ergibt:

$$2021 = 505 \cdot 4 + 1, \quad 505 = 126 \cdot 4 + 1, \quad 126 = 31 \cdot 4 + 2, \quad 31 = 7 \cdot 4 + 3, \quad 7 = 1 \cdot 4 + 3.$$

Indem wir diese Formeln rückwärts ineinander einsetzen, erhalten wir

$$2021 = ((((1 \cdot 4 + 3) \cdot 4 + 3) \cdot 4 + 2) \cdot 4 + 1) \cdot 4 + 1 = \underline{1} \cdot 4^5 + \underline{3} \cdot 4^4 + \underline{3} \cdot 4^3 + \underline{2} \cdot 4^2 + \underline{1} \cdot 4^1 + \underline{1}.$$

Also ist $2021 = (133211)_4$ die 4-adische Entwicklung von 2021. Berechnen Sie als Übung analog die 2-adische oder 3-adische Zerlegung von 2021.

---

Nach all unseren Vorbereitungen im vorherigen Kapitel 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 $\overline{n} = \{a \in \mathbb{Z} \mid m \text{ teilt } n - a\} = \{a \in \mathbb{Z} \mid a \bmod m = n \bmod m\}$. Wie in Beispiel 4.10 ist $\{0, 1, \ldots, m-1\}$ 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 8.3.** *Mit obigen Bezeichnungen können wir für alle* $a, b \in \mathbb{Z}$ *wie folgt eine Addition und eine Multiplikation für die zugehörigen Restklassen definieren:*

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

*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 "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 $a, b, c \in \mathbb{Z}$:

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

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 7.5. 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 $\mathrm{ggT}(p, a) = 1$. Nach dem ***Lemma von Bézout*** 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. $\square$

**Definition 8.4.** 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 ***endlicher Körper mit*** $p$ ***Elementen***.

Zum Beispiel ist $\mathbb{F}_2 = \{\overline{0}, \overline{1}\}$ mit den 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 Körper spielt in der Informatik und in der Kodierungstheorie eine wichtige Rolle.

**Beispiel 8.5.** (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: $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{3}$, $\overline{3}^{-1} = \overline{2}$, $\overline{4}^{-1} = \overline{4}$.

**Beispiel 8.6.** Wir können nun auch einen neuen Beweis für den ***Kleinen Satz von Fermat*** geben. Sei also $p$ eine Primzahl und $n \in \mathbb{Z}$. Zu zeigen: $n^p \equiv n \bmod p$, oder anders ausgedrückt $\overline{n} = \overline{n^p} = \overline{n}^p$, wobei wir im Körper $\mathbb{F}_p$ rechnen.

Ist $\overline{n} = \overline{0}$, so ist die Aussage klar. Sei nun $\overline{n} \neq \overline{0}$. Dann betrachten wir die Abbildung $f\colon \mathbb{F}_p \to \mathbb{F}_p$, $\overline{x} \mapsto \overline{n} \cdot \overline{x}$. Diese ist injektiv nach Lemma 7.5 und Satz 8.3(b). Also ist $f$ bijektiv nach Lemma 5.8(c), d.h.,

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

Auf beiden Seiten kommt hier $\overline{0} = \overline{n} \cdot \overline{0}$ vor (siehe Bemerkung 7.4), also ist auch

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

Bilde das Produkt aller dieser Elemente:

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

Wegen $\overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{(p-1)} \neq \overline{0}$ (Lemma 7.5) können wir diesen Faktor auf beiden Seiten kürzen (noch einmal Lemma 7.5) und erhalten $\overline{1} = \overline{n}^{p-1}$, also $\overline{n} = \overline{n}^p$, wie gewünscht. □

## 9. *Polynome und Polynomfunktionen*

Sei $K$ ein Körper. Eine Funktion $f\colon K \to K$ heißt ***Polynomfunktion***, wenn es ein $n \in \mathbb{N}_0$ und Koeffizienten $a_0, a_1, a_2, \ldots, a_n \in K$ gibt mit

$$(*) \qquad f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \qquad \text{für alle } x \in K.$$

Ein bekanntes Beispiel ist sicherlich die Funktion $f\colon \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^2$ für alle $x \in \mathbb{R}$.

Sei $P(K)$ die Menge aller Polynomfunktionen $f\colon K \to K$. Für $n \in \mathbb{N}_0$ sei $P_n(K) \subseteq P(K)$ die Teilmenge aller $f$ wie oben, so dass $(*)$ gilt mit Koeffizienten $a_0, a_1, \ldots, a_n$. Sei $\hat{P}_n(K) \subseteq P_n(K)$ die Teilmenge aller $f$, so dass $(*)$ gilt mit $a_n \neq 0$.

**Satz 9.1** (***Horner–Schema***). *Sei $n \geqslant 1$ und $f \in \hat{P}_n(K)$, d.h., es gibt $a_0, a_1, \ldots, a_n \in K$ mit $a_n \neq 0$ und $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ für alle $x \in K$. Sei $c \in K$ fest und definiere rekursiv wie folgt Elemente in $K$:*

$$\begin{aligned} b_{n-1} &:= a_n, \qquad b_{n-2} := a_{n-1} + b_{n-1}c, \qquad b_{n-3} := a_{n-2} + b_{n-2}c, \\ &\ldots, \qquad b_1 := a_2 + b_2 c, \qquad b_0 := a_1 + b_1 c, \qquad r := a_0 + b_0 c. \end{aligned}$$

*Sei $g \in \hat{P}_{n-1}(K)$ definiert durch $g(x) := b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1 x + b_0$ für alle $x \in K$. Dann gilt $f(x) = (x-c)g(x) + r$ für alle $x \in K$. Insbesondere also $f(c) = r$.*

*Beweis.* Im Wesentlichen einfaches Nachrechnen. Für $x \in K$ gilt:

$$\begin{aligned} (x-c)g(x) &= (x-c)\sum_{i=0}^{n-1} b_i x^i = \sum_{i=0}^{n-1} b_i x^{i+1} - \sum_{i=0}^{n-1} b_i c x^i = \sum_{i=1}^{n} b_{i-1}x^i - \sum_{i=0}^{n-1} b_i c x^i \\ &= \underbrace{b_{n-1}}_{=a_n} x^n - \underbrace{b_0 c}_{r-a_0} + \sum_{i=1}^{n-1} \underbrace{(b_{i-1} - b_i c)}_{=a_i} x^i = f(x) - r. \end{aligned}$$

□

**Bemerkung.** Rechnet man $c, c^2, \ldots, c^n$ aus und dann $f(c) = a_n c^n + a_{n-1}c^{n-1} + \ldots + a_1 c + a_0$, so braucht man insgesamt $n$ Additionen und $2n-1$ Multiplikationen. Benutzt man das Horner-Schema, so benötigt man auch $n$ Additionen, aber nur $n$ Multiplikationen!
Sei zum Beispiel $f(x) = 2x^3 + 5x^2 - 11x - 3$.

Horner-Schema:

| Koeffs von $f$: | $2$ | $5$ | $-11$ | $-3$ |
|---|---|---|---|---|
| $c = 2$: | $\downarrow$ | $+2 \cdot 2 = 4$ | $+2 \cdot 9 = 18$ | $+2 \cdot 7 = 14$ |
| $g$: | $2$ | $9$ | $7$ | $\boxed{11}$ |

Dann ist $g(x) = 2x^2 + 9x + 7$ und $r = f(2) = 11$. — Nachrechnen:

$$(x-2)(2x^2 + 9x + 7) = 2x^3 + 9x^2 + 7x - 4x^2 - 18x - 14 = f(x) - 11.$$

**Folgerung 9.2.** *Sei $n \geqslant 1$ und $f \in \hat{P}_n(K)$. Dann hat $f$ höchstens $n$ Nullstellen in $K$.*
*(Nach Definition ist eine **Nullstelle** von $f$ ein Element $c \in K$ mit $f(c) = 0$.)*

*Beweis.* (Vollständige Induktion nach $n$.) Für $n = 1$ ist $f(x) = a_1x + a_0$ mit $a_1 \neq 0$. Also gibt es genau $n = 1$ Nullstelle, nämlich $c = -a_0a_1^{-1}$. Sei nun $n \geqslant 2$ und die Aussage bereits gezeigt für alle $g \in \hat{P}_{n-1}(K)$. Sei $f \in \hat{P}_n(K)$. Annahme: Es gibt paarweise verschiedene $c_1, \ldots, c_{n+1} \in K$ mit $f(c_i) = 0$ für $1 \leqslant i \leqslant n+1$. Nach Lemma 9.1 gibt es ein $g \in \hat{P}_{n-1}(K)$ mit $f(x) = (x - c_{n+1})g(x)$ für alle $x \in K$. Nach Induktion hat $g$ höchstens $n-1$ Nullstellen. Für $1 \leqslant i \leqslant n$ gilt dann aber $0 = f(c_i) = (c_i - c_{n+1})g(c_i)$. Wegen $c_i \neq c_{n+1}$ folgt also $g(c_i) = 0$ für $1 \leqslant i \leqslant n$, d.h., $g$ hat $n$ Nullstellen, Widerspruch. □

**Folgerung 9.3.** *Sei $n \geqslant 1$ und $|K| > n$. Dann lässt sich jedes $f \in P_n(K)$ auf eindeutige Weise wie in $(*)$ schreiben, d.h., es gibt eindeutige Koeffizienten $a_0, a_1, \ldots, a_n \in K$ mit $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ für alle $x \in K$.*

*Beweis.* Sei $f \in P_n(K)$. Gegeben seien $a_i, b_j \in K$ mit

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0 \quad \text{für alle } x \in K.$$

Setze $c_i := a_i - b_i$ für alle $i$ und definiere eine Polynomfunktion $g\colon K \to K$ durch $g(x) := c_nx^n + c_{n-1}x^{n-1} + \ldots + c_1x + c_0$ für alle $x \in K$. Dann gilt $g(x) = 0$ für alle $x \in K$.

Annahme, es gibt ein $i$ mit $a_i \neq b_i$, also $c_i \neq 0$. Sei dann $m := \max\{i \mid c_i \neq 0\}$. Wegen $m \leqslant n$, $c_m \neq 0$ und $c_i = 0$ für alle $i > m$ folgt $g \in \hat{P}_m(K)$. Nach Folgerung 9.2 hat $g$ höchstens $m$ Nullstellen. Aber alle Elemente von $K$ sind Nullstellen von $g$; also muss $|K| \leqslant m \leqslant n$ gelten, Widerspruch zur Voraussetzung. □

Die Aussage in Folgerung 9.3 wird tatsächlich falsch, wenn $K$ zu klein ist. Sei z.B. $K = \mathbb{F}_2$ und $f(x) = x^2 + x$ für alle $x \in K$. Dann ist $f \in P_2(\mathbb{F}_2)$ mit $f(\overline{0}) = \overline{0}$ und $f(\overline{1}) = \overline{1} + \overline{1} = \overline{0}$, d.h., es gilt $f(x) = \overline{0}$ für alle $x \in K$. Damit hat $f$ zwei Darstellungen wie in $(*)$; einmal mit Koeffizienten $(a_0, a_1, a_2) = (\overline{0}, \overline{1}, \overline{1})$ und einmal mit Koeffizienten $(b_0, b_1, b_2) = (\overline{0}, \overline{0}, \overline{0})$.

**Folgerung 9.4** (Polynominterpolation)**.** *Sei $n \in \mathbb{N}$. Gegeben seien paarweise verschiedene Elemente $x_1, \ldots, x_{n+1} \in K$ und beliebige Elemente $y_1, \ldots, y_{n+1} \in K$. Dann gibt es genau eine Polynomfunktion $f \in P_n(K)$ mit $f(x_i) = y_i$ für $i = 1, \ldots, n+1$.*

*Beweis.* Zur Existenz: Für $i = 1, 2, \ldots, n+1$ definieren wir $L_i \in P_n(K)$ durch

$$L_i(x) := \prod_{j \in \{1,\ldots,n+1\} \setminus \{i\}} \frac{x - x_j}{x_i - x_j} \qquad \text{für alle } x \in K.$$

(Beachte, dass man durch Ausmultiplizieren wirklich eine Polynomfunktion in $P_n(K)$ erhält.) Diese Funktionen heißen ***Lagrange–Polynomfunktionen***; sie haben folgende Werte, wie man sofort sieht: $L_i(x_j) = \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{falls } i \neq j. \end{cases}$

Definieren wir also $f \in P_n(K)$ durch $f(x) := \sum_{i=1}^{n+1} y_i L_i(x)$ für alle $x \in K$, so gilt $f(x_i) = y_i$ für $i = 1, \ldots, n+1$, wie gewünscht.

Zur Eindeutigkeit: Sind $f, g \in P_n(K)$ mit $f(x_i) = y_i = g(x_i)$ für $i = 1, \ldots, n+1$, so ist die Differenz $f - g$ eine Polynomfunktion in $P_n(K)$, die $n+1$ Nullstellen hat, muss also gleich $0$ sein nach Folgerung 9.2. □

Beispiel: Sei $n = 3$ und folgende Werte gegeben:

| $i$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $x_i$ | $-2$ | $-1$ | 1 | 2 |
| $y_i$ | 1 | 3 | $-3$ | 2 |

. Dann ist

$$L_1(x) = \tfrac{(x+1)(x-1)(x-2)}{(-1)\cdot(-3)\cdot(-4)},\ L_2(x) = \tfrac{(x+2)(x-1)(x-2)}{1\cdot(-2)\cdot(-3)},\ L_3(x) = \tfrac{(x+2)(x+1)(x-2)}{3\cdot2\cdot(-1)},\ L_4(x) = \tfrac{(x+2)(x+1)(x-1)}{4\cdot3\cdot1}$$

und damit $f(x) = 1 \cdot L_1(x) + 3 \cdot L_2(x) - 3 \cdot L_3(x) + 2 \cdot L_4(x) = \ldots = \frac{13}{12}x^3 + \frac{1}{2}x^2 - \frac{49}{12}x - \frac{1}{2}$.

---

Aus verschiedenen Gründen (etwa um die obigen Schwierigkeiten mit zu kleinen Körpern zu vermeiden) ist es sinnvoll, "abstrakte" Polynome anstelle von Polynomfunktionen einzuführen. Was hat man darunter zu verstehen? — Informelle Antwort: Ein "formaler" Ausdruck der Form $x^3 + x$, wobei man für $x$ irgendwelche Werte einsetzen kann. Man kann solche Ausdrücke addieren und multiplizieren (mit den üblichen Rechenregeln), zum Beispiel:

$(2x^2 - 1) + (x^3 + x) = x^3 + 2x^2 + x - 1$ und

$(2x^2 - 1) \cdot (x^3 + x) = 2x^5 + 2x^3 - x^3 - x = 2x^5 + x^3 - x$.

Aber was genau ist ein "formaler" Ausdruck, und woraus soll man Werte einsetzen können? Vielleicht hilft es, sich die allgemeine Form eines solchen Ausdrucks vorzustellen; diese sollte so aussehen: $a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, wobei $n \in \mathbb{N}_0$ und $a_0, a_1, \ldots, a_n \in K$. Letztlich relevant scheinen also eigentlich nur die Koeffizienten $a_0, a_1, a_2, \ldots, a_n$ zu sein. Diese Beobachtung wird tatsächlich zur Grundlage einer ordentlichen Definition.

**Ab hier Woche 6**

Sei $K$ beliebiger Körper; wir betrachten die Menge $\mathcal{F} = \mathrm{Abb}(\mathbb{N}_0, K)$. Jedes $f \in \mathcal{F}$ schreiben wir als Folge $f = (a_n)_{n \geqslant 0}$ (oder einfach $(a_n)$), wobei $a_n = f(n)$ für alle $n \geqslant 0$. Addition und Multiplikation mit einem Skalar $s \in K$ seien gegeben durch:

$$(a_n) + (b_n) := (a_n + b_n) \qquad \text{und} \qquad s.(a_n) := (s a_n).$$

Man rechnet leicht nach, dass damit $(\mathcal{F}, +)$ eine abelsche Gruppe ist. Das neutrale Element bezüglich der Addition ist $\underline{0} = (0, 0, 0, \ldots)$. Für $f, g \in \mathcal{F}$ definieren wir auch ein Produkt $f * g \in \mathcal{F}$ wie folgt: Seien $f = (a_n)$ und $g = (b_n)$; für $n \geqslant 0$ sei

$$c_n := \sum_{i=0}^{n} a_i b_{n-i} = a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \ldots + a_{n-1} b_1 + a_n b_0.$$

Dann setze $f * g := (c_n)$. Diese Verknüpfung heißt ***Konvolution***, oder auch ***Faltung***.

Beispiel: $(-1,0,2,0,0,\ldots)*(0,1,0,1,0,0,\ldots) = (0,-1,0,1,0,2,0,0,\ldots)$, denn $c_0 = a_0b_0 = 0$, $c_1 = a_0b_1 + a_1b_0 = -1$, $c_2 = a_0b_2 + a_1b_1 + a_2b_0 = 0$, usw.

Wir sagen, dass $f = (a_n) \in \mathcal{F}$ endlich ist, wenn es ein $n_0 \geqslant 0$ gibt mit $a_n = 0$ für alle $n > n_0$. In diesem Fall schreiben wir $f$ einfach als $f = (a_0, a_1, \ldots, a_{n_0}, 0, \ldots)$. Ist $f \neq \underline{0}$, so heißt $\mathrm{Grad}(f) := n_0 = \max\{n \in \mathbb{N}_0 \mid a_n \neq 0\}$ der ***Grad*** von $f$ und $a_{n_0}$ der ***Leitkoeffizient*** von $f$. Ist hier $a_{n_0} = 1$, so heißt $f$ ***normiert***.

**Lemma 9.5.** *Sei* $\mathcal{F}_0 := \{f \in \mathcal{F} \mid f \text{ ist endlich}\} \subseteq \mathcal{F}$. *Seien* $f, g \in \mathcal{F}_0$. *Dann gilt:*
(a) *Es ist auch* $sf \in \mathcal{F}_0$ *für* $s \in K$, $f + g \in \mathcal{F}_0$ *und* $f * g \in \mathcal{F}_0$.
(b) *Sind* $f, g \neq \underline{0}$ *und* $f + g \neq \underline{0}$, *so gilt* $\mathrm{Grad}(f+g) \leqslant \max\{\mathrm{Grad}(f), \mathrm{Grad}(g)\}$.
(c) *Sind* $f, g \neq \underline{0}$, *so gilt* $f * g \neq 0$ *und* $\mathrm{Grad}(f * g) = \mathrm{Grad}(f) + \mathrm{Grad}(g)$.

*Beweis.* Seien $f = (a_n)$ und $g = (b_n)$ in $\mathcal{F}_0$. Ist $f = \underline{0} = (0,0,\ldots)$, so ist $f + g = g \in \mathcal{F}_0$ und $sf = \underline{0} \in \mathcal{F}_0$; ebenso $f * g = \underline{0} \in \mathcal{F}_0$. Analog: Ist $g = \underline{0}$, so sind $f + g = f \in \mathcal{F}_0$ und $f * g = \underline{0} \in \mathcal{F}_0$. Seien nun also $f \neq \underline{0}$ und $g \neq \underline{0}$.

Seien $n_0 = \mathrm{Grad}(f)$ und $m_0 = \mathrm{Grad}(g)$; also $f = (a_0, a_1, \ldots, a_{n_0}, 0, \ldots)$ mit $a_{n_0} \neq 0$, und $g = (b_0, b_1, \ldots, b_{m_0}, 0, \ldots)$ mit $b_{m_0} \neq 0$. Dann ist offensichtlich $sf = (sa_0, sa_1, \ldots, sa_{n_0}, 0, \ldots) \in \mathcal{F}_0$ für $s \in K$. Ist $d_0 = \max\{n_0, m_0\}$, so gilt $f+g = (a_0+b_0, a_1+b_1, \ldots, a_{d_0}+b_{d_0}, 0, \ldots) \in \mathcal{F}_0$. Ist $f + g \neq \underline{0}$, so ist damit $\mathrm{Grad}(f+g) \leqslant d_0$, also gilt (b).

Nun betrachte $f * g = (c_n)$. Ist $c_n = \sum_{i=0}^{n} a_i b_{n-i} \neq 0$, so gibt es ein $i$ mit $a_i \neq 0$ und $b_{n-i} \neq 0$, d.h., $i \leqslant n_0$ und $n - i \leqslant m_0$, also $n \leqslant m_0 + i \leqslant m_0 + n_0$. Also folgt $f * g = (c_0, c_1, \ldots, c_{n_0+m_0}, 0, \ldots) \in \mathcal{F}_0$, d.h., es gilt (a). Betrachten wir nun den Koeffizienten $c_{n_0+m_0} = \sum_{i=0}^{n_0+m_0} a_i b_{n_0+m_0-i}$. Ist in dieser Summe $i > n_0$, so folgt $a_i = 0$. Ist $i < n_0$, so ist $n_0 + m_0 - i > m_0$, also $b_{n_0+m_0-i} = 0$. Also bleibt nur $i = n_0$ übrig und es folgt $c_{n_0+m_0} = a_{n_0} b_{m_0} \neq 0$. Also $f * g \neq \underline{0}$ und $\mathrm{Grad}(f * g) = n_0 + m_0$. Damit gilt auch (c). □

**Bemerkung 9.6.** (a) $e := (1,0,0,\ldots) \in \mathcal{F}_0$ ist das neutrale Element bezüglich $*$.
(b) Ist $X := (0,1,0,0,\ldots) \in \mathcal{F}_0$, so gilt $X * (a_n) = (0, a_0, a_1, a_2, \ldots)$.

*Beweis.* (a) Es gilt $e * (a_n) = (c_n)$ mit $c_n = \sum_{i=0}^{n} e_i a_{n-i} = e_0 a_n + e_1 a_{n-1} + \ldots + e_n a_0 = a_n$.
(b) Es ist $X * (a_n) = (c_n)$ mit $c_n = \sum_{i=0}^{n} X_i a_{n-i} = X_0 a_n + X_1 a_{n-1} + X_2 a_{n-2} + \ldots + X_n a_0$. Dies ist gleich $0$ falls $n = 0$, und gleich $a_{n-1}$ falls $n \geqslant 1$. □

**Definition 9.7** ("Abstrakte" Polynome über $K$)**.** Bezeichnen wir $X := (0,1,0,0,\ldots) \in \mathcal{F}_0$ wie oben, so schreiben wir auch $K[X] := \mathcal{F}_0$. Dann definieren wir $X^0 := e = (1,0,0,\ldots)$ und $X^n := X * X^{n-1}$ für alle $n \in \mathbb{N}$, also

$$X^1 := X, \quad X^2 := X * X = (0,0,1,0,0,\ldots), \quad X^3 := X * X^2 = (0,0,0,1,0,0,\ldots), \quad \ldots$$

Ist $f = (a_n) \in \mathcal{F}_0$ und $n_0 \geqslant 0$ mit $f = (a_0, a_1, \ldots, a_{n_0}, 0, \ldots)$, so erhalten wir eine eindeutige

Darstellung $f = \sum_{i=0}^{n_0} a_i X^i = a_{n_0} X^{n_0} + a_{n_0-1} X^{n_0-1} + \ldots + a_1 X + a_0$.
(Hier schreiben wir einfach $a_i X^i$ anstelle von $a_i . X^i$; außerdem werden die Terme $a_i X^i$ meist nach absteigendem Exponenten von $X$ geschrieben, aber die Reihenfolge ist letztlich egal.) Die Elemente von $K[X] = \mathcal{F}_0$ heißen ***Polynome*** in der ***Unbestimmten*** $X$. (Wir könnten auch irgendein anderes Symbol anstelle von $X$ nehmen; dies ist immer nur ein Name für die Folge $(0, 1, 0, 0, \ldots) \in \mathcal{F}_0$.) Schließlich: Wir fassen $K$ als Teilmenge von $K[X] = \mathcal{F}_0$ auf, indem wir ein Element $a \in K$ mit $ae = aX^0 = (a, 0, 0, \ldots) \in \mathcal{F}_0$ identifizieren.

**Lemma 9.8.** *Mit den oben definierten Verknüpfungen "+" und "∗" ist $K[X] = \mathcal{F}_0$ ein kommutativer Ring mit $1$. Sind $f, g \in \mathcal{F}_0$ und $s \in K$, so gilt $(s.f) * g = s.(f * g) = f * (s.g)$.*

*Beweis.* Etwas langwieriges (aber letztlich einfaches) Nachrechnen aller Ringaxiome. □

Gegeben seien Polynome $f = a_{n_0} X^{n_0} + a_{n_0-1} X^{n_0-1} + \ldots + a_1 X + a_0$ und $g = b_{m_0} X^{m_0} + b_{m_0-1} X^{m_0-1} + \ldots + b_1 X + b_0$. Die Tatsache, dass $K[X]$ ein Ring ist und die Formeln in Lemma 9.8 gelten, bedeutet dann, dass wir $f * g$ einfach wie folgt ausmultiplizieren können:

$$f * g = \sum_{i=0}^{n_0} \sum_{j=0}^{m_0} (a_i X^i) * (b_j X^j) = \sum_{i=0}^{n_0} \sum_{j=0}^{m_0} (a_i b_j)(X^i * X^j) = \sum_{i=0}^{n_0} \sum_{j=0}^{m_0} a_i b_j X^{i+j}.$$

Am Ende fasst man die Terme $a_i b_j X^{i+j}$ mit gleichem Exponenten von $X$ zusammen. (Man braucht sich also gar nicht an die genaue Definition von $*$ zu erinnern.)

**Bemerkung 9.9.** Sei $f = a_{n_0} X^{n_0} + a_{n_0-1} X^{n_0-1} + \ldots + a_1 X + a_0 \in K[X]$. Dann erhalten wir eine Polynomfunktion $\dot{f} \in P(K)$ mit $\dot{f}(x) := a_{n_0} x^{n_0} + a_{n_0-1} x^{n_0-1} + \ldots + a_1 x + a_0$ für $x \in K$.

Zum Beispiel: Ist $K = \mathbb{F}_2$ und $f = X^2 + X \in K[X]$, so ist $\dot{f}(x) = x^2 + x = 0$ für $x \in K$. Hier ist $f \neq \underline{0}$, aber $\dot{f}$ ist die Null-Funktion. (Unterschied Polynome $\leftrightarrow$ Polynomfunktionen!)

Ist $s \in K$, so schreiben wir auch einfach $f(s)$ anstelle von $\dot{f}(s)$. In diesem Sinne haben wir also $s$ in $f$ "eingesetzt". Für dieses Einsetzen gelten die Regeln $(f + g)(s) = f(s) + g(s)$ und $(f * g)(s) = f(s)g(s)$ für alle $f, g \in K[X]$ (wie man leicht nachrechnet).

**Bemerkung 9.10.** Analog zu Satz 9.1 gibt es auch ein Horner-Schema für Polynome: Ist $\underline{0} \neq f \in K[X]$ mit $n = \mathrm{Grad}(f) \geqslant 1$, so gilt $f = (X - c) * g + f(c)$, wobei $\underline{0} \neq g \in K[X]$ mit $\mathrm{Grad}(g) = n - 1$. Ist $f(c) = 0$, so heißt $c$ eine ***Nullstelle*** von $f$; in diesem Fall ist also $f = (X - c) * g$. Wie in Folgerung 9.2 sieht man, dass $f$ höchstens $n$ Nullstellen hat.

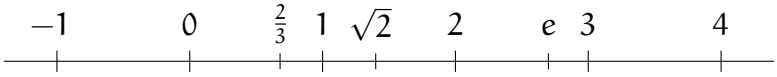
Noch einmal: Polynome in $K[X] = \mathcal{F}_0$ und Polynomfunktionen in $P(K)$ sind zwei völlig verschiedene Objekte! Ein Polynom in $K[X]$ ist letztlich nur die Folge $f = (a_0, a_1, \ldots, a_{n_0}, 0, \ldots)$

seiner Koeffizienten, und keine Funktion $K \to K$ ! Genauso werden Polynome in Computer-Algebra-Systemen (wie z.B. GAP oder Sage) realisiert, nämlich intern durch endlich lange Listen der Koeffizienten; Rechnungen mit Polynomen sind dann letztlich Manipulationen dieser Listen. Das Ergebnis solcher Rechnungen wird nicht als Liste ausgegeben, sondern als "formaler" Ausdruck wie oben mit einer Unbestimmten $X$ gedruckt. (Man kann natürlich auch andere Buchstaben anstelle von "$X$" wählen.) Beispiel:

```
gap> t:=Indeterminate(Rationals,"t");;       # "t"= Name der Unbestimmten
gap> f:=(3*t^4-1)*(t^8-t^5+17);
3*t^12-3*t^9-t^8+t^5+51*t^4-17
gap> CoefficientsOfUnivariatePolynomial(f);
[ -17, 0, 0, 0, 51, 1, 0, 0, -1, -3, 0, 0, 3 ]     # beachte Reihenfolge!
gap> Value(f,11)                                    # s=11 in f eingesetzt
9407997835934
```

## 10. *Die reellen Zahlen*

Die reellen Zahlen $\mathbb{R}$ bilden einen Körper mit $\mathbb{Q} \subseteq \mathbb{R}$; die üblichen Rechen-Operationen (also Addition, Multiplikation, Anordnung $\leqslant$) werden dabei von $\mathbb{Q}$ auf $\mathbb{R}$ fortgesetzt. Wir geben hier keine formale Definition oder Konstruktion (dazu siehe zum Beispiel Kapitel 2 im Buch von Ebbinghaus et al.), sondern stellen uns $\mathbb{R}$ als Zahlengerade vor:




Elemente von $\mathbb{R}\setminus\mathbb{Q}$ heißen ***irrationale Zahlen***; wir haben bereits gesehen, dass $\sqrt{2}$ irrational ist (Satz 2.10). Wir wollen hier die grundlegenden Eigenschaften von $\mathbb{R}$ herausarbeiten, die sicherstellen, dass man so etwas wie $\sqrt{2}$ (oder die oben in der Zahlengeraden genannte ***Eulersche Zahl*** $e \approx 2{,}71828\ldots$) in $\mathbb{R}$ konstruieren kann.

**Bemerkung 10.1.** Für $x \in \mathbb{R}$ ist der ***Absolutbetrag*** gegeben durch $|x| := \begin{cases} x & \text{falls } x \geqslant 0, \\ -x & \text{falls } x < 0. \end{cases}$
Es gilt die (oft nützliche) ***Dreiecksungleichung***: $\quad |x+y| \leqslant |x| + |y|$ für alle $x, y \in \mathbb{R}$.

Beweis der Ungleichung: Es gilt $-|x| \leqslant x \leqslant |x|$. Ist $x + y \geqslant 0$, so erhalten wir $|x+y| = x+y \leqslant |x|+|y|$; ist $x+y < 0$, so erhalten wir $|x+y| = -(x+y) = (-x)+(-y) \leqslant |x|+|y|$.

**Definition 10.2.** Sei $S \subseteq \mathbb{R}$ eine nicht-leere Teilmenge. Wir sagen, dass $S$ ***nach oben beschränkt*** ist, wenn es ein $M \in \mathbb{R}$ gibt mit $x \leqslant M$ für alle $x \in S$. In diesem Fall heißt $M$ eine ***obere Schranke*** für $S$. Ist $M$ eine obere Schranke und gilt $M \leqslant M_1$ für jede weitere obere Schranke $M_1$ für $S$, so heißt $M$ ***kleinste obere Schranke*** von $S$.

Beachte: Es ist keineswegs klar, dass eine nach oben beschränkte Menge auch eine kleinste obere Schranke besitzt. Aber wenn dies der Fall ist, so bezeichnen wir die kleinste obere Schranke mit $M = \sup(S)$ ("***Supremum***" von $S$).

Analog werden die Begriffe "***nach unten beschränkt***", "***untere Schranke***" und "***größte untere Schranke***" definiert. Wiederum: Gibt es eine größte untere Schranke, so bezeichnen wir diese mit $\inf(S)$ ("***Infimum***" von $S$).

Sei zum Beispiel $S := \mathbb{N} \subseteq \mathbb{R}$. Dann ist $\mathbb{N}$ nach unten beschränkt; z.B. sind $M = 0$ or $M = -17$ untere Schranken. Man sieht sofort, dass $\inf(\mathbb{N}) = 1$ gilt; in diesem Fall gehört also das Infimum selbst zur Menge dazu. (Wir werden noch Beispiele sehen, wo dies nicht der Fall ist.) Da natürliche Zahlen beliebig groß werden können, scheint es ebenso klar zu sein, dass $\mathbb{N}$ nicht nach oben beschränkt ist. (Ein präziser Beweis folgt unten.)

Hier ist nun die fundamentale, alles entscheidende Eigenschaft von $\mathbb{R}$.

**Satz 10.3.** *Der Körper $\mathbb{R}$ ist ein **vollständiger Körper**, d.h., jede nicht-leere, nach oben beschränkte Teilmenge von $\mathbb{R}$ besitzt ein Supremum, und jede nicht-leere, nach unten beschränkte Teilmenge von $\mathbb{R}$ besitzt ein Infimum.*

Als erste Mini-Anwendung sei wieder $S := \mathbb{N} \subseteq \mathbb{R}$. Angenommen, $\mathbb{N}$ wäre nach oben beschränkt; dann existiert $M := \sup(\mathbb{N}) \in \mathbb{R}$. Da $M$ die kleinste obere Schranke ist, ist folglich $M-1$ keine obere Schranke für $\mathbb{N}$ mehr. Also gibt es ein $n \in \mathbb{N}$ mit $n > M-1$. Dann ist aber auch $n+1 > (M-1)+1 = M$, also ist $n+1 \in \mathbb{N}$ echt grösser als $M$, Widerspruch dazu, dass $M$ eine obere Schranke für $\mathbb{N}$ ist. Also ist in der Tat $\mathbb{N}$ nicht nach oben beschränkt.

**Lemma 10.4.** (a) *Seien $x, y \in \mathbb{R}$ mit $x > 0$. Dann gibt es ein $n \in \mathbb{N}$ mit $nx > y$.*
(b) *Sei $x \in \mathbb{R}$. Dann gibt es (genau) ein $n \in \mathbb{Z}$ mit $n \leqslant x < n+1$.*
(c) *Seien $x, y \in \mathbb{R}$ mit $x < y$. Dann gibt es ein $r \in \mathbb{Q}$ mit $x < r < y$.*
Die Aussage in (c) wird auch als ***Dichtheit*** von $\mathbb{Q}$ in $\mathbb{R}$ bezeichnet.

*Beweis.* (a) Wir haben gerade gesehen, dass $\mathbb{N}$ nicht nach oben beschränkt ist. Also gibt es ein $n \in \mathbb{N}$ mit $n > y/x$. Multiplizieren mit $x > 0$ ergibt $nx > y$.

(b) Da $\mathbb{N}$ nicht nach oben beschränkt ist, gibt es ein $a \in \mathbb{N}$ mit $x < a$; analog gibt es ein $b \in \mathbb{N}$ mit $-x < b$. Dann gilt $-b < x < a$. Jetzt betrachte die endlich vielen ganzen Zahlen $-b, -b+1, -b+2, \ldots, a-1, a$. Sei $n \in \mathbb{Z}$ die erste Zahl in dieser Liste (von rechts nach links) mit $n \leqslant x$. Dann ist $n \leqslant x \leqslant n+1$. Offenbar ist $n$ eindeutig bestimmt.

(c) Wegen $y - x > 0$ gibt es nach (a) ein $n \in \mathbb{N}$ mit $n(y-x) > 1$, also $ny > nx + 1$. Nach (b) gibt es ein $n' \in \mathbb{Z}$ mit $n' \leqslant nx < n'+1$. Setze nun $m := n'+1$. Dann folgt $nx < m = n'+1 \leqslant nx+1 < ny$. Teilen durch $n$ ergibt $x < r < y$ mit $r := m/n \in \mathbb{Q}$. □

**Beispiel 10.5.** Sei $a \in \mathbb{R}$, $a > 0$, und $S := \{\frac{a}{n} \mid n \in \mathbb{N}\} \subseteq \mathbb{R}$. Es gilt $x > 0$ für alle $x \in S$, also ist $0$ eine untere Schranke (aber $0 \notin S$). Behauptung: Es gilt $\inf(S) = 0$.

Dazu: Sei $M \in \mathbb{R}$ eine weitere untere Schranke. Wir müssen zeigen, dass $M \leqslant 0$ gilt. Annahme, es wäre $M > 0$. Nach Lemma 10.4(a) gibt es ein $n \in \mathbb{N}$ mit $nM > a$. Dann ist aber $M > \frac{a}{n} \in S$, Widerspruch dazu, dass $M$ eine untere Schranke von $S$ sein soll. Also war die Annahme falsch und es gilt $M \leqslant 0$, wie gewünscht.

**Folgerung 10.6.** *Sei* $x \in \mathbb{R}$ *und* $S := \{r \in \mathbb{Q} \mid r \leqslant x\}$. *Dann gilt* $x = \sup(S)$.

*Beweis.* Die Menge $S$ ist nach oben beschränkt durch $x$, also existiert $y := \sup(S) \in \mathbb{R}$ und es gilt $y \leqslant x$. Wäre $y < x$, so gibt es nach Lemma 10.4(c) ein $r \in \mathbb{Q}$ mit $y < r < x$. Dann ist aber auch $r \in S$, Widerspruch dazu, dass $y$ eine obere Schranke für $S$ ist. Also ist $x = y$. □

**Beispiel 10.7** (Dezimalentwicklung)**.** Gegeben sei $x \in \mathbb{R}$, $x > 0$. Die Dezimalentwicklung von $x$ ist eine Darstellung der Form $x = z_0{,}z_1z_2z_3\ldots$ mit $z_0 \in \mathbb{N}_0$ und "Nachkomma-Ziffern" $z_n \in \{0, 1, 2, \ldots, 9\}$ für alle $n \geqslant 1$. Zum Beispiel $\sqrt{2} = 1{,}41421356237309504880168872 4\ldots$ (Für konkrete Rechnungen gibt man sich dann eine gewünschte Genauigkeit vor und bricht die Entwicklung ab einer bestimmten Stelle ab — darauf werden wir hier allerdings nicht weiter eingehen. Siehe z.B. Kapitel 19 "`Floats`" im GAP-Manual.) Wir zeigen nun, wie man die Dezimalentwicklung mathematisch präzise herleitet. Wir definieren dazu eine Folge $(z_n)_{n\in\mathbb{N}}$ in $\mathbb{N}_0$ rekursiv wie folgt. Nach Lemma 10.4(b) gibt es $z_0 \in \mathbb{Z}$ mit $z_0 \leqslant x < z_0 + 1$; wegen $x \geqslant 0$ ist auch $z_0 \geqslant 0$. Dann setze $x_1 := x - z_0$. Es gilt $0 \leqslant x_1 < 1$ und damit $0 \leqslant 10x_1 < 10$. Wiederum nach Lemma 10.2(b) gibt es $z_1 \in \mathbb{Z}$ mit $z_1 \leqslant 10x_1 < z_1 + 1$; wegen $0 \leqslant 10x_1 < 10$ ist $z_1 \in \{0, 1, 2, \ldots, 9\}$. Dann setze $x_2 := 10x_1 - z_1$. Es gilt $0 \leqslant x_2 < 1$ und wir können das ganze Argument wiederholen. Es gibt also $z_2 \in \{0, 1, 2, \ldots, 9\}$ mit $z_2 \leqslant 10x_2 < z_2 + 1$; setze dann $x_3 := 10x_2 - z_2$ und so weiter. Damit erhalten wir Folgen $(z_n)_{n\in\mathbb{N}_0}$ und $(x_n)_{n\in\mathbb{N}}$ mit $0 \leqslant x_n < 1$ und $0 \leqslant x_{n+1} = 10x_n - z_n$ für alle $n \in \mathbb{N}$. Wir setzen nun

$$S := \{a_n \mid n \in \mathbb{N}_0\} \qquad \text{wobei} \qquad a_n := \sum_{i=0}^{n} \frac{z_i}{10^i} \in \mathbb{Q} \quad \text{für alle } n \in \mathbb{N}_0.$$

Mit einer (leichten) vollständigen Induktion nach $n$ zeigt man sofort:

$$x = z_0 + x_1 = a_n + \frac{x_{n+1}}{10^n} \qquad \text{für alle } n \in \mathbb{N}_0.$$

Wegen $0 \leqslant x_{n+1} < 1$ ist dann $0 \leqslant x - a_n < \frac{1}{10^n}$ für alle $n \in \mathbb{N}_0$. Wegen $z_i \geqslant 0$ für alle $i$ ist außerdem $a_0 \leqslant a_1 \leqslant a_2 \leqslant \ldots \leqslant x$; die Differenz zwischen $a_n$ und $x$ ist jeweils $< \frac{1}{10^n}$, wird also immer kleiner. Wir überlassen es als Übung zu zeigen, dass daraus $x = \sup(S)$ folgt. (Argumentieren Sie so ähnlich wie im Beweis von Folgerung 10.6.) Die Folge $(z_n)_{n\in\mathbb{N}_0}$ definiert die Dezimaldarstellung $x = z_0{,}z_1z_2z_3\ldots$ von $x$.

Wir können an dieser Darstellung auch ablesen, wann $x \in \mathbb{Q}$ gilt. Dazu nennen wir die Folge $(z_n)_{n\in\mathbb{N}_0}$ "periodisch", wenn es ein $n_0 \geqslant 0$ and $d \geqslant 1$ gibt mit

$$z_{n_0+di+1} = z_{n_0+1}, \quad z_{n_0+di+2} = z_{n_0+2}, \quad \ldots, \quad z_{n_0+di+d} = z_{n_0+d} \quad \text{für } i = 1, 2, 3, \ldots,$$

d.h., aber einer bestimmten Stelle wiederholt sich ein Block von $d$ Ziffern. Dann kann man zeigen: Es gilt $x \in \mathbb{Q}$ genau dann, wenn $(z_n)_{n\in\mathbb{N}_0}$ periodisch ist.

Beispiel: Sei $x = 0{,}312121212\ldots$. Wir schreiben dies einfach als $x = 0{,}3\overline{12}$, wobei der obere Querstrich den sich wiederholenden Block angibt. Sei $y := 0{,}\overline{12}$. Weil der sich wiederholende Block die Länge 2 hat, multiplizieren wir mit $10^2$ und erhalten $100y = 12{,}\overline{12} = 12 + y$. Also $99y = 12$ and damit $x = 0{,}3\overline{12} = \frac{3}{10} + \frac{y}{10} = \frac{3}{10} + \frac{12}{99} \cdot \frac{1}{10} = \frac{3}{10} + \frac{4}{330} = \frac{99+4}{330} = \frac{103}{330} \in \mathbb{Q}$.
Umgekehrt hat jedes $x \in \mathbb{Q}$ eine periodische Dezimaldarstellung, z.B. $x = \frac{3103}{9990} = 0{,}3\overline{106}$.

**Bemerkung 10.8.** Die Existenz von Suprema oder Infima kann im Prinzip dazu benutzt werden, um diverse Konstruktionen mit reellen Zahlen mathematisch präzise zu rechtfertigen. Sei zum Beispiel $a \in \mathbb{R}$, $a \geqslant 0$; dann existiert für jedes $n \in \mathbb{N}$ die (positive) $n$-te Wurzel $\sqrt[n]{a} \in \mathbb{R}$ (insbesondere also auch $\sqrt{2} \in \mathbb{R}$). Um dies zu begründen, kann man die Menge $S := \{x \in \mathbb{R} \mid x^n \leqslant a\}$ betrachten und zeigen, dass sie nicht leer und nach oben beschränkt ist (was nicht sehr schwierig ist); danach müsste man noch zeigen, dass $\sup(S) \in \mathbb{R}$ die gesuchte $n$-te Wurzel von $a$ ist — aber dies ist etwas mühsam. Im 2. Semester werden wir wesentlich effizientere Methoden kennenlernen, um derartige Fragestellungen zu lösen.

---

Zum Schluss betrachten wir noch eine weitere grundlegende Konstruktion: "Intervallschachtelungen". Zuerst einige Bezeichnungen. Seien $a, b \in \mathbb{R}$ mit $a \leqslant b$. Dann heißt

$$[a, b] := \{x \in \mathbb{R} \mid a \leqslant x \leqslant b\} \qquad \textbf{\textit{abgeschlossenes Intervall}},$$
$$(a, b) := \{x \in \mathbb{R} \mid a < x < b\} \qquad \textbf{\textit{offenes Intervall}}.$$

Es gibt natürlich auch die Mischformen $[a, b) := \{x \in \mathbb{R} \mid a \leqslant x < b\}$ und $(a, b] := \{x \in \mathbb{R} \mid a < x \leqslant b\}$, die wir aber im Moment nicht weiter benötigen. Ist $I$ ein solches Intervall (abgeschlossen oder nicht), so bezeichnen wir manchmal mit $\ell(I) := b - a$ die Länge von $I$.

**Satz 10.9** (***Intervallschachtelung***)**.** *Gegeben sei eine Folge von abgeschlossenen Intervallen* $I_1, I_2, I_3, \ldots \subseteq \mathbb{R}$ *mit* $I_1 \supseteq I_2 \supseteq I_3 \supseteq \ldots$. *Dann gibt es ein* $x \in \mathbb{R}$ *mit* $x \in I_n$ *für alle* $n \in \mathbb{N}$. *Gilt* $\inf(\{\ell(I_n) \mid n \in \mathbb{N}\}) = 0$, *so gibt es genau ein* $x \in \mathbb{R}$ *mit* $x \in I_n$ *für alle* $n \in \mathbb{N}$.

*Beweis.* Für $n \in \mathbb{N}$ schreiben wir $I_n = [a_n, b_n]$ mit $a_n, b_n \in \mathbb{R}$ und $a_n \leqslant b_n$. Die Bedingung $I_1 \supseteq I_2 \supseteq I_3 \supseteq \ldots$ übersetzt sich dann in

$$(*) \qquad a_n \leqslant a_{n+1} \qquad \text{und} \qquad b_n \geqslant b_{n+1} \qquad \text{für alle } n \in \mathbb{N}.$$

Sei $S := \{a_n \mid n \in \mathbb{N}\} \subseteq \mathbb{R}$. Wegen $a_n \leqslant b_n \leqslant b_1$ für alle $n \in \mathbb{N}$ ist $b_1$ eine obere Schranke für $S$; also existiert $x := \sup(S) \in \mathbb{R}$ und es gilt $a_n \leqslant x$ für alle $n \in \mathbb{N}$. Wir müssen noch

zeigen, dass auch $x \leqslant b_n$ für alle $n \in \mathbb{N}$ gilt. Annahme, es gäbe ein $n_0 \in \mathbb{N}$ mit $x > b_{n_0}$. Nun ist $a_1 \leqslant a_2 \leqslant \ldots \leqslant a_{n_0} \leqslant b_{n_0}$. Für $n > n_0$ ist $a_n \leqslant b_n \leqslant b_{n_0}$. Also gilt $a_n \leqslant b_{n_0}$ für alle $n \in \mathbb{N}$, d.h., $b_{n_0}$ ist eine obere Schranke für $S$ und damit $x \leqslant b_{n_0}$, Widerspruch.

Es gelte nun zusätzlich $\inf(T) = 0$ wobei $T := \{\ell(I_n) \mid n \in \mathbb{N}\}$. Nehmen wir an, es sei auch $y \in \mathbb{R}$ mit $y \in I_n$ für alle $n \in \mathbb{N}$. Dann müssen wir $x = y$ zeigen. Dazu: Wegen $a_n \leqslant y$ für alle $n \in \mathbb{N}$ ist $y$ eine obere Schranke für $S$, also gilt bereits $x = \inf(S) \leqslant y$. Für $n \in \mathbb{N}$ gilt $y \leqslant b_n = b_n - a_n + a_n = \ell(I_n) + a_n \leqslant \ell(I_n) + x$ und damit $\ell(I_n) \geqslant y - x$. Also ist $y - x$ eine untere Schranke für $T$ und damit $y - x \leqslant \inf(T) = 0$, d.h., es gilt auch $y \leqslant x$. □

Um das folgende Beispiel zu behandeln, benötigen wir die ***Bernoulli–Ungleichung***:

$$(1 + x)^n \geqslant 1 + nx \qquad \text{für alle } n \in \mathbb{N} \text{ und } x \in \mathbb{R} \text{ mit } x \geqslant -1.$$

(Dies können Sie selbst leicht mit vollständiger Induktion nach $n$ beweisen.)

**Beispiel 10.10.** Wir definieren Folgen $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ von rationalen Zahlen durch

$$a_n := \Big(1 + \frac{1}{n}\Big)^n \qquad \text{und} \qquad b_n := \Big(1 + \frac{1}{n}\Big)^{n+1} \qquad \text{für alle } n \in \mathbb{N}.$$

Wegen $a_n > 0$ und $b_n = a_n(1+\frac{1}{n}) = a_n + \frac{1}{n}a_n > a_n$ erhalten wir eine Folge von abgeschlossenen Intervallen $I_n := [a_n, b_n] \subseteq \mathbb{R}$ für alle $n \in \mathbb{N}$. Wir zeigen nun, dass die Voraussetzungen von Satz 10.9 erfüllt sind. Sei $n \in \mathbb{N}$, $n \geqslant 2$. Zunächst beachte $a_n = \big(\frac{n+1}{n}\big)^n > 0$ und $b_n = \big(\frac{n+1}{n}\big)^{n+1} > 0$; damit folgt

$$\frac{a_n}{b_{n-1}} = \frac{\big(\frac{n+1}{n}\big)^n}{\big(\frac{n}{n-1}\big)^n} = \Big(\frac{(n+1)(n-1)}{n^2}\Big)^n = \big(\frac{n^2-1}{n^2}\big)^n = \big(1-\frac{1}{n^2}\big)^n \geqslant 1-\frac{n}{n^2} = 1-\frac{1}{n} = \frac{n-1}{n},$$

wobei wir die Bernoulli–Ungleichung (mit $x = -\frac{1}{n^2}$) benutzt haben. Analog erhalten wir

$$\frac{b_{n-1}}{a_n} = \Big(\frac{n^2}{n^2-1}\Big)^n = \big(1+\frac{1}{n^2-1}\big)^n \geqslant 1+\frac{n}{n^2-1} \geqslant 1+\frac{n}{n^2} = 1+\frac{1}{n} = \frac{n+1}{n},$$

wobei wir wieder die Bernoulli–Ungleichung (diesmal mit $x = \frac{1}{n^2-1}$) sowie die Abschätzung $\frac{1}{n^2-1} \geqslant \frac{1}{n^2}$ benutzt haben. Aus der ersten der beiden obigen Ungleichung folgt

$$a_n \geqslant \tfrac{n-1}{n} b_{n-1} = \tfrac{n-1}{n}\big(\tfrac{n}{n-1}\big)^n = \big(\tfrac{n}{n-1}\big)^{n-1} = \big(1+\tfrac{1}{n-1}\big)^{n-1} = a_{n-1};$$

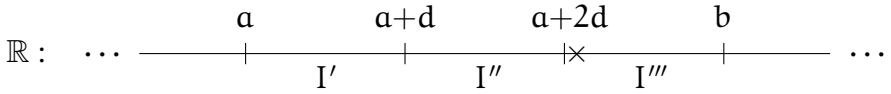
aus der zweiten Ungleichung folgt analog $b_{n-1} \geqslant \frac{n+1}{n} a_n = \frac{n+1}{n}\big(\frac{n+1}{n}\big)^n = \big(1+\frac{1}{n}\big)^{n+1} = b_n$. Also gilt Bedingung $(*)$ im obigen Beweis. Schließlich folgt

$$\ell(I_n) = b_n - a_n = a_n\big(1 + \tfrac{1}{n}\big) - a_n = \tfrac{1}{n} a_n \leqslant \tfrac{1}{n} b_n \leqslant \tfrac{1}{n} b_1 = \tfrac{1}{n} 2^2 = \tfrac{4}{n}.$$

Wie in Beispiel 10.5 folgt $\inf(\{\ell(I_n) \mid n \in \mathbb{N}\}) = 0$. Also gibt es nach Satz 10.9 genau eine reelle Zahl, die in allen $I_n$ enthalten ist. Diese reelle Zahl ist die berühmte ***Eulersche Zahl*** und wird mit $e \in \mathbb{R}$ bezeichnet. Zum Beispiel erhält man für $n = 10000$ die Abschätzungen $2{,}7181 < e < 2{,}7184$. Man kann zeigen, dass $e$ irrational ist.

**Satz 10.11** (Cantor)**.** *Der Köper* $\mathbb{R}$ *is überabzählbar.*

*Beweis.* Der (genial einfache) "Trick" des Beweises besteht aus folgender Bemerkung. Gegeben sei ein abgeschlossenes Intervall $I = [a, b] \subseteq \mathbb{R}$ mit $a < b$. Dann können wir I in genau drei gleich große Teilintervalle aufteilen: $I = I' \cup I'' \cup I'''$ wobei $I' = [a, a + d]$, $I'' = [a+d, a+2d]$ und $I''' = [a+2d, b]$ mit $d = (b-a)/3$. Nun beachte: Ist $x \in \mathbb{R}$ beliebig, so gibt es stets (mindestens) eines dieser drei Teilintervalle, in dem $x$ nicht enthalten ist. In der Zeichnung, wo $\times$ die Position von $x$ markiert, ist $x \in I'''$, aber $x \notin I'$ und $x \notin I''$.




Ist dagegen z.B. $x = a+d$ (also genau die Grenze zwischen $I'$ und $I''$), so gilt $x \in I'$ und $x \in I''$ aber $x \notin I'''$. Jetzt zum eigentlichen Beweis. Nehmen wir an, $\mathbb{R}$ sei abzählbar. Dann ist auch das Intervall $I = [0, 1] \subseteq \mathbb{R}$ abzählbar. Es gibt also eine Aufzählung $I = [0, 1] = \{x_n \mid n \in \mathbb{N}\}$. Wir definieren nun eine Folge von Intervallen $I_1, I_2, I_3, \ldots$ nach folgendem Verfahren. Wir teilen I wie oben in genau drei gleiche Teilintervalle auf; sei $I_1$ eines dieser drei Teilintervalle mit $x_1 \notin I_1$. Danach teilen wir $I_1$ in genau drei gleiche Teilintervalle auf; sei $I_2$ eines dieser drei Teilintervalle mit $x_2 \notin I_2$. Wir fahren mit dem gleichen Schema fort und erhalten Intervalle $I_n$ mit $x_n \notin I_n$, für alle $n \in \mathbb{N}$. Nach Konstruktion ist dabei $I \supseteq I_1 \supseteq I_2 \supseteq I_3 \supseteq \ldots$, also gibt es nach Satz 10.9 ein $x \in \mathbb{R}$ mit $x \in I_n$ für alle $n \in \mathbb{N}$. Wegen $x \in I$ und unserer Annahme ist nun $x = x_{n_0}$ für ein $n_0 \in \mathbb{N}$. Weil $x$ in allen $I_n$ enthalten ist, gilt insbesondere $x \in I_{n_0}$; andererseits gilt aber nach Konstruktion von $I_{n_0}$ auch $x = x_{n_0} \notin I_{n_0}$, Widerspruch. □

Wir können nun auch schließen, dass $\mathbb{Q}$ kein vollständiger Körper ist. Denn wenn $\mathbb{Q}$ vollständig wäre, so könnten wir Satz 10.9 völlig analog für Intervallschachtelungen in $\mathbb{Q}$ zeigen. Und dann würde anschließend völlig analog zum obigen Beweis auch folgen, dass $\mathbb{Q}$ überabzählbar ist, Widerspruch. — Die obigen wenigen Betrachtungen zeigen bereits, dass zum Umgang mit reellen Zahlen völlig andere Methoden benötigt werden als mit ganzen oder rationalen Zahlen oder den Ringen $\mathbb{Z}/m\mathbb{Z}$; wir werden dies im 2. Semester weiter vertiefen.

**Ab hier Woche 7**

## 11. *Die komplexen Zahlen*

Die komplexen Zahlen $\mathbb{C}$ bilden einen Körper mit $\mathbb{R} \subseteq \mathbb{C}$. Konkret kann man als Menge $\mathbb{C} := \{(a, b) \mid a, b \in \mathbb{R}\}$ nehmen und darauf folgende Verknüpfungen definieren:

$$(a, b) + (a', b') := (a + a', b + b') \qquad \text{und} \qquad (a, b) \cdot (a', b') := (aa' - bb', ab' + a'b)$$

für alle $a, a', b, b' \in \mathbb{R}$. Man muss dann zeigen, dass die Körperaxiome erfüllt sind. (Dazu sind viele kleinere Rechnungen zu machen, die aber alle nicht besonders schwierig sind; siehe

z.B. §9.3 im Buch von Glosauer für die Details.) Das Paar $(0,0)$ ist das neutrale Element bezüglich der Addition; das Paar $(1,0)$ ist das neutrale Element bezüglich der Multiplikation. Die Inversen von $z := (a,b) \in \mathbb{C}$ bezüglich Addition und Multiplikation sind gegeben durch

$$-z = (-a,-b) \in \mathbb{C} \qquad \text{und} \qquad z^{-1} = \Big(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\Big) \in \mathbb{C},$$

wobei wir für $z^{-1}$ natürlich $z \neq (0,0)$ voraussetzen müssen, d.h., $a \neq 0$ oder $b \neq 0$; beachte, dass in diesem Fall $a^2+b^2$ eine positive reelle Zahl ist. Wir können $\mathbb{R}$ als Teilmenge von $\mathbb{C}$ auffassen, indem wir $a \in \mathbb{R}$ mit $(a,0) \in \mathbb{C}$ identifizieren. Setzen wir außerdem $i := (0,1) \in \mathbb{C}$, so folgt $i^2 = -(1,0) = -1$ und $(a,b) = (a,0) + (0,b) = a + b \cdot (0,1) = a + bi$; hier heißt $a$ der ***Realteil*** und $b$ der ***Imaginärteil***. Also erhalten wir die übliche Schreibweise $\mathbb{C} = \{a+bi \mid a,b \in \mathbb{R}\}$; das Rechnen mit solchen Ausdrücken erfolgt dann ebenfalls nach den üblichen Reglen, wobei man sich nur daran erinnern muss, dass $i^2 = -1$ gilt. Zum Beispiel:

$$\frac{2+3i}{-5+i} = \frac{2+3i}{-5+i} \cdot \frac{-5-i}{-5-i} = \frac{(2+3i)(-5-i)}{25+1} = \frac{-10-2i-15i-3i^2}{26} = -\frac{7}{2} - \frac{17}{26}i \in \mathbb{C}.$$

**Bemerkung 11.1.** Ist $z = a + bi \in \mathbb{C}$ so heißt $\overline{z} := a - bi \in \mathbb{C}$ die ***konjugiert-komplexe Zahl***. Dann ist $z\overline{z} = a^2 + b^2$ eine nicht-negative reelle Zahl und wir nennen

$$|z| := \sqrt{z\overline{z}} = \sqrt{a^2+b^2} \in \mathbb{R}$$

den Absolutbetrag von $z$. Damit gilt $z^{-1} = (|z|^2)^{-1}\overline{z}$ für $0 \neq z \in \mathbb{C}$. Weiterhin gilt:

$$\overline{\overline{z}} = z, \qquad \overline{z_1+z_2} = \overline{z}_1 + \overline{z}_2, \qquad \overline{z_1 \cdot z_2} = \overline{z}_1 \cdot \overline{z}_2, \qquad z \in \mathbb{R} \Leftrightarrow \overline{z} = z,$$

$$\tfrac{1}{2}(z+\overline{z}) = \text{Realteil von } z, \qquad \tfrac{1}{2i}(z-\overline{z}) = \text{Imaginärteil von } z,$$

für alle $z, z_1, z_2 \in \mathbb{C}$. (Beweis durch leichtes Nachrechnen.)

**Bemerkung 11.2.** Wie oben diskutiert, setzen sich Addition und Multiplikation von $\mathbb{R}$ auf $\mathbb{C}$ fort. Aber die Anordnung $\leqslant$ auf $\mathbb{R}$ lässt sich nicht sinnvollerweise auf $\mathbb{C}$ fortsetzen. Natürlich kann man $\mathbb{C}$ irgendwie anordnen, aber dies sollte auch mit den Körperoperationen zusammenpassen (genauso wie in $\mathbb{R}$), also zum Beispiel $x+y > 0$ und $x \cdot y > 0$, wenn $x > 0$ und $y > 0$. Daraus folgt sofort $x^2 = x \cdot x = (-x) \cdot (-x) > 0$ für jedes $x \neq 0$; inbesondere $1 = 1^2 > 0$. Gäbe es eine solche Anordnung auf $\mathbb{C}$, so wäre $-1 = i^2 > 0$, Widerspruch.

**Bemerkung 11.3.** In $\mathbb{R}$ hat die Gleichung $x^2 = -1$ keine Lösung, aber in $\mathbb{C}$ sehr wohl, nämlich $x = \pm i$. Es gilt sogar, dass jedes $z \in \mathbb{C}$ eine Quadratwurzel in $\mathbb{C}$ besitzt, nämlich

$$z = \Big(\sqrt{\tfrac{1}{2}\big(\sqrt{a^2+b^2}+a\big)} \pm i\sqrt{\tfrac{1}{2}\big(\sqrt{a^2+b^2}-a\big)}\Big)^2 \quad \text{wobei} \quad z = a+bi \quad \text{mit } a,b \in \mathbb{R}$$

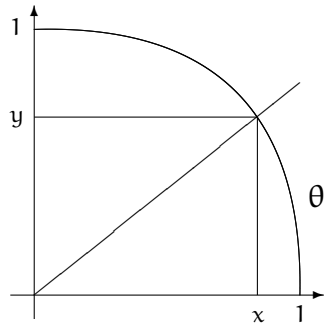
und das Vorzeichen gleich "+" ist, falls $b \geqslant 0$, und gleich "−", falls $b < 0$. (Einfaches Nachrechnen.) Damit hat auch jede quadratische Gleichung der Form $x^2 + px + q = 0$ mit $p, q \in \mathbb{C}$ Lösungen in $\mathbb{C}$, nämlich $x_{1,2} = \frac{1}{2}\big(-p \pm \sqrt{p^2-4q}\big) \in \mathbb{C}$.

Man hätte erwarten können, dass für Lösungen von Gleichungen vom Grad $3, 4, \ldots$ noch größere Körper als $\mathbb{C}$ konstruiert werden müssten. Aber es gilt:

**Satz 11.4** (***Fundamentalsatz der Algebra***)**.** *Sei* $n \in \mathbb{N}$ *und* $0 \neq f \in \mathbb{C}[X]$ *ein Polynom mit* $\mathrm{Grad}(f) = n$*. Dann zerfällt* $f$ *in Linearfaktoren über* $\mathbb{C}$*, d.h., es gibt* $a, z_1, \ldots, z_n \in \mathbb{C}$ *mit* $a \neq 0$ *und* $f = a(X - z_1)(X - z_2)\cdots(X - z_n)$*. Insbesondere hat jedes nicht-konstante Polynom* $f \in \mathbb{C}[X]$ *eine Nullstelle in* $\mathbb{C}$*.*

Für diverse Beweise und mehr zur (interessanten) Geschichte dieses Satzes und seine Bedeutung in der Mathematik insgesamt siehe Kapitel 4 im Buch von Ebbinhaus et al.

Zum Schluss geben wir noch eine geometrisch etwas anschaulichere Beschreibung der Multiplikation in $\mathbb{C}$. Dazu setzen wir die übliche (reelle) ***Sinus-Funktion*** und die ***Cosinus-Funktion*** als bekannt voraus (mehr dazu im 2. Semester). Für einen Winkel $\theta$ sind $\sin(\theta)$ und $\cos(\theta)$ anschaulich wie in folgender Zeichnung definiert, wobei wir den Kreis mit Radius $1$ und Mittelpunkt im Ursprung von $\mathbb{R}^2$ betrachten:




$$x = \cos(\theta) \quad \text{oder} \quad \theta = \arccos(x)$$
$$y = \sin(\theta) \quad \text{oder} \quad \theta = \arcsin(y)$$
$$\sin(\theta)^2 + \cos(\theta)^2 = 1 \qquad \text{(Pythagoras)}$$

Der Winkel ist durch die Länge des Kreisbogens vom Punkt $(1, 0) \in \mathbb{R}^2$ zum Punkt $(x, y) \in \mathbb{R}^2$ bestimmt. Da der gesamte Kreis den Umfang $2\pi$ hat, ist also $\theta \in [0, 2\pi]$; die Werte $\sin(\theta)$ und $\cos(\theta)$ liegen im Intervall $[-1, 1]$. Hier sind einige oft gebrauchte Werte von sin und cos:

| $\theta$ | $0$ | $\frac{\pi}{6}$ | $\frac{\pi}{4}$ | $\frac{\pi}{3}$ | $\frac{\pi}{2}$ | $\pi$ |
|---|---|---|---|---|---|---|
| $\sin(\theta)$ | $0$ | $\frac{1}{2}$ | $\frac{\sqrt{2}}{2}$ | $\frac{\sqrt{3}}{2}$ | $1$ | $0$ |
| $\cos(\theta)$ | $1$ | $\frac{\sqrt{3}}{2}$ | $\frac{\sqrt{2}}{2}$ | $\frac{1}{2}$ | $0$ | $-1$ |

Die Funktionen sin and cos können auf ganz $\mathbb{R}$ fortgesetzt werden, wobei sich die Werte mit Periode $2\pi$ wiederholen, also

$$\sin(x + 2\pi) = \sin(x) \qquad \text{und} \qquad \cos(x + 2\pi) = \cos(x) \qquad \text{für alle } x \in \mathbb{R}.$$

Hierbei gilt $\sin(-x) = -\sin(x)$ und $\cos(-x) = \cos(x)$ für alle $x \in \mathbb{R}$. Außerdem gelten die folgenden ***Additionstheoreme*** für alle $x, y \in \mathbb{R}$:

$$\begin{aligned} \sin(x + y) &= \sin(x)\cos(y) + \cos(x)\sin(y), \\ \cos(x + y) &= \cos(x)\cos(y) - \sin(x)\sin(y). \end{aligned}$$

**Satz 11.5** (Polardarstellung komplexer Zahlen)**.** *Für jedes $z \in \mathbb{C}$ existieren eindeutige reelle Zahlen $r, \theta \in \mathbb{R}$ mit $z = r\big(\cos(\theta) + \sin(\theta)i\big)$ wobei $r = |z| \geqslant 0$ und $\theta \in [0, 2\pi)$ (und wir die Konvention benutzen, $\theta = 0$ für $z = 0$ zu nehmen).*

Anstelle eines formalen Beweises illustrieren wir dies mit einem Beispiel. Sei also etwa $z = \sqrt{2} - \sqrt{2}\mathrm{i} \in \mathbb{C}$. Dann ist $r = |z| = \sqrt{(\sqrt{2})^2 + (-\sqrt{2})^2} = 2$. Damit ist $z = 2(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\mathrm{i})$. Jetzt müssen wir noch $\theta \in [0, 2\pi)$ finden mit $\cos(\theta) = \frac{1}{\sqrt{2}}$ und $\sin(\theta) = -\frac{1}{\sqrt{2}}$. Mit obiger Tabelle und den Regeln $\sin(-x) = -\sin(x)$, $\cos(-x) = \cos(x)$ sieht man, dass man die richtigen Werte für $x = -\frac{\pi}{4}$ erhält. Um einen Winkel im Intervall $[0, 2\pi)$ zu erhalten, addieren wir $2\pi$, was zu $\theta = 2\pi - \frac{\pi}{4} = \frac{7}{4}\pi$ führt. Damit erhalten wir die Polardarstellung:

$$z = \sqrt{2} - \sqrt{2}\mathrm{i} = 2\big(\cos(\tfrac{7}{4}\pi) + \sin(\tfrac{7}{4}\pi)\mathrm{i}\big).$$

Nach diesen Vorbereitungen kommen wir nun zur versprochenen anschaulichen Beschreibung der Multiplikation in $\mathbb{C}$. Seien $z, z' \in \mathbb{C}$ mit Polardarstellungen

$$z = r\big(\cos(\theta) + \sin(\theta)\mathrm{i}\big) \qquad \text{und} \qquad z' = r'\big(\cos(\theta') + \sin(\theta')\mathrm{i}\big).$$

Multiplikation ergibt

$$\begin{aligned} z \cdot z' &= rr'\big((\cos(\theta)\cos(\theta') - \sin(\theta)\sin(\theta')) + (\sin(\theta)\cos(\theta') + \cos(\theta)\sin(\theta'))\mathrm{i}\big) \\ &= rr'\big(\cos(\theta + \theta') + \sin(\theta + \theta')\mathrm{i}\big) \end{aligned}$$

wobei wir die obigen Additionstheoreme verwendet haben. D.h. wir erhalten die Polardarstellung von $z \cdot z'$, indem wir $r, r'$ multiplizieren und die Winkel $\theta, \theta'$ einfach addieren. Mit einer vollständigen Induktion nach $n$ folgt dann auch sofort

$$z^n = r^n\big(\cos(n\theta) + \sin(n\theta)\mathrm{i}\big) \qquad \text{für alle } n \in \mathbb{N}.$$

**Beispiel 11.6.** Sei $n \geqslant 1$ und $f_n := X^n - 1 \in \mathbb{C}[X]$. In diesem Fall kann man die Nullstellen von $f_n$ explizit beschreiben. Dazu teilen wir den Kreis (in der Ebene $\mathbb{C} = \mathbb{R}^2$) mit Radius $1$ und Mittelpunkt im Ursprung in genau $n$ gleiche Stücke ein; die entsprechenden Punkte auf diesem Kreis sind gegegen durch

$$\zeta_k := \cos(\theta_k) + \sin(\theta_k)\mathrm{i} \in \mathbb{C} \qquad \text{für } k = 0, 1, 2, \ldots, n-1,$$

wobei $\theta_0 := 0,\ \theta_1 := \frac{2\pi}{n},\ \theta_2 := 2\theta_1 = 2\frac{2\pi}{n},\ \ldots,\ \theta_{n-1} := (n-1)\theta_1 = (n-1)\frac{2\pi}{n}$. Mit Hilfe der obigen Formeln erhalten wir dann für $k = 0, 1, 2, \ldots, n$:

$$\begin{aligned} \zeta_k^n &= \cos(n\theta_k) + \sin(n\theta_k)\mathrm{i} = \cos\big(\tfrac{2\pi k n}{n}\big) + \sin\big(\tfrac{2\pi k n}{n}\big)\mathrm{i} \\ &= \cos(2\pi k) + \sin(2\pi k)\mathrm{i} = \cos(0) + \sin(0)\mathrm{i} = 1. \end{aligned}$$

D.h., die $n$ komplexen Zahlen $\zeta_0, \zeta_1, \ldots, \zeta_{n-1} \in \mathbb{C}$ sind alle Nullstellen von $f_n$. Damit folgt

$$f_n = X^n - 1 = (X - \zeta_0)(X - \zeta_1) \cdots (X - \zeta_{n-1}).$$

Die Zahlen $\zeta_k$ heißen $n$-te ***Einheitswurzeln***.

# Kapitel III: Matrizen

Matrizen spielen eine einzigartige Rolle nicht nur in der Mathematik selbst (Matrix-Theorie ist immer noch ein aktives Forschungsgebiet), sondern auch in zahlreichen Anwendungen in den Natur- und Ingenieurwissenschaften — immer dort, wo "lineare" Probleme auftreten. In diesem Kapitel führen wir die grundlegenden Definitionen und Operationen mit Matrizen ein, und betrachten auch erste Anwendungen.

## 12. *Definition, Operationen mit Matrizen*

Sei $R$ ein kommutativer Ring mit $1$ (zum Beispel $R = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/m\mathbb{Z}$). Seien $m, n \in \mathbb{N}$. Ein recht-eckiges Schema der Form

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

mit $m$ Zeilen und $n$ Spalten heißt eine $m \times n$-***Matrix***. Für $1 \leqslant i \leqslant m$ und $1 \leqslant j \leqslant n$ ist $a_{ij}$ der Eintrag an der Position $(i, j)$, also in der $i$-ten Zeile und $j$-ten Spalte. Es sei $R^{m\times n}$ die Menge aller $m \times n$-Matrizen mit Einträgen in $R$. Ist $A \in R^{m\times n}$, so bezeichnen wir mit $A_{ij}$ die einzelnen Einträge von $A$, oder schreiben explizit $A = [a_{ij}]_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$.

Formal ist eine $m \times n$-Matrix also einfach eine Abbildung $f\colon \{1, \dots, m\} \times \{1, \dots, n\} \to R$, deren Wert an der Stelle $(i, j)$ mit $f(i, j) = f_{ij}$ bezeichnet wird.

**Beispiel 12.1.** (a) $A = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 5 \end{bmatrix}$ ist eine $2 \times 3$-Matrix mit Einträgen in $\mathbb{Z}$.

(b) Ist $n = m$ (gleich viele Zeilen wie Spalten), so erhalten wir quadratische Matrizen und benutzen als Bezeichnung oft $M_n(R)$ anstelle von $R^{n\times n}$.

(c) Ist $m = 1$ (d.h., nur $1$ Zeile), so ist $A = [a_1, \dots, a_n]$; wir nennen dies einen ***Zeilenvektor***. Analog, ist $n = 1$ (d.h., nur $1$ Spalte), so erhalten wir einen ***Spaltenvektor***

$$A = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix}.$$

Ist $m = n = 1$, so ist $A = [a]$; wir identifizieren dann einfach $a$ mit $[a]$. Als Konvention bezeichnen wir noch mit $R^n = R^{n\times 1}$ die Menge der Spaltenvektoren der Länge $n$.

**Definition 12.2.** Für $A, B \in R^{m\times n}$ definieren wir die ***Matrixsumme*** $A + B$ als die $m \times n$-Matrix mit Eintrag $A_{ij} + B_{ij}$ an der Stelle $(i, j)$. Ist $s \in R$, so definieren wir das ***skalare Matrixprodukt*** $sA$ als die $m \times n$-Matrix mit Eintrag $sa_{ij}$ an der Stelle $(i, j)$.

Beispiele: $\begin{bmatrix}2&1&0\\1&3&5\end{bmatrix}+\begin{bmatrix}1&0&3\\4&-3&1\end{bmatrix}=\begin{bmatrix}3&1&3\\5&0&6\end{bmatrix}$ und $(-2)\begin{bmatrix}2&1&0\\1&3&5\end{bmatrix}=\begin{bmatrix}-4&-2&0\\-2&-6&-10\end{bmatrix}$.

**Bemerkung 12.3.** Es gelten die folgenden Rechenregeln.
(a) Seien $A, B, C \in R^{m\times n}$. Dann gilt $A+B = B+A$ und $(A+B)+C = A+(B+C)$. Die Menge $R^{m\times n}$ zusammen mit der oben definierten Matrixaddition ist eine ***abelsche Gruppe***. Das neutrale Element ist $0_{m\times n}$, die Matrix, die nur aus Nullen besteht; das zu $A = [a_{ij}] \in R^{m\times n}$ inverse Element (bezüglich der Addition) ist die Matrix $-A = [-a_{ij}]$.
(b) Es gilt $1 \cdot A = A$ und $(s+t)A = sA + tA$, $(st)A = s(tA)$, $s(A+B) = sA + sB$ für alle $s, t \in R$.

*Beweis.* Einfaches Nachrechnen mit den entsprechenden Regeln für $R$. □

**Definition 12.4.** Seien $m, n, p \in \mathbb{N}$ und $A \in R^{m\times n}$, $B \in R^{n\times p}$. Dann ist das ***Matrixprodukt*** $A \cdot B \in R^{m\times p}$ definiert als die Matrix mit $(i,j)$-Eintrag

$$(A \cdot B)_{ij} := \sum_{k=1}^{n} a_{ik} b_{kj} \qquad \text{für } 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant p.$$

Um das Produkt bilden zu können, muss also die erste Matrix genauso viele Spalten haben, wie die zweite Matrix Zeilen hat. Beispiel:

$$\begin{bmatrix}1&0&5\\0&1&7\end{bmatrix} \cdot \begin{bmatrix}2&3&1&1\\4&1&0&0\\0&1&1&0\end{bmatrix} \text{ ist eine } 2\times 4\text{-Matrix, nämlich gleich } \begin{bmatrix}2&8&6&1\\4&8&7&0\end{bmatrix};$$

zum Beispiel ergibt sich der Eintrag an der Stelle $(2,3)$ als $7 = 0\cdot 1 + 1\cdot 0 + 7\cdot 1$.

Spezialfall $m = 1$, $p = 1$ ("Zeile mal Spalte"): $\begin{bmatrix}3&1&2\end{bmatrix} \cdot \begin{bmatrix}1\\-1\\4\end{bmatrix} = [3\cdot 1 + 1\cdot(-1) + 2\cdot 4] = [10]$
und nach unserer Vereinbarung in Beispiel 12.1 schreiben wir dies einfach als $10$.
Damit gilt allgemein für $A \in R^{m\times n}$ und $B \in R^{n\times p}$: Sind $Z_1, \ldots, Z_m \in R^{1\times n}$ die Zeilen von $A$ und $S_1, \ldots, S_p \in R^{m\times 1}$ die Spalten von $B$, so folgt:

$$\text{Der } (i,j)\text{-Eintrag von } A \cdot B \text{ ist gleich } Z_i \cdot S_j \qquad \text{für } 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant p.$$

Außerdem: $A \cdot S_j = j\text{-te Spalte von } A \cdot B$ und $Z_i \cdot B = i\text{-te Zeile von } A \cdot B$.

Zum Beispiel in GAP werden Matrizen einfach als Listen von Listen realisiert:

```
gap> a:=[[1,0,5],[0,1,7]];;
gap> b:=[[2,3,1,1],[4,1,0,0],[0,1,1,0]];;
gap> a*b;
[ [ 2, 8, 6, 1 ], [ 4, 8, 7, 0 ] ]
```

**Bemerkung 12.5.** (a) Seien $A \in R^{m\times n}$, $B \in R^{n\times p}$, $C \in R^{p\times q}$. Dann gilt $(A\cdot B)\cdot C = A\cdot(B\cdot C)$.
(b) Seien $A, B \in R^{m\times n}$, $C \in R^{n\times l}$, $D \in R^{q\times m}$. Dann gilt $(A+B)\cdot C = A\cdot C + B\cdot C$ und

$D \cdot (A + B) = D \cdot A + D \cdot B$.
(c) Seien $A \in R^{m\times n}$ und $B \in R^{n\times p}$. Dann gilt $s(A \cdot B) = (sA) \cdot B = A \cdot (sB)$ für alle $s \in K$.

*Beweis.* Wiederum einfaches Nachrechnen; wir gehen durch die Einzelheiten in (a), weil dies eine gute Übung im Umgang mit den obigen Formeln ist. Sei $X := A\cdot B \in R^{m\times p}$. Dann ist

$$\big((A\cdot B)\cdot C\big)_{ij} = (X\cdot C)_{ij} = \sum_{k=1}^{p} X_{ik}C_{kj} \qquad \text{und} \qquad X_{ik} = \sum_{l=1}^{n} A_{il}B_{lk}$$

und damit:
$$\big((A\cdot B)\cdot C\big)_{ij} = \sum_{k=1}^{p}\Big(\sum_{l=1}^{n} A_{il}B_{lk}\Big)C_{kj} = \sum_{k=1}^{p}\sum_{l=1}^{n}(A_{il}B_{lk})C_{kj}. \tag{1}$$

Analog erhält man

$$\big(A\cdot(B\cdot C)\big)_{ij} = \sum_{k=1}^{n} A_{ik}\Big(\sum_{l=1}^{p} B_{kl}C_{lj}\Big) = \sum_{k=1}^{n}\sum_{l=1}^{p} A_{ik}(B_{kl}C_{lj}) = \sum_{l=1}^{n}\sum_{k=1}^{p} A_{il}(B_{lk}C_{kj}), \tag{2}$$

wobei im letzten Schritt die Symbole $k$ und $l$ vertauscht werden. Weil die Multiplikation in $R$ assoziativ ist, sind die Ausdrücke (1) und (2) gleich. Der Beweis von (b), (c) geht analog. □

**Satz 12.6.** *Sei $m = n$. Dann ist $(M_n(R), +, \cdot)$ ein Ring mit Einselement gegeben durch*

$$I_n := \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{bmatrix} \qquad \textit{“}\boldsymbol{Einheitsmatrix}\textit{”}.$$

*Für $n = 1$ ist $M_n(R)$ kommutativ; für $n \geqslant 2$ ist $M_n(R)$ nicht kommutativ.*

*Beweis.* Nach Bemerkung 12.3 ist $(M_n(R), +)$ eine abelsche Gruppe. Nach Bemerkung 12.5 ist die Multiplikation assoziativ und es gelten die Distributivregeln. Schließlich überzeugt man sich davon, dass $A \cdot I_n = I_n \cdot A = A$ für alle $A \in M_n(R)$ gilt, also $I_n$ das neutrale Element bezüglich der Multiplikation ist.

Für $n = 1$ ist $M_1(R) = \{[a] \mid a \in R\}$ und $[a] \cdot [b] = [ab]$ für alle $a, b \in R$. Damit folgt sofort $[a] \cdot [b] = [b] \cdot [a]$, also ist $M_1(R)$ kommutativ.

Für $n = 2$ ist z.B. $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ und $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, also ist $M_2(R)$ nicht kommutativ. Für $n > 3$ erhält man analog:

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix},$$

also ist $M_n(R)$ nicht kommutativ. □

**Beispiel 12.7.** Seien $m, n \in \mathbb{N}$. Seien $1 \leqslant i \leqslant m$ und $1 \leqslant j \leqslant n$.

Dann heißt die Matrix $E_{ij}^{(m,n)} = \begin{bmatrix} 0 & \dots & 0 \\ \vdots & 1 & \vdots \\ 0 & \dots & 0 \end{bmatrix} \in R^{m\times n}$ die $(i,j)$-***Standardmatrix***;

hier ist der Eintrag $1$ an der Position $(i,j)$, alle anderen Einträge sind $0$.

Für $A = [a_{ij}] \in R^{m\times n}$ gilt dann die Gleichung $A = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} E_{ij}^{(m,n)}$.

Ist $n = 1$ oder $m = 1$, so erhalten wir die ***Standardvektoren***

$$e_i := E_{i1}^{(m,1)} = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \in R^{m\times 1} \qquad \text{und} \qquad f_j := E_{1j}^{(1,n)} = \begin{bmatrix} 0 & \dots & 1 & \dots & 0 \end{bmatrix} \in R^{1\times n},$$

wobei in $e_i$ die $1$ an der $i$-ten und in $f_j$ die $1$ an der $j$-ten Stelle steht (und alle anderen Einträge jeweils wieder $0$ sind). Ist auch $p \in \mathbb{N}$, so gilt die Produktformel

$$E_{ij}^{(m,n)} \cdot E_{kl}^{(n,p)} = \delta_{jk} E_{il}^{(m,p)} \in R^{m\times p} \qquad \text{für alle erlaubten } i,j,k,l;$$

hier heißt $\delta_{jk}$ das ***Kronecker-Delta***; dies ist $1$ falls $j = k$, und $0$ für $j \neq k$.

Ist $B \in R^{n\times m}$ (also $n$ Zeilen und $m$ Spalten) so erhält man die nützlichen Formeln

$$B \cdot e_i = \text{ } i\text{-te Spalte von } B \qquad \text{und} \qquad f_j \cdot B = \text{ } j\text{-te Zeile von } B.$$

**Bemerkung 12.8.** Seien $n, m \in \mathbb{N}$ beliebig und $A = [a_{ij}] \in R^{m\times n}$. Sei dann $A^{tr} \in R^{n\times m}$ die Matrix mit Eintrag $a_{ji}$ an der Position $(i,j)$, wobei $1 \leqslant i \leqslant n$ und $1 \leqslant j \leqslant m$.

Die Matrix $A^{tr}$ heißt ***transponierte Matrix***. Zum Beispiel ist $\begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 5 \end{bmatrix}^{tr} = \begin{bmatrix} 2 & 1 \\ 1 & 3 \\ 0 & 5 \end{bmatrix}$.

Für das Transponieren gelten die folgenden Regeln (Beweis durch leichtes Nachrechnen):

(a) Es gilt offenbar $(A^{tr})^{tr} = A$.

(b) Für $B \in R^{m\times n}$ und $s \in R$ gelten $(A + B)^{tr} = A^{tr} + B^{tr}$ und $(sA)^{tr} = s(A^{tr})$.

(c) Ist auch $p \in \mathbb{N}$ und $B \in R^{n\times p}$, so gilt $(A \cdot B)^{tr} = B^{tr} \cdot A^{tr}$.

Ist $n = m$, so heißt $A$ eine ***symmetrische Matrix***, wenn $A = A^{tr}$ gilt. Aufgrund der obigen Regeln sind Summen und skalare Vielfache von symmetrischen Matrizen wieder symmetrisch.

**Ab hier Woche 8**

**Definition 12.9.** Sei $m = n$. Eine Matrix $A \in M_n(R)$ heißt ***invertierbar*** (oder ***nicht-singulär***), wenn es eine Matrix $B \in M_n(R)$ gibt mit $A \cdot B = B \cdot A = I_n$.

Zum Beispiel ist $A = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \in M_2(\mathbb{Q})$ nicht-singulär, denn mit $B = \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix}$ gilt $A \cdot B = B \cdot A = I_2$. Ebenso ist $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \in M_2(\mathbb{Q})$ nicht-singulär, denn mit $B = \begin{bmatrix} 1 & 0 \\ 0 & 1/2 \end{bmatrix}$ gilt $A \cdot B = B \cdot A = I_2$. (Beachten Sie: Dieses $A$ hat Einträge in $\mathbb{Z}$, aber $A$ ist nicht invertierbar in $M_2(\mathbb{Z})$.) Die Matrix $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ ist nicht invertierbar, denn ist $B \in M_2(R)$ beliebig, so besteht die zweite Zeile von $A \cdot B$ nur aus Nullen, also $A \cdot B \neq I_2$.

**Satz 12.10.** *Sei $m = n$. Dann ist $GL_n(R) := \{A \in M_n(R) \mid A$ nicht-singulär$\}$ eine Gruppe bezüglich der Matrixmultiplikation. Das neutrale Element ist die Einheitsmatrix $I_n$; die inverse Matrix zu $A$ wird mit $A^{-1}$ bezeichnet.*

*Beweis.* Nach Satz 12.6 ist die Matrixmultiplikation assoziativ, und $I_n$ ist ein neutrales Element. Sind $A, B \in M_n(R)$ nicht-singulär, so ist auch $A \cdot B$ nicht-singulär, mit inverser Matrix $B^{-1} \cdot A^{-1}$ (siehe Bemerkung 7.1(c)). Also gilt: $A, B \in GL_n(R) \Rightarrow A \cdot B \in GL_n(R)$. Damit sind alle Axiome in Definition 7.2 erfüllt. □

**Bemerkung 12.11.** (a) Sei $m = n$ und $R = K$ ein Körper. Wir werden später noch effiziente Methoden kennenlernen, um zu testen ob $A \in M_n(K)$ invertierbar ist und dann auch $A^{-1}$ zu berechnen. Außerdem werden wir sehen: Ist $B \in M_n(K)$ mit $A \cdot B = I_n$, so folgt automatisch $B \cdot A = I_n$. — Dies ist nicht offensichtlich!

(b) Für $n = 2$ ist $GL_n(R)$ nicht abelsch. Für $n = 2$ betrachte z.B. die Matrizen $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ und $B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Dann rechnen Sie nach, dass $A, B$ invertierbar sind, aber $A \cdot B \neq B \cdot A$.

Sei $K$ ein Körper. Wir versuchen nun zum Schluss, möglichst einfache invertierbare Matrizen in $GL_n(K)$ zu finden; dies wird sich im nächsten Abschnitt als nützlich erweisen. Sei $n \in \mathbb{N}$. Für $1 \leqslant i, j \leqslant n$ sei $E_{ij} \in M_n(K)$ die $(i,j)$-Standard-Matrix $E_{ij}^{(n,n)}$; siehe Beispiel 12.7.

Für $1 \leqslant i \leqslant n$ und $0 \neq c \in K$ sei $M_i(c) := I_n + (c-1)E_{ii} = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & c & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{bmatrix}$.

(Diagonalmatrix mit $c$ an der $i$-ten Position und 1 sonst auf der Diagonalen.)

Für $c \in K$ und $1 \leqslant i, j \leqslant n$ mit $i \neq j$ sei $I_{ij}(c) := I_n + cE_{ij} =$

$$\begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & c & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{bmatrix}.$$

(Man nimmt die Einheitsmatrix und setzt noch das $c$ an die Stelle $(i, j)$.)

Für $1 \leqslant i, j \leqslant n$ mit $i \neq j$ sei $V_{ij} := I_n + E_{ij} + E_{ji} - E_{ii} - E_{jj} =$

$$\begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 0 & \dots & 1 & \\ & & \vdots & & \vdots & \\ & & i & \dots & 0 & \\ & & & & & \ddots \\ & & & & & & 1 \end{bmatrix}.$$

(Vertausche in der Einheitsmatrix die $i$-te und $j$-te Zeile.)

Diese Matrizen $M_i(c)$, $I_{ij}(c)$, $V_{ij}$ heißen ***Elementarmatrizen***.

**Lemma 12.12.** *Die oben definierten Elementarmatrizen sind invertierbar, also in* $\mathrm{GL}_n(K)$ *enthalten. Es gilt* $M_i(c)^{-1} = M_i(c^{-1})$, $I_{ij}(c)^{-1} = I_{ij}(-c)$ *und* $V_{ij}^{-1} = V_{ij}$. *Insbesondere ist das Inverse einer Elementarmatrix auch wieder eine Elementarmatrix.*

*Beweis.* Einfaches Nachrechnen, mit Hilfe der Formeln in Beispiel 12.7. □

Wir werden späten sehen (siehe Satz **??**), dass sich jede invertierbare Matrix in $\mathrm{GL}_n(K)$ als Produkt von Elementar-Matrizen schreiben lässt.

## 13. *Elementare Umformungen und das Gauß–Verfahren*

Sei $K$ ein Körper. Ein ***lineares Gleichungssystem*** (LGS) ist ein Gleichungssystem der Form

$$\left.\begin{array}{ccccccccc} a_{11}x_1 & + & \dots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & \dots & + & a_{2n}x_n & = & b_2 \\ \vdots & & & & \vdots & & \vdots \\ a_{m1}x_1 & + & \dots & + & a_{mn}x_n & = & b_m \end{array}\right\} \quad (*)$$

wobei $m, n \in \mathbb{N}$, die Koeffizienten $a_{ij} \in K$ und $b_i \in K$ vorgegeben und die $x_i \in K$ gesucht sind. (Wir haben $m$ Gleichungen und $n$ Unbekannte $x_1, \dots, x_n$.) Das LGS heißt ***homogen***, wenn $b_i = 0$ für alle $i$ gilt; sonst heißt das LGS ***inhomogen***. Die ***Lösungsmenge*** eines LGS (egal ob homogen oder inhomogen) ist gegeben durch

$$L := \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in K^n \;\middle|\; x_1, \dots, x_n \text{ Lösung von } (*) \right\}.$$

**Bemerkung 13.1.** Mit obigen Bezeichnungen bilden wir die $(m \times n)$-Matrix $A = [a_{ij}] \in K^{m \times n}$ und den Spaltenvektor $b \in K^n$ mit Einträgen $b_1, \dots, b_n$. Seien $x_1, \dots, x_n \in K$. Mit der Definition des Matrixproduktes folgt dann sofort:

$$x := \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in L \quad \text{(d.h., } x \text{ ist Lüsung von } (*)) \qquad \Leftrightarrow \qquad A \cdot x = b.$$

Dann heißt $[A|b] := \left[\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array}\right] \in K^{m\times(n+1)}$ ***erweiterte Matrix des LGS***.

(Ist $b_i = 0$ für alle $i$, so bezeichnen wir einfach $A$ als Matrix des LGS.)

**Beispiel 13.2.** (a) Sei $K$ beliebig. Die beiden Gleichungen $x_1 + x_2 = 1$, $x_1 + x_2 = 0$ bilden ein LGS mit $m = n = 2$; die erweiterte Matrix ist $\left[\begin{array}{cc|c} 1 & 1 & 1 \\ 1 & 1 & 0 \end{array}\right]$. Es gibt keine Lösung, $L = \varnothing$.

(b) Sei $K = \mathbb{Q}$. Die Gleichungen $x_1 + x_2 = 1$ und $x_2 - x_3 = 2$ bilden ein LGS mit $m = 2$, $n = 3$; die erweiterte Matrix ist $\left[\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & -1 & 2 \end{array}\right]$.
Lösung: Aus der 2. Gleichung erhalten wir $x_2 = 2 + x_3$; einsetzen in die 1. Gleichung ergibt $x_1 + (2 + x_3) = 1$, also $x_1 = -1 - x_3$. Damit

$$L = \left\{ \begin{bmatrix} -1 - x_3 \\ 2 + x_3 \\ x_3 \end{bmatrix} \;\middle|\; x_3 \in \mathbb{Q} \text{ beliebig} \right\}.$$

(c) Sei $K = \mathbb{Q}$. Die Gleichungen $x_1 + x_2 = 3$ und $3x_1 - x_2 = 1$ bilden ein LGS mit $m = n = 2$; die erweiterte Matrix ist $\left[\begin{array}{cc|c} 1 & 1 & 3 \\ 3 & -1 & 1 \end{array}\right]$.
Lösung: Addiere 1. Gleichung zur 2. Gleichung und erhalte $4x_1 = 4$, also $x_1 = 1$; einsetzen in die 1. Gleichung ergibt dann $1 + x_2 = 3$, also $x_2 = 2$. Damit $L = \left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right\}$.

Wir sehen also: Ein LGS kann gar keine Lösung haben, genau eine Lösung oder unendlich viele Lösungen. Ein systematisches Lösungsverfahren ist durch die ***Gauß–Elimination*** gegeben. Dabei formt man die Gleichungen so um, dass das LGS eine einfachere Gestalt bekommt und man die Lösungen leicht ablesen kann. Grundlage dafür ist folgende Bemerkung.

**Bemerkung 13.3.** Gegeben sei ein LGS $(*)$, mit erweiterter Matrix $[A|b] \in K^{m\times(n+1)}$ und Lösungsmenge $L \subseteq K^n$. Sei nun $Q \in M_m(K)$; setze $A' := Q \cdot A$, $b' := Q \cdot b$. Aufgrund der Definition der Matrixmultiplikation gilt dann auch $[A'|b'] = Q \cdot [A|b]$. Wir erhalten ein neues LGS mit erweiterter Matrix $[A'|b'] \in K^{m\times(n+1)}$; sei $L' \subseteq K^n$ dessen Lösungsmenge. Dann gilt $L \subseteq L'$; ist $Q \in GL_m(K)$ invertierbar, so gilt $L = L'$.

Denn: Sei $x \in L$, also $A \cdot x = b$. Dann folgt $A' \cdot x = (Q \cdot A) \cdot x = Q \cdot (A \cdot x) = Q \cdot b = b'$, also $x \in L'$. Damit ist $L \subseteq L'$ gezeigt. Sei nun $Q$ invertierbar. Dann folgt $A = Q^{-1} \cdot A'$ und $b = Q^{-1} \cdot b'$. Ist also $x' \in L'$, so folgt mit dem gleichen Argument wie zuvor auch $x' \in L$. □

Wir bringen nun die am Ende des letzten Abschnitts definierten ***Elementarmatrizen*** ins Spiel. Im folgenden Satz sind $M_i(c)$, $I_{ij}(c)$ und $V_{ij}$ Matrizen der Grösse $m \times m$.

**Satz 13.4.** *Sei* $A \in K^{m\times n}$*. Dann gilt:*
(a) $M_i(c) \cdot A$ *ist die Matrix, die aus* $A$ *entsteht, wenn man die* $i$*-te Zeile mit* $c$ *multipliziert.*
(b) $I_{ij}(c) \cdot A$ *ist die Matrix, die aus* $A$ *entsteht, wenn man das* $c$*-Fache der* $j$*-ten Zeile zur* $i$*-ten Zeile addiert.*
(c) $V_{ij} \cdot A$ *ist die Matrix, die aus* $A$ *entsteht, wenn man die* $i$*-te und* $j$*-te Zeile vertauscht.*

*Entsprechende Aussagen gelten auch für* $B \in R^{n\times m}$ *und die Produkte* $B \cdot M_i(c)$, $B \cdot I_{ij}(c)$, $B \cdot V_{ij}$, *wobei die obigen Operationen mit den Spalten von* $B$ *ausgeführt werden.*

*Beweis.* Auch dies erfolgt durch Nachrechnen, wobei man mehrere Fälle unterscheiden muss. Es hilft, wenn man zuerst den Fall $m = 2$ betrachtet, also:

$$M_1(c) \cdot A = \begin{bmatrix} c & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \end{bmatrix} = \begin{bmatrix} ca_{11} & ca_{12} & \dots & ca_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \end{bmatrix};$$

$$M_2(c) \cdot A = \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ ca_{21} & ca_{22} & \dots & ca_{2n} \end{bmatrix};$$

$$I_{12}(c) \cdot A = \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \end{bmatrix} = \begin{bmatrix} a_{11}+ca_{21} & a_{12}+ca_{22} & \dots & a_{1n}+ca_{2n} \\ a_{21} & a_{22} & \dots & a_{2n} \end{bmatrix};$$

$$I_{21}(c) \cdot A = \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21}+ca_{11} & a_{22}+ca_{12} & \dots & a_{2n}+ca_{1n} \end{bmatrix};$$

$$V_{12} \cdot A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \end{bmatrix} = \begin{bmatrix} a_{21} & a_{22} & \dots & a_{2n} \\ a_{11} & a_{12} & \dots & a_{1n} \end{bmatrix}.$$

Die weiteren Details seien Ihnen als Übung überlassen. □

Seien $A, B \in K^{m\times n}$. Wir sagen, dass $B$ aus $A$ durch ***elementare Umformungen*** (oder genauer: ***elementare Zeilenumformungen***) entsteht (und schreiben $A \to B$), wenn man $B$ aus $A$ durch eine endliche Folge von Operationen wie in Satz 13.4 erhält, also:

(a) Multipliziere eine Zeile mit einem Element $0 \neq c \in K$.
(b) Addiere das $c$-Fache (für ein $c \in K$) einer Zeile zu einer anderen Zeile.
(c) Vertausche zwei Zeilen.

Entsprechend können auch ***elementare Spaltenumformungen*** definiert werden.

**Satz 13.5** (***Gauß–Elimination***)**.** *Sei* $K$ *ein Körper und* $A \in K^{m\times n}$*. Dann lässt sich* $A$ *durch eine endliche Folge von elementaren Zeilenumformungen auf* ***Stufenform*** *bringen.*

Hier sagen wir, dass $A' = [a'_{ij}] \in K^{m\times n}$ **Stufenform** hat, wenn es ein $r \in \{0, 1, 2, \ldots, m\}$ und (Spalten-)Indizes $1 \leqslant j_1 < j_2 < \ldots < j_r \leqslant n$ gibt, so dass $A'$ folgende Gestalt besitzt:

$$\begin{array}{c|c} & \begin{array}{ccccccccccccc} & & & j_1 & & & j_2 & & & j_3 & \cdots & & j_r & \\ 1 & 0 & \ldots & 0 & 1 & *\cdots* & 0 & *\cdots* & 0 & *\cdots* & 0 & *\cdots & & \\ 2 & & & & & & 1 & *\cdots* & 0 & *\cdots* & 0 & *\cdots & & \\ \vdots & & & & & & & & 1 & *\cdots* & 0 & *\cdots & & \\ & \multicolumn{3}{c}{\text{(Hier 0 vor jeder 1)}} & & & & & & & \ddots & & & \\ r & & & & & & & & & & & & 1 & *\cdots* \end{array} \\ \hline \begin{array}{c} r+1 \\ \vdots \\ m \end{array} & \multicolumn{13}{c}{\text{(Alles 0 hier)}} \end{array}$$

Die Sterne $*$ stehen hier für beliebige Elemente aus $K$ als Einträge; links vor sowie oberhalb und unterhalb den Einsen in den Spalten $j_1, \ldots, j_r$ stehen nur Nullen. Oder in Formeln:

$$\begin{array}{rcll} a'_{ij} & = & 0 & \text{für } i > r \text{ und alle } j = 1, \ldots, n, \\ a'_{ij} & = & 0 & \text{für } 1 \leqslant i \leqslant r \text{ und } 1 \leqslant j < j_i, \\ a'_{ij_i} & = & 1 & \text{für } 1 \leqslant i \leqslant r, \\ a'_{kj_i} & = & 0 & \text{für } 1 \leqslant k \leqslant r \text{ und } k \neq i. \end{array}$$

Die Indizes $j_1, \ldots, j_r$ werden auch ***Pivots*** genannt. (Beachten Sie, dass in manchen Texten nicht verlangt wird, dass oberhalb der Einsen in den Spalten $j_1, \ldots, j_r$ nur Nullen stehen.) Bevor wir dies allgemein beweisen, zuerst ein Beispiel (mit $K = \mathbb{Q}$).

$$\begin{aligned} A = \begin{bmatrix} 0 & 0 & 2 & 2 & 0 & 2 \\ 2 & 4 & 2 & 6 & 0 & 4 \\ 3 & 6 & 0 & 6 & 1 & 4 \end{bmatrix} &\to \begin{bmatrix} 2 & 4 & 2 & 6 & 0 & 4 \\ 0 & 0 & 2 & 2 & 0 & 2 \\ 3 & 6 & 0 & 6 & 1 & 4 \end{bmatrix} \to \begin{bmatrix} 1 & 2 & 1 & 3 & 0 & 2 \\ 0 & 0 & 2 & 2 & 0 & 2 \\ 3 & 6 & 0 & 6 & 1 & 4 \end{bmatrix} \\ &\to \begin{bmatrix} \underline{1} & 2 & 1 & 3 & 0 & 2 \\ 0 & 0 & 2 & 2 & 0 & 2 \\ 0 & 0 & -3 & -3 & 1 & -2 \end{bmatrix} \to \begin{bmatrix} \underline{1} & 2 & 1 & 3 & 0 & 2 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & -3 & -3 & 1 & -2 \end{bmatrix} \to \begin{bmatrix} \underline{1} & 2 & 1 & 3 & 0 & 2 \\ 0 & 0 & \underline{1} & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \underline{1} & 1 \end{bmatrix} \\ &\to \begin{bmatrix} \underline{1} & 2 & 0 & 2 & 0 & 1 \\ 0 & 0 & \underline{1} & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \underline{1} & 1 \end{bmatrix} =: A' \qquad \text{mit } r = 3 \text{ und Pivots } j_1 = 1,\ j_2 = 3,\ j_3 = 5. \end{aligned}$$

Die 6 Pfeile $\to$ entsprechen dabei (von links nach rechts) den elementaren Schritten $V_{12}$, $M_1(1/2)$, $I_{31}(-3)$, $M_2(1/2)$, $I_{32}(3)$, $I_{12}(-1)$. (Der letzte Schritt ist nur nötig um alle Einträge über dem Pivot $j_2 = 3$ gleich $0$ zu machen.) Mit Satz 13.4 erhalten wir dann auch $A' = Q \cdot A$ mit $Q := I_{12}(-1) \cdot I_{32}(3) \cdot M_2(1/2) \cdot I_{31}(-3) \cdot M_1(1/2) \cdot V_{12}$.

*Beweis von Satz 13.5.* (Vollständige Induktion nach $m$.) Für den Startwert $m = 1$ ist $A = [a_{11} \ \ldots \ a_{1n}] \in K^{1\times n}$ eine Zeile. Sind alle Einträge gleich $0$, so sind wir fertig mit $r = 0$. Andernfalls sei $j_1 := \min\{j \mid a_{1j} \neq 0\}$. Multplizieren mit $a_{1j_1}^{-1}$ ergibt $A \to [0 \ \ldots \ 0 \ 1 \ * \ \ldots \ *]$, wobei die $1$ an der Stelle $j_1$ steht; also haben wir Stufenform erreicht mit $r = 1$.

Sei nun $m \geqslant 2$ und die Aussage bereits für $(m-1)\times n$-Matrizen gezeigt. Ist $A = 0_{m\times n}$, so hat $A$ Stufenform mit $r = 0$. Andernfalls sei $j_1 := \min\{j \mid j\text{-te Spalte von } A \text{ enthält Eintrag} \neq 0\}$. Sei $i \in \{1,\dots,m\}$ mit $a_{ij_1} \neq 0$. Dann multipliziere die $i$-te Zeile mit $a_{ij_1}^{-1}$; ist $i > 1$, so vertausche außerdem die $i$-te mit der 1. Zeile. Dies ergibt:

$$A \quad \to \quad B := \begin{bmatrix} 0 & \dots & 0 & 1 & * & \dots & * \\ 0 & \dots & 0 & b_{2j_1} & * & \dots & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & b_{mj_1} & * & \dots & * \end{bmatrix}$$

Dann addiere nacheinander:

$$\left.\begin{array}{l} \text{das } (-b_{2j_1})\text{-Fache der 1. Zeile zur 2. Zeile} \\ \text{das } (-b_{3j_1})\text{-Fache der 1. Zeile zur 3. Zeile} \\ \quad\vdots \\ \text{das } (-b_{mj_1})\text{-Fache der 1. Zeile zur m. Zeile} \end{array}\right\} \quad \to \quad \begin{bmatrix} 0 & \dots & 0 & 1 & * & \dots & * \\ 0 & \dots & 0 & 0 & * & \dots & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & * & \dots & * \end{bmatrix}$$

Sei nun $C \in K^{(m-1)\times n}$ die Matrix, die aus den Zeilen $2, 3, \dots, m$ der Matrix auf der rechten Seite besteht. Nach Induktion kann man $C$ auf Stufenform bringen. Insgesamt also

$$A \to \begin{array}{c|c} & \begin{array}{ccccccccccccc} & & & j_1 & & & j_2 & & & j_3 & & & j_r & \end{array} \\ \hline \begin{array}{c} 1 \\ 2 \\ \vdots \\ \\ \\ r \end{array} & \left[\begin{array}{ccccccccccccc} 0 & \dots & 0 & 1 & * & \cdots & * & * & \cdots & * & * & \cdots & * & * & \cdots \\ & & & & & & 1 & * & \cdots & * & 0 & \cdots & * & * & \cdots \\ & & & & & & & & & 1 & * & \cdots & * & * & \cdots \\ & & & & & & & & & & & \ddots & & & \\ & & & & & & & & & & & & 1 & * & \cdots * \end{array}\right] \\ \hline \begin{array}{c} r+1 \\ \vdots \\ m \end{array} & \left[\begin{array}{ccccccc} 0 & & & & \dots & & 0 \\ \vdots & & & & & & \vdots \\ 0 & & & & \dots & & 0 \end{array}\right] \end{array}$$

Schließlich addiere noch passende Vielfache der Zeilen $2, 3, \dots, r$ zur 1. Zeile, um die Einträge in der 1. Zeile oberhalb der Pivots $j_2, \dots, j_r$ zu Null zu machen. □

Es ist eine exzellente Übung, obiges Verfahren in einer Programmiersprache Ihrer Wahl zu programmieren. In GAP gibt es dazu bereits eine Funktion:

```
gap> EchelonizeMat([[0,0,2,2,0,2],[2,4,2,6,0,4],[3,6,0,6,1,4]]);
[ [ 1, 2, 0, 2, 0, 1 ], [ 0, 0, 1, 1, 0, 1 ], [ 0, 0, 0, 0, 1, 1 ] ]
```

**Folgerung 13.6.** *Sei $A \in K^{m\times n}$. Dann gibt es eine invertierbare Matrix $Q \in \mathrm{GL}_m(K)$, so dass $Q\cdot A \in K^{m\times n}$ Stufenform hat; $Q$ ist ein Produkt von endlich vielen Elementar-Matrizen.*

*Beweis.* Nach Satz 13.4 werden die im Gauß–Verfahren verwendeten elementaren Umformungen durch schrittweise Multiplikationen mit Elementarmatrizen realisiert; letztere sind invertierbar nach Lemma 12.12. Ist also $A \to A'$ und $A'$ in Stufenform, so gilt $A' = Q \cdot A$, wobei $Q$ Produkt von Elementarmatrizen ist. □

## Anwendung auf lineare Gleichungssysteme

Gegeben sei ein LGS mit erweiterter Matrix $[A|b] \in K^{m\times(n+1)}$. Gesucht ist die Lösungsmenge $L = \{x \in K^n \mid A \cdot x = b\}$. Dazu bringen wie $[A|b]$ nach obigem Verfahren auf Stufenform, also $[A|b] \to [A'|b']$ mit $A' \in K^{m\times n}$ und $b' \in K^m$. Mit Folgerung 13.6 und Bemerkung 13.3 folgt dann $L = \{x \in K^n \mid A' \cdot x = b'\}$. Nehmen wir an, dass $[A|b]$ nicht nur aus Nullen besteht; dann haben wir $r \in \{1, \dots, m\}$ Stufen in $[A'|b']$ und Pivots $1 \leqslant j_1 < \dots < j_r \leqslant n+1$.

1. Fall: $j_r = n+1$. Dann ist die $r$-te Zeile in $[A'|b']$ gegeben durch $[0 \ \dots \ 0 \ 1]$. Dies entspricht der Gleichung $0 \cdot x_1 + \dots + 0 \cdot x_n = 1$. Also gibt es in diesem Fall keine Lösung, $L = \varnothing$.

2. Fall: $j_r \leqslant n$. Setzen wir $I := \{1, \dots, n\} \setminus \{j_1, \dots, j_r\}$, so besteht das durch $[A'|b']$ gegebene LGS aufgrund der Bedingungen in der Stufenform aus den folgenden Gleichungen:

$$\begin{array}{rcl}
x_{j_1} + \sum_{j\in I} a'_{1j}x_j &=& b'_1 \\
x_{j_2} + \sum_{j\in I} a'_{2j}x_j &=& b'_2 \\
\vdots \qquad\quad \vdots &&\ \vdots \\
x_{j_r} + \sum_{j\in I} a'_{rj}x_j &=& b'_r
\end{array}
\quad\rightsquigarrow\quad
\begin{array}{rcl}
x_{j_1} &=& b'_1 - \sum_{j\in I} a'_{1j}x_j \\
x_{j_2} &=& b'_2 - \sum_{j\in I} a'_{2j}x_j \\
\vdots \quad\ \vdots &&\ \vdots \\
x_{j_r} &=& b'_r - \sum_{j\in I} a'_{rj}x_j
\end{array}$$

Hier sind alle $x_j$ mit $j \in I$ (d.h., alle $x_j$ außer $\{x_{j_1}, \dots, x_{j_r}\}$) frei wählbar, und $x_{j_1}, \dots, x_{j_r}$ sind dann durch die obigen Gleichungen bestimmt. Daher heißen $x_{j_1}, \dots, x_{j_r}$ auch "Pivot-Variablen" und die restlichen $n - r$ Unbekannten $\{x_j \mid j \in I\}$ heißen "freie Variablen".

**Beispiel 13.7.** (a) Betrachte das LGS mit $[A|b] = \left[\begin{array}{cc|c} 1 & 1 & 1 \\ 1 & 1 & 0 \end{array}\right]$, wie in Beispiel 13.2(a). Dann ist $[A|b] \to \left[\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right]$, also $r = 2$, $j_1 = 1$, $j_2 = 3$. Wir sind im 1. Fall, also $L = \varnothing$.

(b) Sei $[A|b] = \left[\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & -1 & 2 \end{array}\right]$, wie in Beispiel 13.2(b). Dann ist $[A|b] \to \left[\begin{array}{ccc|c} 1 & 0 & 1 & -1 \\ 0 & 1 & -1 & 2 \end{array}\right]$. Wir sind im 2. Fall, mit Pivot-Variablen $x_1$, $x_2$ und einer freien Variablen $x_3$. Wir schreiben die neuen Gleichungen hin und lösen dann nach den Pivot-Variablen auf:

$$\begin{array}{rcl}
\underline{x_1} + x_3 &=& -1 \\
\underline{x_2} - x_3 &=& 2
\end{array}
\quad\rightsquigarrow\quad
\begin{array}{rcl}
x_1 &=& -1 - x_3 \\
x_2 &=& 2 + x_3
\end{array}.$$

Also erhalten wir als Lösungsmenge $L = \left\{ \begin{bmatrix} -1 - x_3 \\ 2 + x_3 \\ x_3 \end{bmatrix} \;\middle|\; x_3 \in \mathbb{Q} \right\} = \left\{ \begin{bmatrix} -1 - t \\ 2 + t \\ t \end{bmatrix} \;\middle|\; t \in \mathbb{Q} \right\}$.

(c) Sei $[A|b] = \left[\begin{array}{cc|c} 1 & 1 & 3 \\ 3 & -1 & 1 \end{array}\right]$, wie in Beispiel 13.2(c). Dann ist $[A|b] \to \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 2 \end{array}\right]$, also 2. Fall mit Pivot-Variablen $x_1$, $x_2$ und keiner freien Variablen. Die neuen Gleichungen sind jetzt einfach gegeben durch $x_1 = 1$ und $x_2 = 2$. Also erhalten wir $L = \left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right\}$.

Betrachten wir schließlich auch noch das LGS mit erweiterter Matrix

$$[A|b] = \left[\begin{array}{ccccc|c} 0 & 0 & 2 & 2 & 0 & 2 \\ 2 & 4 & 2 & 6 & 0 & 4 \\ 3 & 6 & 0 & 6 & 1 & 4 \end{array}\right] \qquad \to \qquad \left[\begin{array}{ccccc|c} \underline{1} & 2 & 0 & 2 & 0 & 1 \\ 0 & 0 & \underline{1} & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \underline{1} & 1 \end{array}\right] \qquad \text{(siehe oben).}$$

Wir sind im 2. Fall mit Pivot-Variablen $x_1, x_3, x_5$ und freien Variablen $x_2, x_4$. Wir schreiben wieder die neuen Gleichungen hin und lösen dann nach den Pivot-Variablen auf:

$$\begin{array}{rcl} \underline{x_1} + 2x_2 + 2x_4 &=& 1 \\ \underline{x_3} + x_4 &=& 1 \\ \underline{x_5} &=& 1 \end{array} \quad \rightsquigarrow \quad \begin{array}{rcl} x_1 &=& 1 - 2x_2 - 2x_4 \\ x_3 &=& 1 - x_4 \\ x_5 &=& 1 \end{array} \quad \rightsquigarrow \quad L = \left\{ \begin{bmatrix} 1-2s-2t \\ s \\ 1-t \\ t \\ 1 \end{bmatrix} \;\middle|\; s, t \in \mathbb{Q} \right\}.$$

**Bemerkung 13.8.** Ist $r = n \leqslant m$ und $j_r \leqslant n$, so gibt es keine freien Variablen und die Pivot-Variablen sind $x_1, \ldots, x_n$. In diesem Fall gibt es eine eindeutige Lösung:

$$[A|b] \qquad \to \qquad [A'|b'] = \left[\begin{array}{ccc|c} 1 & & 0 & b'_1 \\ & \ddots & & \vdots \\ 0 & & 1 & b'_n \\ \hline 0 & \ldots & 0 & 0 \end{array}\right] \qquad \rightsquigarrow \qquad L = \left\{ \begin{bmatrix} b'_1 \\ \vdots \\ b'_n \end{bmatrix} \right\}.$$

(Unterhalb des Querstrichs sind die Zeilen $n+1, n+2, \ldots, m$, mit allen Einträgen gleich $0$.)

**Ab hier Woche 9**

# Index