Sebastian Thomas

RWTH Aachen, 2018
16. Februar 2018 *

Diskrete Strukturen

Manuskript

Die Vorlesung richtet sich an Studierende des Studiengangs Bachelor of Science Informatik und verwandter Studiengänge. Das Ziel ist die Vermittlung einiger grundlegender und für die Informatik relevanter Begriffe und Methoden aus der Mathematik.
Nach einem ausführlichen Überblick über die Sprache und Grundlagen der Mathematik im Rahmen der mathematischen Logik und der Mengenlehre werden exemplarisch Konzepte aus der Algebra, der Zahlentheorie, der linearen Algebra und der diskreten Mathematik behandelt. Nicht behandelt werden analytische, numerische und statistische Methoden sowie konzeptionelle Methoden aus der linearen Algebra – diesen sind jeweils eigene Vorlesungen gewidmet.
Es werden keinerlei Vorkenntnisse vorausgesetzt – lediglich eine gewisse Vertrautheit mit den Zahlbereichen aus der Schule ist von Vorteil, um den Beispielen folgen zu können, vgl. etwa Beispiel (2.3).
Für Hinweise und Korrekturen danke ich meinen Studierenden und Tutoren; insbesondere Lars Göttgens, J. Isabel Klöter, Konrad Kollnig, Tomas L. De Stefano und Klara Tyroller für zahlreiche Korrekturen in vorherigen Versionen dieses Manuskripts. Über weitere Hinweise auf Fehler und Unklarheiten freue ich mich.

Aachen, 16. Februar 2018
Sebastian Thomas

Inhaltsverzeichnis

Dieses Vorlesungsmanuskript enthält Inhalte zur Veranstaltung *Diskrete Strukturen*; vom Autor zuletzt gehalten im Wintersemester 2017/18 an der RWTH Aachen. Es basiert auf dem Manuskript [15] sowie zu Teilen auf dem Manuskript [14].

*Dies ist eine leicht überarbeitete Version vom 5. Juli 2018. (Version 1.3.7)

1 Mathematische Logik

Zu Beginn geben wir einen Einblick in die mathematische Logik. Hierbei beschränken wir uns auf einige wenige Grundbegriffe, welche uns helfen sollen, ein Gefühl für die Struktur mathematischer Argumentführung zu entwickeln.
Nach einer Einführung über Aussagen werden aussagenlogische Formeln und ihre Wahrheitswerte sowie einige darauf aufbauende semantische Konzepte eingeführt. Danach stellen wir verschiedene Beweistechniken an Hand einfacher Resultate der Aussagenlogik vor. Mit der Behandlung von Normalformen schließen wir das Studium der Aussagenlogik ab. Zum Schluss des Abschnitts geben wir eine weitgehend informelle Behandlung der Prädikatenlogik.
Die durch Anführungsstriche markierten Wörter in diesem Abschnitt werden nicht genauer präzisiert.

Aussagen

Wir beginnen unsere Abhandlung zur mathematischen Logik mit der sogenannten *Aussagenlogik*. Unter einer *Aussage* verstehen wir einen „(umgangssprachlichen, ggf. mit Formeln angereicherten) Ausdruck“, welcher entweder wahr oder falsch ist (Bivalenzprinzip).
Beispiele für Aussagen sind

- „Die RWTH Aachen hat eine Mensa.“ (wahr),
- „Es gibt unendlich viele Primzahlen.“ (wahr),
- „$2 + 3 = 6$.“ (falsch),
- „Zu jeder reellen Zahl y gibt es eine reelle Zahl x mit $y = x^2$.“ (falsch),
- „Jede gerade Zahl, welche größer als 2 ist, ist eine Summe aus zwei Primzahlen.“ (unbekannt).

Hierbei ist der letzte Ausdruck eine Aussage, da er entweder wahr oder falsch ist, auch wenn wir den Wahrheitswert dieser Aussage nicht kennen. ([1])
Keine Aussagen sind

- „Es ist kalt.“ und
- „$a^2 + b^2 = c^2$.“,

denn beim ersten Ausdruck scheitert die Zuordnung eines eindeutigen Wahrheitswertes an der mangelnden Objektivität, während dies beim zweiten Ausdruck nicht (ohne Weiteres) gelingt, da a, b und c nicht spezifiziert ([2]) sind.

[1] Die *Goldbachsche Vermutung* besagt, dass die Aussage wahr ist.
[2] Sind a, b und c zuvor spezifiziert worden, z.B. indem man a bzw. b bzw. c als Bezeichnung für 3 bzw. 4 bzw. 5 gewählt hat, so wird dieser Ausdruck zu einer (wahren) Aussage.

Neben solchen einfachen Aussagen gibt es auch zusammengesetzte Aussagen wie etwa

„Wenn es regnet oder schneit, dann ist die Straße nass.“.

Um diese Aussage zu analysieren, betrachten wir die Aussagen

- „Es regnet.“,
- „Es schneit.“ und
- „Die Straße ist nass.“.

Unsere ursprüngliche Aussage lässt sich dann umformulieren zu

„Wenn ‚es regnet‘ oder ‚es schneit‘, dann ‚die Straße ist nass‘.“

Auch wenn diese Umformulierung zu einem schlechteren Deutsch führt, so lässt sich die logische Struktur der zusammengesetzten Aussage hierdurch besser erkennen. Noch deutlicher wird dies, wenn wir mit Abkürzungen arbeiten: Verwenden wir anstatt „Es regnet.“ das Symbol A, anstatt „Es schneit.“ das Symbol B und anstatt „Die Straße ist nass.“ das Symbol C, so erhalten wir

„Wenn (A oder B), dann C.“

Ersetzen wir schließlich noch die sprachlichen Konnektoren durch Symbole, etwa „oder“ durch das Symbol $\vee$ und „wenn ..., dann ...“ durch das Symbol $\Rightarrow$, so ergibt sich der vollständig formalisierte Ausdruck

$$(A \vee B) \Rightarrow C.$$

Wenn wir nun die Aussage „Wenn du ein Smartphone oder ein Tablet besitzt, so kannst du mobil im Internet surfen.“ auf analoge Weise formalisieren, so landen wir bei demselben logischen Ausdruck

$$(A \vee B) \Rightarrow C.$$

Der Wahrheitswert der jeweiligen zusammengesetzten Aussagen hängt nicht von den Aussagen selbst ab, sondern nur von der logischen Struktur der zusammengesetzten Aussage sowie den Wahrheitswerten der Einzelaussagen (Extensionalitätsprinzip).

Aussagenlogische Formeln

Nach unserem einführenden Beispiel werden wir nun die Logik beim Zusammensetzen von Aussagen systematisch studieren. Bevor wir die Wahrheitswerte zusammengesetzter Aussagen betrachten, führen wir zunächst eine formale Sprache ein. Die Wörter dieser Sprache werden uns als Ersatz für unsere konkreten Aussagen dienen.
Da wir noch nicht die Begriffe der Mengenlehre beherrschen, führen wir diese Sprache der Aussagenlogik etwas informell ein. Eine weitergehende Präzisierung wird erst in weiterführenden Veranstaltungen vorgenommen. Vgl. auch Anwendungsbeispiel (10.7).
Unter einem *Alphabet* verstehen wir eine vorgegebene Menge an „Symbolen“, welche wir auch *Buchstaben* oder *Zeichen* des Alphabets nennen. Die *Wörter* einer *Sprache* entstehen dann einfach durch *Aneinanderreihung* dieser Buchstaben. Vgl. Definition (10.2) und Definition (10.5).

(1.1) Definition (aussagenlogische Formel)**.**

(a) Das *Alphabet der Aussagenlogik* besteht aus „Symbolen“ A_1, A_2, A_3, ..., Symbolen 0, 1, $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ und Symbolen (und).

Die Symbole A_1, A_2, A_3, ... werden *Aussagenvariablen* ([3]) genannt. Die Symbole 0, 1, $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ werden (*aussagenlogische*) *Junktoren* genannt. Die Symbole 0 und 1 werden außerdem auch *Boolesche Konstanten* genannt. Die Symbole (und) werden *Hilfsklammern* genannt.

Das Symbol $\neg$ wird als *nicht*, das Symbol $\wedge$ als *und*, das Symbol $\vee$ als *oder*, das Symbol $\Rightarrow$ als *impliziert* und das Symbol $\Leftrightarrow$ als *äquivalent* gelesen.

Statt A_1, A_2, ..., A_{26} schreiben wir oft auch A, B, ..., Z. ([4])

[3] Auch wenn diese Terminologie sehr etabliert ist, macht sie streng genommen keinen Sinn: Eine Aussagenvariable ist ein einzelnes Symbol und nimmt keine Werte aus einem (festgelegten) Bereich an. Wir können den Aussagenvariablen allerdings gewisse Werte zuordnen, siehe Definition (1.7)(a).

[4] Da wir in Beispielen oft nur eine geringe Anzahl von Aussagenvariablen betrachten, erlaubt uns diese Konvention die Vermeidung von Indizes.

(b) Die *Sprache der Aussagenlogik* besteht aus den Wörtern über dem Alphabet der Aussagenlogik, welche in folgender Weise „sinnvoll“ ([5]) zusammengesetzt sind.

- Die Aussagenvariablen sind Wörter in der Sprache der Aussagenlogik.
- Die Boolesche Konstanten sind Wörter in der Sprache der Aussagenlogik.
- Für jedes Wort F in der Sprache der Aussagenlogik ist $\neg F$ ein Wort in der Sprache der Aussagenlogik, wobei $\neg F$ die Konkatenation des Junktors $\neg$ und des Worts F, nötigenfalls umschlossen mit Hilfsklammern, bezeichnet.
- Für Wörter F und G in der Sprache der Aussagenlogik ist $F \wedge G$ ein Wort in der Sprache der Aussagenlogik, wobei $F \wedge G$ die Konkatenation des Worts F, nötigenfalls umschlossen mit Hilfsklammern, des Junktors $\wedge$, und des Worts G, nötigenfalls umschlossen mit Hilfsklammern, bezeichnet.
- Für Wörter F und G in der Sprache der Aussagenlogik ist $F \vee G$ ein Wort in der Sprache der Aussagenlogik, wobei $F \vee G$ die Konkatenation des Worts F, nötigenfalls umschlossen mit Hilfsklammern, des Junktors $\vee$, und des Worts G, nötigenfalls umschlossen mit Hilfsklammern, bezeichnet.
- Für Wörter F und G in der Sprache der Aussagenlogik ist $F \Rightarrow G$ ein Wort in der Sprache der Aussagenlogik, wobei $F \Rightarrow G$ die Konkatenation des Worts F, nötigenfalls umschlossen mit Hilfsklammern, des Junktors $\Rightarrow$, und des Worts G, nötigenfalls umschlossen mit Hilfsklammern, bezeichnet.
- Für Wörter F und G in der Sprache der Aussagenlogik ist $F \Leftrightarrow G$ ein Wort in der Sprache der Aussagenlogik, wobei $F \Leftrightarrow G$ die Konkatenation des Worts F, nötigenfalls umschlossen mit Hilfsklammern, des Junktors $\Leftrightarrow$, und des Worts G, nötigenfalls umschlossen mit Hilfsklammern, bezeichnet.

Ein Wort in der Sprache der Aussagenlogik wird *aussagenlogische Formel* (oder *Aussageform* oder *Aussageschema*) genannt. Für eine aussagenlogische Formel F wird $\neg F$ die *Negation* von F genannt. Für aussagenlogische Formeln F und G wird $F \wedge G$ die *Konjunktion* von F und G genannt; und es werden F und G die *Konjunkte* von $F \wedge G$ genannt. Für aussagenlogische Formeln F und G wird $F \vee G$ die *Disjunktion* von F und G genannt; und es werden F und G die *Disjunkte* von $F \vee G$ genannt. Für aussagenlogische Formeln F und G wird $F \Rightarrow G$ die *Implikation* (oder die *Subjunktion* oder das *Konditional*) von F und G genannt; und es wird F die *Prämisse* von $F \Rightarrow G$ und G die *Konklusion* (oder *Conclusio*) von $F \Rightarrow G$ genannt. Für aussagenlogische Formeln F und G wird $F \Leftrightarrow G$ die *Äquivalenz* (oder das *Bikonditional*) von F und G genannt.

(1.2) Beispiel.

(a) Es ist A eine aussagenlogische Formel.

(b) Es ist 1 eine aussagenlogische Formel.

(c) Es ist $\neg B$ eine aussagenlogische Formel.

(d) Es ist $A \wedge B$ eine aussagenlogische Formel.

(e) Es ist $0 \vee 1$ eine aussagenlogische Formel.

(f) Es ist $A \vee (B \wedge (\neg C))$ eine aussagenlogische Formel.

(g) Es ist $\vee D$ keine aussagenlogische Formel.

(h) Es ist $A \Rightarrow B \Rightarrow C$ keine aussagenlogische Formel.

Wie wir an Beispiel (1.2)(f) erahnen können, tauchen in längeren aussagenlogischen Formeln vergleichsweise viele Hilfsklammern auf. Da dies zu unübersichtlichen Ausdrücken führen kann, vereinbaren wir der besseren Lesbarkeit wegen:

(1.3) Konvention. Gemäß den folgenden Regeln lassen wir im Folgenden oftmals Klammern in aussagenlogischen Formeln weg:

- Es binde $\neg$ stärker als alle anderen Junktoren.

[5] Was „sinnvoll“ konkret bedeutet, wird (hoffentlich) in Beispiel (1.2) deutlich. Wir verzichten auf eine weitergehende Präzisierung zugunsten einer knapperen Darstellung und verweisen auf weiterführende Veranstaltungen.

- Es binde $\wedge$ stärker als $\vee$, $\Rightarrow$ und $\Leftrightarrow$.
- Es binde $\vee$ stärker als $\Rightarrow$ und $\Leftrightarrow$.

Nach Konvention (1.3) schreiben wir etwa $A \vee B \wedge \neg C$ statt $A \vee (B \wedge (\neg C))$, und wir schreiben $A \Rightarrow \neg B$ statt $A \Rightarrow (\neg B)$.
Durch die Sprache der Aussagenlogik können wir jede zusammengesetzte Aussage durch eine aussagenlogische Formel formalisieren, wie zu Beginn des Abschnitts angedeutet. Umgekehrt kommt man von einer aussagenlogischen Formel zu einer (zusammengesetzten) Aussage, indem man jede Aussagenvariable durch eine Aussage und $\neg$ durch „nicht“, $\wedge$ durch „und“, usw. ersetzt.
Die (formalsprachlichen) Junktoren entsprechen dabei wie folgt den (umgangssprachlichen) Konnektoren:

- Der Junktor $\neg$ entspricht „nicht“.
- Der Junktor $\wedge$ entspricht „und“.
- Der Junktor $\vee$ entspricht „oder“. ([6])
- Der Junktor $\Rightarrow$ entspricht „aus ... folgt ...“ oder „wenn ..., dann ...“ oder „nur dann ..., wenn ...“.
- Der Junktor $\Leftrightarrow$ entspricht „genau dann ..., wenn ...“, „... genau dann, wenn ...“, „... ist äquivalent zu ...“.

(1.4) Anwendungsbeispiel. Die Aussage „Es regnet.“ werde modelliert durch die Aussagenvariable A. Die Aussage „Es schneit.“ werde modelliert durch die Aussagenvariable B. Die Aussage „Die Straße ist nass.“ werde modelliert durch die Aussagenvariable C. Die Aussage „Es regnet oder es schneit.“ werde modelliert durch die Aussagenvariable D. Die Aussage „Die Straße ist trocken.“ werde modelliert durch die Aussagenvariable E. Die Aussage „Es gibt unendlich viele Primzahlen.“ werde modelliert durch die Aussagenvariable F. Die Aussage „$2 + 3 = 6$.“ werde modelliert durch die Aussagenvariable G. Die Aussage „Zu jeder reellen Zahl x gibt es eine reelle Zahl y mit $x + y = 0$.“ werde modelliert durch die Aussagenvariable H.

(a) Die aussagenlogische Formel $A \vee B \Rightarrow C$ ist ein Modell für die Aussage „Wenn es regnet oder schneit, dann ist die Straße nass.“.

(b) Die aussagenlogische Formel $D \Rightarrow C$ ist ein Modell für die Aussage „Wenn es regnet oder schneit, dann ist die Straße nass.“.

(c) Die aussagenlogische Formel $A \vee B \Rightarrow E$ ist ein Modell für die Aussage „Wenn es regnet oder schneit, dann ist die Straße trocken.“.

(d) Die aussagenlogische Formel $A \vee B \Rightarrow \neg C$ ist ein Modell für die Aussage „Wenn es regnet oder schneit, dann ist die Straße trocken.“.

(e) Die aussagenlogische Formel $A \Rightarrow F$ ist ein Modell für die Aussage „Wenn es regnet, dann gibt es unendlich viele Primzahlen.“.

(f) Die aussagenlogische Formel $\neg A \wedge \neg F$ ist ein Modell für die Aussage „Es regnet nicht und es gibt endlich viele Primzahlen.“.

(g) Die aussagenlogische Formel $C \wedge G$ ist ein Modell für die Aussage „Die Straße ist nass und $2 + 3 = 6$.“.

(h) Die aussagenlogische Formel $C \wedge \neg G$ ist ein Modell für die Aussage „Die Straße ist nass und es gilt nicht $2 + 3 = 6$.“.

(i) Die aussagenlogische Formel $C \wedge \neg G$ ist ein Modell für die Aussage „Die Straße ist nass und $2 + 3 \neq 6$.“.

(j) Die aussagenlogische Formel $H \Leftrightarrow C \wedge G$ ist ein Modell für die Aussage „Genau dann gibt es zu jeder reellen Zahl x eine reelle Zahl y mit $x + y = 0$, wenn die Straße nass ist und $2 + 3 = 6$ gilt.“.

[6] Genauer entspricht der Junktor $\vee$ einem *einschließenden oder*: Wenn wir sagen, dass eine Aussage oder eine andere gilt, so schließt dies die Möglichkeit ein, dass beide Aussagen gelten. Vgl. die Wahrheitstafel zu $A \vee B$ in Definition (1.7)(b).

(1.5) Definition (aussagenlogische Formel)**.** Es seien eine nicht-negative ganze Zahl n und eine aussagenlogische Formel F gegeben. Wir sagen, dass F eine *aussagenlogische Formel* in den Aussagenvariablen $A_1, \ldots, A_n$ ist, falls an keiner Stelle von F eine Aussagenvariable A_i für eine natürliche Zahl i mit $i > n$ vorkommt.

(1.6) Beispiel.

(a) Es ist $A \wedge B \Rightarrow C$ eine aussagenlogische Formel in den Aussagenvariablen A, B, C.

(b) Es ist $A \wedge B \Rightarrow D$ eine aussagenlogische Formel in den Aussagenvariablen A, B, C, D.

(c) Es ist $A \wedge B \Rightarrow C$ eine aussagenlogische Formel in den Aussagenvariablen A, B, C, D.

(d) Es ist $A \wedge B \Rightarrow D$ keine aussagenlogische Formel in den Aussagenvariablen A, B, C.

Beweis.

(a) In der aussagenlogischen Form $A \wedge B \Rightarrow C$ kommt an keiner Stelle eine Aussagenvariable ungleich A, B oder C vor. Somit ist $A \wedge B \Rightarrow C$ eine aussagenlogische Formel in den Aussagenvariablen A, B, C.

(b) In der aussagenlogischen Form $A \wedge B \Rightarrow D$ kommt an keiner Stelle eine Aussagenvariable ungleich A, B, C oder D vor. Somit ist $A \wedge B \Rightarrow D$ eine aussagenlogische Formel in den Aussagenvariablen A, B, C, D.

(c) In der aussagenlogischen Form $A \wedge B \Rightarrow C$ kommt an keiner Stelle eine Aussagenvariable ungleich A, B, C oder D vor. Somit ist $A \wedge B \Rightarrow C$ eine aussagenlogische Formel in den Aussagenvariablen A, B, C, D.

(d) In der aussagenlogischen Form $A \wedge B \Rightarrow D$ kommt die Aussagenvariable D und damit eine Aussagenvariable ungleich A, B oder C vor. Somit ist $A \wedge B \Rightarrow D$ keine aussagenlogische Formel in den Aussagenvariablen A, B, C. □

Wahrheitswerte aussagenlogischer Formeln

Oftmals sind wir lediglich an der logischen Struktur einer zusammengesetzten Aussage interessiert. Aus logischen Gesichtspunkten ist aber nicht der konkrete Inhalt einer zusammengesetzten Aussage von Belang, sondern nur deren Wahrheitswert. Dieser lässt sich allein aus der zugehörigen aussagenlogischen Formel gemäß folgenden Regeln ableiten, welche den aussagenlogischen Formeln eine Semantik geben.

(1.7) Definition (Wahrheitswert)**.** Es sei eine nicht-negative ganze Zahl n gegeben.

(a) Eine *Interpretation* (oder *Belegung*) der Aussagenvariablen $A_1, \ldots, A_n$ ist eine „eindeutige Zuordnung“ von entweder 0 (*falsch*) oder 1 (*wahr*) zur Aussagenvariable A_j für jede natürliche Zahl j mit $1 \leq j \leq n$. ([7])

Es sei eine Interpretation der Aussagenvariablen $A_1, \ldots, A_n$ gegeben. Für jede natürliche Zahl j mit $1 \leq j \leq n$ nennen wir den A_j zugeordneten Wert v_j den *Wahrheitswert* von A_j unter der Interpretation. Ferner notieren wir die gegebene Interpretation als $v_1 \ldots v_n$.

(b) Es sei eine Interpretation der Aussagenvariablen $A_1, \ldots, A_n$ gegeben. Der *Wahrheitswert* einer aussagenlogischen Formel in den Aussagenvariablen $A_1, \ldots, A_n$ ergebe sich rekursiv gemäß folgender *Wahrheitstafeln.*

0-*stellige Junktoren.*

0	1

1-*stellige Junktoren.*

F	$\neg F$
1	0
0	1

2-*stellige Junktoren.*

F	G	$F \wedge G$
1	1	1
1	0	0
0	1	0
0	0	0

F	G	$F \vee G$
1	1	1
1	0	1
0	1	1
0	0	0

F	G	$F \Rightarrow G$
1	1	1
1	0	0
0	1	1
0	0	1

F	G	$F \Leftrightarrow G$
1	1	1
1	0	0
0	1	0
0	0	1

[7] Im Fall $n = 0$ ordnet eine Interpretation also *keiner* Aussagenvariablen den Wert 0 oder 1 zu.

Es sei eine nicht-negative ganze Zahl n gegeben. Durch eine Interpretation der Aussagenvariablen $A_1, \ldots, A_n$ geben wir uns also Wahrheitswerte für die Aussagenvariablen $A_1, \ldots, A_n$ vor und erhalten einen eindeutigen Wahrheitswert für jede aussagenlogische Formel in den Aussagenvariablen $A_1, \ldots, A_n$. Dieser hängt lediglich von den Aussagenvariablen ab, welche in der aussagenlogischen Formel tatsächlich vorkommen.

(1.8) Beispiel.

(a) Es ist 101 eine Interpretation der Aussagenvariablen A, B, C.

(b) Der Wahrheitswert von $A \vee B \Rightarrow C$ unter der Interpretation 101 ist 1.

Beweis.

(b) Unter der Interpretation 101 ist der Wahrheitswert von A gleich 1 und der Wahrheitswert von B gleich 0, also ist der Wahrheitswert von $A \vee B$ gleich 1. Ferner ist der Wahrheitswert von C gleich 1 und damit auch der Wahrheitswert von $A \vee B \Rightarrow C$ gleich 1. □

(1.9) Beispiel. Die Interpretationen der Aussagenvariablen A, B, C sind gegeben durch

$$111, 110, 101, 100, 011, 010, 001, 000.$$

Der Wahrheitswert einer aussagenlogischen Formel bzgl. *aller* möglichen Interpretationen lässt sich am Besten kompakt mit Hilfe einer sogenannten *Wahrheitstafel* angeben. Eine solche Tabelle ist stets wie folgt aufgebaut. Die Spalten links des Doppelstrichs sind mit Aussagenvariablen beschriftet, wobei jede in der betrachteten aussagenlogischen Formel vorkommende Aussagenvariable auch eine solche Spalte beschriften muss. Die Spalte rechts vom Doppelstrich wird mit der betrachteten aussagenlogischen Formel beschriftet. In den Spalten links stehen die Werte der jeweiligen Interpretation (welche mit den Wahrheitswerten der Aussagenvariablen übereinstimmen), wobei alle möglichen Interpretationen durchlaufen werden. Rechts steht der sich jeweils resultierende Wahrheitswert der aussagenlogischen Formel.
Durch die Betrachtung mehrerer rechter Seiten lassen sich auch die Wahrheitswerte komplexerer aussagenlogischer Formeln schrittweise ermitteln, indem man zunächst Teilformeln betrachtet, siehe den Beweis zu Beispiel (1.10)(a). Sofern wir mehrere aussagenlogische Formeln simultan zu betrachten haben, welche von den gleichen Aussagenvariablen abhängen, fassen wir mehrere Wahrheitstafeln oftmals zu einer einzigen Wahrheitstafel zusammen. Hierbei schreiben wir die Aussagenvariablen links des Doppelstrichs nur einmal, während wir die betrachteten aussagenlogischen Formeln zusammen mit ihren jeweiligen Teilformeln durch Doppelstriche voneinander abgrenzen, siehe (den Beweis zu) Beispiel (1.10)(b).

(1.10) Beispiel.

(a) Die Wahrheitswerte der aussagenlogischen Formel $A \vee B \Rightarrow A \wedge C$ sind wie folgt gegeben.

A	B	C	$A \vee B \Rightarrow A \wedge C$
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	1

(b) Die Wahrheitswerte der aussagenlogischen Formeln $A \vee B \Leftrightarrow B$ und $A \wedge \neg B$ sind wie folgt gegeben.

A	B	$A \vee B \Leftrightarrow B$	$A \wedge \neg B$
1	1	1	0
1	0	0	1
0	1	1	0
0	0	1	0

Beweis.

(a) Wir erstellen eine Wahrheitstafel, in welcher wir die Wahrheitswerte der Teilformeln von $A \vee B \Rightarrow A \wedge C$ rekursiv berechnen:

A	B	C	$A \vee B$	$A \wedge C$	$A \vee B \Rightarrow A \wedge C$
1	1	1	1	1	1
1	1	0	1	0	0
1	0	1	1	1	1
1	0	0	1	0	0
0	1	1	1	0	0
0	1	0	1	0	0
0	0	1	0	0	1
0	0	0	0	0	1

(b) Wir erstellen eine Wahrheitstafel, in welcher wir die Wahrheitswerte der Teilformeln von $A \vee B \Leftrightarrow B$ und $A \wedge \neg B$ jeweils rekursiv berechnen:

A	B	$A \vee B$	$A \vee B \Leftrightarrow B$	$\neg B$	$A \wedge \neg B$
1	1	1	1	0	0
1	0	1	0	1	1
0	1	1	1	0	0
0	0	0	1	1	0

□

Tautologien und Kontradiktionen

Für aussagenlogische Formeln, welche unabhängig von der Interpretation stets denselben Wahrheitswert haben, führen wir folgende Bezeichnungen ein:

(1.11) Definition (Tautologie, Kontradiktion)**.**

(a) Eine aussagenlogische Formel heißt *allgemeingültig* (oder eine *Tautologie*), wenn sie unter jeder Interpretation den Wahrheitswert 1 hat.

(b) Eine aussagenlogische Formel heißt *unerfüllbar* (oder eine *Kontradiktion* oder ein *Widerspruch*), wenn sie unter jeder Interpretation den Wahrheitswert 0 hat.

Eine aussagenlogische Formel ist also genau dann eine Tautologie, wenn jede Ersetzung der Aussagenvariablen durch Aussagen stets eine wahre Aussage liefert, und genau dann eine Kontradiktion, wenn jede Ersetzung der Aussagenvariablen durch Aussagen eine falsche Aussage ergibt.

(1.12) Beispiel (tertium non datur, principium contradictionis)**.**

(a) Die aussagenlogische Formel $A \vee \neg A$ ist eine Tautologie.

(b) Die aussagenlogische Formel $A \wedge \neg A$ ist eine Kontradiktion.

Beweis.

(a) Wir erstellen eine Wahrheitstafel:

A	$\neg A$	$A \vee \neg A$
1	0	1
0	1	1

Da der Wahrheitswert von $A \vee \neg A$ unter jeder Interpretation gleich 1 ist, bildet diese aussagenlogische Formel eine Tautologie.

(b) Wir erstellen eine Wahrheitstafel:

A	$\neg A$	$A \wedge \neg A$
1	0	0
0	1	0

Da der Wahrheitswert von $A \wedge \neg A$ unter jeder Interpretation gleich 0 ist, bildet diese aussagenlogische Formel eine Kontradiktion. □

(1.13) Bemerkung. Es sei eine aussagenlogische Formel F gegeben. Genau dann ist F eine Tautologie, wenn $\neg F$ eine Kontradiktion ist.

Beweis. Genau dann ist die aussagenlogische Formel F eine Tautologie, wenn sie unter jeder Interpretation den Wahrheitswert 1 hat. Dies ist aber äquivalent zur Tatsache, dass $\neg F$ unter jeder Interpretation den Wahrheitswert 0 hat, also dass $\neg F$ eine Kontradiktion ist. □

Logische Äquivalenz aussagenlogischer Formeln

Im Folgenden werden wir oftmals eine zusammengesetzte Aussage in eine andere umformen wollen ohne hierbei den Wahrheitswert zu verändern. Hierzu werden wir uns nun die logischen Grundlagen erarbeiten. Eine solche Umformung können wir nämlich auch ohne Kenntnis des Wahrheitswerts machen, sofern wir die zusammengesetzte Aussage durch eine zusammengesetzte Aussage ersetzen, welche bei *jeder* möglichen Kombination von Wahrheitswerten der Einzelaussagen denselben Wahrheitswert für die umformulierte zusammengesetzte Aussage liefert wie für die ursprüngliche zusammengesetzte Aussage.

(1.14) Definition (logische Äquivalenz)**.** Es seien aussagenlogische Formeln F und G gegeben. Wir sagen, dass F *logisch äquivalent* (oder *semantisch äquivalent*) zu G ist, geschrieben $F \equiv G$, falls die Wahrheitswerte von F und G unter jeder Interpretation gleich sind.

(1.15) Beispiel. Es gilt $A \Rightarrow B \equiv \neg A \vee B$.

Beweis. Wir erstellen eine Wahrheitstafel:

A	B	$A \Rightarrow B$	$\neg A$	$\neg A \vee B$
1	1	1	0	1
1	0	0	0	0
0	1	1	1	1
0	0	1	1	1

Da die Wahrheitswerte von $A \Rightarrow B$ und $\neg A \vee B$ unter jeder Interpretation übereinstimmen, gilt $A \Rightarrow B \equiv \neg A \vee B$. □

Wir haben den Begriff der logischen Äquivalenz von aussagenlogischen Formeln und den Begriff der Äquivalenz als Junktor. Diese sprachliche Übereinstimmung ist nicht zufällig gewählt, wie folgendes Lemma zeigt:

(1.16) Proposition. Es seien aussagenlogische Formeln F und G gegeben. Genau dann gilt $F \equiv G$, wenn $F \Leftrightarrow G$ eine Tautologie ist.

Beweis. Genau dann gilt $F \equiv G$, wenn F und G unter jeder Interpretation den gleichen Wahrheitswert haben. Dies ist jedoch dazu äquivalent, dass der Wahrheitswert von $F \Leftrightarrow G$ unter jeder Interpretation gleich 1 ist, also dazu, dass $F \Leftrightarrow G$ eine Tautologie ist. □

(1.17) Bemerkung. Es sei eine aussagenlogische Formel F gegeben.

(a) Genau dann ist F eine Tautologie, wenn $F \equiv 1$ ist.

(b) Genau dann ist F eine Kontradiktion, wenn $F \equiv 0$ ist.

Beweis.

(a) Genau dann ist die aussagenlogische Formel F eine Tautologie, wenn sie unter jeder Interpretation den Wahrheitswert 1 hat. Da 1 unter jeder Interpretation den Wahrheitswert 1 hat, ist dies also dazu äquivalent, dass die Wahrheitswerte von F und 1 für jede Interpretation gleich sind, also dazu, dass $F \equiv 1$ ist.

(b) Dies lässt sich dual zu (a) beweisen. □

Wir halten einige oft benutzte logische Äquivalenzen fest:

(1.18) Beispiel.

(a) (i) *Assoziativität der Konjunktion.* Es gilt $A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$.

(ii) *Assoziativität der Disjunktion.* Es gilt $A \vee (B \vee C) \equiv (A \vee B) \vee C$.

(b) (i) *Neutrales Element der Konjunktion.* Es gilt $A \wedge 1 \equiv A$.
(ii) *Neutrales Element der Disjunktion.* Es gilt $A \vee 0 \equiv A$.

(c) (i) *Kommutativität der Konjunktion.* Es gilt $A \wedge B \equiv B \wedge A$.
(ii) *Kommutativität der Disjunktion.* Es gilt $A \vee B \equiv B \vee A$.

(d) (i) *Idempotenz der Konjunktion.* Es gilt $A \wedge A \equiv A$.
(ii) *Idempotenz der Disjunktion.* Es gilt $A \vee A \equiv A$.

(e) (i) *Komplemente der Konjunktion.* Es gilt $A \wedge \neg A \equiv 0$.
(ii) *Komplemente der Disjunktion.* Es gilt $A \vee \neg A \equiv 1$.

(f) (i) *Distributivität.* Es gilt $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$.
(ii) *Distributivität.* Es gilt $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$.

(g) (i) *Absorption.* Es gilt $A \wedge (A \vee B) \equiv A$.
(ii) *Absorption.* Es gilt $A \vee (A \wedge B) \equiv A$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(1.19) Konvention. Wegen der Assoziativität der Konjunktion und der Disjunktion kommt es bei iterierter Bildung bis auf logische Äquivalenz nicht auf die Klammerung an. Im Regelfall lassen wir daher die Klammern im Folgenden weg und schreiben $A \wedge B \wedge C$ statt $A \wedge (B \wedge C)$, usw.

(1.20) Beispiel. Es gilt $\neg(\neg A) \equiv A$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(1.21) Beispiel (De Morgansche Gesetze)**.**

(a) Es gilt $\neg(A \vee B) \equiv \neg A \wedge \neg B$.

(b) Es gilt $\neg(A \wedge B) \equiv \neg A \vee \neg B$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

Semantische Implikation

Die logische Äquivalenz von aussagenlogischen Formeln F und G ist äquivalent zur Tatsache, dass $F \Leftrightarrow G$ eine Tautologie ist, siehe Proposition (1.16). Wir können nun einen analogen Begriff für die Implikation definieren, welcher in Beweisen beim Schließen von gegebenen Aussagen auf neue Aussagen benutzt wird.

(1.22) Definition (semantische Implikation)**.** Es seien aussagenlogische Formeln F und G gegeben. Wir sagen, dass G *semantisch* durch F *impliziert* wird (oder dass G *semantisch* aus F *folgt*), geschrieben $F \models G$, falls unter jeder Interpretation, unter der F den Wahrheitswert 1 annimmt, auch G den Wahrheitswert 1 annimmt.

(1.23) Beispiel. Es gilt $A \wedge B \models A \vee C$.

Beweis. Wir erstellen eine Wahrheitstafel:

A	B	C	$A \wedge B$	$A \vee C$
1	1	1	1	1
1	1	0	1	1
1	0	1	0	1
1	0	0	0	1
0	1	1	0	1
0	1	0	0	0
0	0	1	0	1
0	0	0	0	0

Da unter jeder Interpretation, unter der $A \wedge B$ den Wahrheitswert 1 annimmt, auch $A \vee C$ den Wahrheitswert 1 annimmt, gilt $A \wedge B \models A \vee C$. □

(1.24) Proposition. Es seien aussagenlogische Formeln F und G gegeben. Genau dann gilt $F \models G$, wenn $F \Rightarrow G$ eine Tautologie ist.

Beweis. Zunächst gelte $F \models G$, d.h. unter jeder Interpretation, unter der F den Wahrheitswert 1 annimmt, nehme auch G den Wahrheitswert 1 an. Ferner sei eine beliebige Interpretation gegeben. Wenn F unter dieser den Wahrheitswert 1 annimmt, so nach unserer Annahme auch G und folglich auch $F \Rightarrow G$. Wenn hingegen F den Wahrheitswert 0 annimmt, so hat $F \Rightarrow G$ ebenfalls den Wahrheitswert 1, unabhängig vom Wahrheitswert von G. Also hat $F \Rightarrow G$ in jedem Fall den Wahrheitswert 1, d.h. $F \Rightarrow G$ ist eine Tautologie.
Nun sei umgekehrt $F \Rightarrow G$ eine Tautologie, d.h. unter jeder Interpretation habe $F \Rightarrow G$ den Wahrheitswert 1. Unter jeder Interpretation, unter der F den Wahrheitswert 1 annimmt, nimmt G dann nicht den Wahrheitswert 0 an, muss also notwendigerweise ebenfalls den Wahrheitswert 1 annehmen, d.h. es gilt $F \models G$. □

(1.25) Proposition. Es seien aussagenlogische Formeln F und G gegeben. Genau dann gilt $F \equiv G$, wenn $F \models G$ und $G \models F$ gilt.

Beweis. Zunächst gelte $F \equiv G$, d.h. die Wahrheitswerte von F und G seien unter jeder Interpretation gleich. Dann nimmt G unter jeder Interpretation, unter der F den Wahrheitswert 1 annimmt, ebenfalls den Wert 1 an, d.h. es gilt $F \models G$, und umgekehrt nimmt F unter jeder Interpretation, unter der G den Wahrheitswert 1 annimmt, ebenfalls den Wert 1 an, d.h. es gilt $G \models F$.
Nun gelte umgekehrt $F \models G$ und $G \models F$. Um zu zeigen, dass $F \equiv G$ gilt, sei eine beliebige Interpretation gegeben. Wenn F unter dieser den Wahrheitswert 1 annimmt, so wegen $F \models G$ auch G. Nimmt hingegen F unter dieser den Wahrheitswert 0 an, so nimmt G wegen $G \models F$ nicht den Wahrheitswert 1 an, also den Wahrheitswert 0. Also haben F und G unter jeder Interpretation denselben Wahrheitswert, d.h. es gilt $F \equiv G$.
□

Direkter Beweis

Im Folgenden werden wir einige Strategien betrachten, um eine Aussage der Form $A \Rightarrow B$ zu beweisen. (De facto lässt sich jede Aussage der Form C in eine Aussage dieser Form umformulieren, es ist C logisch äquivalent zu $1 \Rightarrow C$.)
Wir beginnen mit der Strategie des *direkten Beweises*. Um zu zeigen, dass eine gegebene Aussage der Form $A \Rightarrow B$ gilt, nehmen wir oft an, dass die Aussage der Form A gilt, und zeigen unter dieser Annahme, dass auch die Aussage der Form B gilt. Dieses Vorgehen lässt sich anhand der Wahrheitstafel der Implikation begründen:

A	B	$A \Rightarrow B$
1	1	1
1	0	0
0	1	1
0	0	1

Ist die Aussage der Form A falsch, so ist die Aussage der Form $A \Rightarrow B$ unabhängig vom Wahrheitswert der Aussage der Form B wahr. Können wir also unter der Annahme, dass die Aussage der Form A wahr ist, zeigen, dass auch die Aussage der Form B wahr ist, so wissen wir, dass unabhängig vom Wahrheitswert der Aussage der Form A in jedem Fall die Aussage der Form $A \Rightarrow B$ wahr ist.
Wollen wir umgekehrt die Aussage der Form $A \Rightarrow B$ widerlegen, d.h. wollen wir zeigen, dass diese Aussage falsch ist, so müssen wir unter der Annahme, dass die Aussage der Form A gilt, zeigen, dass die Aussage der Form B falsch ist.
Der Beweis einer Aussage der Form $A \Rightarrow B$ geschieht durch eine endliche Folge von logischen Schlussfolgerungen (etwa durch Anwenden von Definitionen oder bereits bewiesenen Aussagen, siehe Beispiel (1.27)). Hierbei entspricht die Aussage der Form A der Prämisse der ersten Implikation und die Aussage der Form B der Konklusion der letzten Implikation in dieser Folge. Wir rechtfertigen das „Zusammensetzen logischer Schlussfolgerungen“ wie folgt.

(1.26) Beispiel. Es gilt $(A \Rightarrow B) \wedge (B \Rightarrow C) \models (A \Rightarrow C)$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

Als nächstes betrachten wir einige Typen logischer Schlussfolgerungen. Wir beginnen mit dem Anwenden bereits bewiesener Aussagen der Form einer Implikation:

(1.27) Beispiel (modus ponens)**.** Es gilt $A \wedge (A \Rightarrow B) \models B$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

Es sei eine Aussage der Form $A \Rightarrow B$ bereits bewiesen, d.h. deren Gültigkeit sei bereits gezeigt. Aus der Gültigkeit der Aussage der Form A folgt dann die Gültigkeit der Aussage der Form $A \wedge (A \Rightarrow B)$. Da aber B nach dem modus ponens (1.27) semantisch aus $A \wedge (A \Rightarrow B)$ folgt, impliziert die Gültigkeit der Aussage der Form $A \wedge (A \Rightarrow B)$ bereits die Gültigkeit der Aussage der Form B. Somit können wir also aus der Gültigkeit der Aussage A die Gültigkeit der Aussage B schließen.
Dies folgt auch direkt aus der Wahrheitstafel der Implikation, denn die Ungültigkeit der Aussage der Form B hätte die Ungültigkeit der Aussage der Form $A \Rightarrow B$ zur Folge. Letztere haben wir durch den Beweis der Aussage der Form $A \Rightarrow B$ aber bereits widerlegt.
Die nächste in der Praxis vorkommende logische Schlussfolgerung ist das Spezialisieren: Wenn eine Aussage der Form $A \wedge B$ gilt, so folgt hieraus insbesondere die Gültigkeit der Aussage der Form A.
Wenn wir hingegen wissen, dass eine Aussage der Form A gilt, so wissen wir auch, dass für jede Aussage der Form B die Aussage der Form $A \vee B$ gilt.

(1.28) Beispiel.

(a) Es gilt $A \wedge B \models A$.

(b) Es gilt $A \models A \vee B$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

Alternativer Beweis von Beispiel (1.23). Nach Beispiel (1.28)(a) gilt $A \wedge B \models A$ und nach (einem Analogon zu) Beispiel (1.28)(b) gilt $A \models A \vee C$. Folglich gilt auch $A \wedge B \models A \vee C$. □

Um eine Aussage der Form $A \Rightarrow B$ zu beweisen, kommt es in der Praxis oft vor, dass wir mehrere bereits bewiesene Aussagen anwenden müssen. Hierzu ist es oftmals nötig, die Gültigkeit der Aussage der Form A für mehr als einmal anzuwenden. In einer Folge von Implikationen können wir aber zunächst nicht ohne weiteres davon ausgehen, dass wir die Aussage der Form A in einem Zwischenschritt noch zur Verfügung haben. Dass ein „Mitschleppen“ bereits angewandter Aussagen trotzdem möglich ist, wird wie folgt begründet:

(1.29) Beispiel. Es gilt $A \Rightarrow B \equiv A \Rightarrow A \wedge B$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

Anhand eines Beispiels wollen wir nun einen direkten Beweis einer Aussage der Form $A \Rightarrow B$ durchführen. Um dies zu machen, werden wir annehmen, dass die Aussage der Form A gilt und werden dann zeigen, dass aus dieser Annahme die Gültigkeit der Aussage der Form B folgt.
Bevor wir uns dem Beispiel widmen, merken wir an, dass der Beweis jeder Aussage auf Definitionen oder bereits bewiesene Aussagen zurückgeführt wird. Da das Beispiel eine Aussage über gerade Zahlen macht, erinnern wir daher an deren Definition: Eine ganze Zahl n heißt *gerade*, falls es eine ganze Zahl k mit $n = 2k$ gibt.

(1.30) Anwendungsbeispiel. Für jede gerade ganze Zahl n ist auch n^2 gerade.

Beweis. Es sei eine ganze Zahl n gegeben. Wir zeigen: Wenn n gerade ist, dann ist auch n^2 gerade.
Wenn n gerade ist, dann gibt es eine ganze Zahl k mit $n = 2k$. Wenn es eine ganze Zahl k mit $n = 2k$ gibt, dann gibt es eine ganze Zahl k mit $n^2 = (2k)^2$. Wenn es eine ganze Zahl k mit $n^2 = (2k)^2$ gibt, dann gibt es eine ganze Zahl k mit $n^2 = 4k^2$. Wenn es eine ganze Zahl k mit $n^2 = 4k^2$ gibt, dann gibt es eine ganze Zahl k mit $n^2 = 2(2k^2)$. Wenn es eine ganze Zahl k mit $n^2 = 2(2k^2)$ gibt, dann ist n^2 gerade.
Insgesamt gilt ([8]): Wenn n gerade ist, dann ist n^2 gerade. □

Im Beweis zu Anwendungsbeispiel (1.30) ist die logische Struktur sehr gut ersichtlich. Dies führt leider zu einem länglichen, schwer zu erfassenden Text. Üblicherweise würde man den Beweis wie folgt verkürzen:

[8] In diesem Schritt benutzen wir die uns verinnerlichte logische Tatsache des „Zusammensetzens logischer Schlussfolgerungen“, deren formale Entsprechung sich in Beispiel (1.26) findet.

Beweis. Es sei eine gerade ganze Zahl n gegeben. Dann gibt es eine ganze Zahl k mit $n = 2k$. Es folgt

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2).$$

Somit ist auch n^2 gerade. □

Der zweite gegebene Beweis von (1.30) unterscheidet sich nur unwesentlich vom ersten, da die zu Grunde liegende logische Struktur die gleiche ist – er wird lediglich durch sprachliche Konventionen lesbarer gestaltet.

Kontraposition

Als nächstes betrachten wir das Beweisverfahren des *Umkehrschlusses*, auch *Kontraposition* genannt. Anstatt eine Aussage der Form $A \Rightarrow B$ zu beweisen, können wir auch die Aussage der Form $\neg B \Rightarrow \neg A$ zeigen:

(1.31) Beispiel (Kontraposition)**.** Es gilt $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

Wir verdeutlichen die Strategie der Kontraposition wieder an einem Beispiel.

(1.32) Anwendungsbeispiel. Für jede ganze Zahl n gilt: Wenn n^2 gerade ist, dann ist auch n gerade.

Beweis. Es sei eine ganze Zahl n gegeben. Wir zeigen: Wenn n ungerade ist, dann ist auch n^2 ungerade.
Es sei also n ungerade. Dann gibt es eine ganze Zahl k mit $n = 2k + 1$. Es folgt

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Somit ist auch n^2 ungerade.
Im Umkehrschluss folgt: Wenn n^2 gerade ist, dann ist auch n gerade. □

Indirekter Beweis

Eine weitere Beweisstrategie ist der sogenannte *indirekte Beweis*. Anstatt der Gültigkeit einer Aussage der Form $A \Rightarrow B$ beweist man hierbei die Ungültigkeit der Aussage der Form $A \wedge \neg B$, was der Gültigkeit der Aussage der Form $\neg(A \wedge \neg B)$ entspricht:

(1.33) Beispiel (indirekter Beweis)**.** Es gilt $A \Rightarrow B \equiv \neg(A \wedge \neg B)$.

Beweis. Nach Beispiel (1.15), Beispiel (1.20) und dem De Morganschen Gesetz (1.21)(b) gilt

$$A \Rightarrow B \equiv \neg A \vee B \equiv \neg A \vee \neg(\neg B) \equiv \neg(A \wedge \neg B).$$ □

Auch das Prinzip des indirekten Beweises verdeutlichen wir wieder durch ein Beispiel.

(1.34) Anwendungsbeispiel. Jede reelle Zahl x mit $x^3 + x = 1$ ist irrational.

Beweis. Es sei eine reelle Zahl x gegeben. Wir zeigen: Wenn $x^3 + x = 1$ ist, dann ist x irrational.
Angenommen, es gilt $x^3 + x = 1$ und x ist rational. Dann gibt es teilerfremde ([9]) ganze Zahlen a und b mit $x = \frac{a}{b}$.
Es folgt

$$1 = x^3 + x = (\frac{a}{b})^3 + \frac{a}{b} = \frac{a^3}{b^3} + \frac{a}{b}$$

und damit $b^3 = a^3 + ab^2$.
Wäre nun b ungerade, so wäre einerseits b^3 ungerade ([10]) und andererseits $a^3 + ab^2$ gerade (unabhängig davon, ob a gerade oder ungerade ist). Da $b^3 = a^3 + ab^2$ nicht gleichzeitig ungerade und gerade sein kann, ist somit b gerade. Wäre nun weiter a ungerade, so wäre b^3 gerade und $a^3 + ab^2$ ungerade. Da $b^3 = a^3 + ab^2$ nicht gleichzeitig gerade und ungerade sein kann, ist somit auch a gerade. Damit sind aber a und b beide gerade, also durch 2 teilbar im Widerspruch zu ihrer Teilerfremdheit.
Folglich war unsere Annahme, dass $x^3 + x = 1$ und x rational ist, falsch. Wenn also $x^3 + x = 1$ gilt, so muss notwendigerweise x irrational sein. □

[9] Die Teilerfremdheit bedeutet, dass der Bruch gekürzt ist.
[10] An dieser Stelle und weiteren Stellen im Beweis benutzen wir implizit zu Anwendungsbeispiel (1.30) analoge Aussagen.

Die Gültigkeit einer Aussage der Form A können wir ebenfalls indirekt zeigen. Hierzu zeigen wir die Gültigkeit der Aussage der Form $\neg A \Rightarrow 0$, d.h. wir führen die Annahme, dass die Aussage der Form $\neg A$ richtig ist, also dass die Aussage der Form A falsch ist, zu einem Widerspruch. Hierbei wird die Aussage der Form 0, also eine falsche Aussage, in der Regel durch den Widerspruch $B \wedge \neg B$ für eine beliebige Aussage der Form B gezeigt, d.h. man zeigt die logisch äquivalente Aussage der Form $\neg A \Rightarrow B \wedge \neg B$, vgl. Beispiel (1.18)(e)(i).

(1.35) Beispiel. Es gilt $A \equiv \neg A \Rightarrow 0$.

Beweis. Nach Beispiel (1.15), Beispiel (1.20) und Beispiel (1.18)(b)(ii) gilt

$$\neg A \Rightarrow 0 \equiv \neg(\neg A) \vee 0 \equiv A \vee 0 \equiv A.$$ □

Beweis einer Äquivalenz

Um eine Äquivalenz zweier Aussagen, also eine Aussage der Form $A \Leftrightarrow B$, zu zeigen, zerlegen wir diese oft in zwei Implikationen:

(1.36) Beispiel. Es gilt $A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(1.37) Anwendungsbeispiel. Für jede ganze Zahl n gilt: Genau dann ist n^2 gerade, wenn n gerade ist.

Beweis. Es sei eine ganze Zahl n gegeben. Wenn n^2 gerade ist, dann ist auch n gerade nach Anwendungsbeispiel (1.32). Umgekehrt, wenn n gerade ist, dann ist auch n^2 gerade nach Anwendungsbeispiel (1.30). Insgesamt ist n^2 genau dann gerade, wenn n gerade ist. □

Disjunktive und konjunktive Normalform

Als nächstes wollen wir zeigen, dass jede potentielle Wahrheitstafel im folgenden Sinn als Wahrheitstafel einer aussagenlogischen Formel vorkommt.

(1.38) Definition (potentielle Wahrheitstafel)**.** Es sei eine nicht-negative ganze Zahl n gegeben. Eine *potentielle Wahrheitstafel* für die Aussagenvariablen $A_1, \ldots, A_n$ ist eine „eindeutige Zuordnung“ von entweder 0 oder 1 zu jeder Interpretation der Aussagenvariablen $A_1, \ldots, A_n$.

Wir können potentielle Wahrheitstafeln wie Wahrheitstafeln von aussagenlogischen Formeln verbildlichen; der einzige Unterschied ist das Fehlen einer aussagenlogischen Formel, zu denen die Wahrheitswerte auf der rechten Seite gehören:

(1.39) Beispiel. Es ist

A	B	C	
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	1

eine potentielle Wahrheitstafel für die Aussagenvariablen A, B, C.

Wir werden sehen, dass wir potentielle Wahrheitstafeln sogar durch aussagenlogische Formeln in einer speziellen Normalform realisieren können, genau genommen sogar auf zwei verschiedene zueinander duale Weisen.
Zunächst definieren wir die auftauchenden Normalformen:

(1.40) Definition (disjunktive Normalform, konjunktive Normalform)**.** Es seien eine nicht-negative ganze Zahl n und eine aussagenlogische Formel F in den Aussagenvariablen $A_1, \ldots, A_n$ gegeben.

(a) Wir sagen, dass F in (*kanonischer*) *disjunktiver Normalform* bzgl. $A_1, \ldots, A_n$ ist, wenn es eine nicht-negative ganze Zahl k und verschiedene ([11]) aussagenlogische Formeln $F_1, \ldots, F_k$ derart gibt, dass

$$F = F_1 \vee \ldots \vee F_k,$$

und so, dass für alle natürlichen Zahlen i mit $1 \leq i \leq n$ stets

$$F_i = X_{i,1} \wedge \ldots \wedge X_{i,n}$$

gilt, wobei $X_{i,j} = A_j$ oder $X_{i,j} = \neg A_j$ für alle natürlichen Zahlen j mit $1 \leq j \leq n$. ([12])

(b) Wir sagen, dass F in (*kanonischer*) *konjunktiver Normalform* bzgl. $A_1, \ldots, A_n$ ist, wenn es eine nicht-negative ganze Zahl k und verschiedene aussagenlogische Formeln $F_1, \ldots, F_k$ derart gibt, dass

$$F = F_1 \wedge \ldots \wedge F_k,$$

und so, dass für alle natürlichen Zahlen i mit $1 \leq i \leq n$ stets

$$F_i = X_{i,1} \vee \ldots \vee X_{i,n}$$

gilt, wobei $X_{i,j} = A_j$ oder $X_{i,j} = \neg A_j$ für alle natürlichen Zahlen j mit $1 \leq j \leq n$. ([13])

(1.41) Beispiel.

(a) Die aussagenlogische Formel

$$A \wedge B \vee A \wedge \neg B$$

ist in disjunktiver Normalform.

(b) Die aussagenlogische Formel

$$(A \vee B \vee \neg C) \wedge (A \vee \neg B \vee C) \wedge (\neg A \vee B \vee C) \wedge (\neg A \vee \neg B \vee \neg C)$$

ist in konjunktiver Normalform.

Wir leiten nun eine Methode her, mit der sich zu einer gegebenen potentiellen Wahrheitstafel eine aussagenlogische Formel in disjunktiver Normalform konstruieren lässt, welche die gegebene potentielle Wahrheitstafel als Wahrheitstafel hat. Die Methode beruht auf der Beobachtung, dass sich die Wahrheitstafel einer aussagenlogischen Formel in disjunktiver Normalform sehr leicht aus der Gestalt der aussagenlogischen Formel bestimmen lässt. Beispielsweise nimmt die aussagenlogische Formel $A \wedge B \vee A \wedge \neg B$ aus Beispiel (1.41)(a) genau dann den Wahrheitswert 1 an, wenn $A \wedge B$ den Wahrheitswert 1 oder $A \wedge \neg B$ den Wahrheitswert 1 annimmt. Ersteres ist genau dann der Fall, wenn A den Wahrheitswert 1 annimmt und B den Wahrheitswert 1 annimmt, und zweiteres ist genau dann der Fall, wenn A den Wahrheitswert 1 und B nicht den Wahrheitswert 0 annimmt.
Wir werden gleich zum ersten Mal das Symbol „:=“ sehen, welches bei Definitionen von „mathematischen Objekten“ verwendet wird. Wenn ein *gegebener Ausdruck* y als x *definiert* werden soll, so schreibt man $x := y$; man gibt also dem „bekannten“ Ausdruck y den neuen Namen x.

(1.42) Definition (zu einer Interpretation zugehöriges Disjunkt/Konjunkt)**.** Es seien eine nicht-negative ganze Zahl n und eine Interpretation $v_1 \ldots v_n$ der Aussagenvariablen $A_1, \ldots, A_n$ gegeben.

(a) Für jede natürliche Zahl j mit $1 \leq j \leq n$ setzen wir

$$X_j := \begin{cases} A_j, & \text{falls } v_j = 1, \\ \neg A_j, & \text{falls } v_j = 0. \end{cases}$$

Die aussagenlogische Formel

$$\mathrm{Dis}(v_1 \ldots v_n) := X_1 \wedge \ldots \wedge X_n$$

heißt das zu $v_1 \ldots v_n$ gehörige *Disjunkt*.

[11] „Objekte“ $x_1, \ldots, x_k$ werden *verschieden* genannt, falls für alle natürlichen Zahlen i und j mit $1 \leq i \leq n$ und $1 \leq j \leq n$ und $i \neq j$ stets $x_i \neq x_j$ gilt, oder äquivalent ausgedrückt, falls für alle natürlichen Zahlen i und j mit $1 \leq i \leq n$ und $1 \leq j \leq n$ aus $x_i = x_j$ bereits $i = j$ folgt.

[12] Im Fall $k = 0$ ist F eine Disjunktion über 0 Disjunkte, eine sogenannte *leere Disjunktion*, was per Konvention der Booleschen Konstanten 0 entspricht.

[13] Im Fall $k = 0$ ist F eine Konjunktion über 0 Konjunkte, eine sogenannte *leere Konjunktion*, was per Konvention der Booleschen Konstanten 1 entspricht.

(b) Für jede natürliche Zahl j mit $1 \leq j \leq n$ setzen wir

$$X_j := \begin{cases} \neg A_j, & \text{falls } v_j = 1, \\ A_j, & \text{falls } v_j = 0. \end{cases}$$

Die aussagenlogische Formel

$$\mathrm{Con}(v_1 \dots v_n) := X_1 \vee \dots \vee X_n$$

heißt das zu $v_1 \dots v_n$ gehörige *Konjunkt*.

(1.43) Beispiel.

(a) Das zur Interpretation 1011 der Aussagenvariablen A, B, C, D gehörige Disjunkt ist

$$\mathrm{Dis}(1011) = A \wedge \neg B \wedge C \wedge D.$$

(b) Das zur Interpretation 1011 der Aussagenvariablen A, B, C, D gehörige Konjunkt ist

$$\mathrm{Con}(1011) = \neg A \vee B \vee \neg C \vee \neg D.$$

(1.44) Bemerkung. Es seien eine nicht-negative ganze Zahl n und Interpretationen $v_1 \dots v_n$ und $w_1 \dots w_n$ der Aussagenvariablen $A_1, \dots, A_n$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Der Wahrheitswert von $\mathrm{Dis}(w_1 \dots w_n)$ für die Interpretation $v_1 \dots v_n$ ist gleich 1.

(b) Der Wahrheitswert von $\mathrm{Con}(w_1 \dots w_n)$ für die Interpretation $v_1 \dots v_n$ ist gleich 0.

(c) Für jede natürliche Zahl j mit $1 \leq j \leq n$ ist $w_j = v_j$.

Beweis. Für jede natürliche Zahl j mit $1 \leq j \leq n$ setzen wir

$$X_j := \begin{cases} A_j, & \text{falls } w_j = 1, \\ \neg A_j, & \text{falls } w_j = 0, \end{cases}$$

so dass $\mathrm{Dis}(w_1 \dots w_n) = X_1 \wedge \dots \wedge X_n$ gilt. Nun ist aber genau dann der Wahrheitswert von $\mathrm{Dis}(w_1 \dots w_n)$ unter der Interpretation $v_1 \dots v_n$ gleich 1, wenn der Wahrheitswert von X_j für jede natürliche Zahl j mit $1 \leq j \leq n$ gleich 1 ist, also genau dann, wenn $w_j = v_j$ für jede natürliche Zahl j mit $1 \leq j \leq n$ gilt. Dies zeigt die Äquivalenz von Bedingung (a) und Bedingung (c).
Die Äquivalenz von Bedingung (b) und Bedingung (c) lässt sich dual zeigen.
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

Die nachfolgende Proposition gibt an, wie wir zu den Werten einer potentiellen Wahrheitstafel eine aussagenlogische Formel in disjunktiver bzw. konjunktiver Normalform erstellen können.

(1.45) Proposition. Es seien eine nicht-negative ganze Zahl n und eine potentielle Wahrheitstafel für die Aussagenvariablen $A_1, \dots, A_n$ gegeben.

(a) Es sei F eine Disjunktion (in beliebiger Reihenfolge) über all diejenigen Disjunkte, welche zu Interpretationen der Aussagenvariablen $A_1, \dots, A_n$ gehören, die in der potentiellen Wahrheitstafel den Wahrheitswert 1 zugewiesen bekommen. Dann ist F die bis auf der Reihenfolge der Disjunkte eindeutige aussagenlogische Formel in disjunktiver Normalform bzgl. $A_1, \dots, A_n$, welche die Wahrheitswerte der gegebenen potentiellen Wahrheitstafel annimmt.

(b) Es sei F eine Konjunktion (in beliebiger Reihenfolge) über all diejenigen Konjunkte, welche zu Interpretationen der Aussagenvariablen $A_1, \dots, A_n$ gehören, die in der potentiellen Wahrheitstafel den Wahrheitswert 0 zugewiesen bekommen. Dann ist F die bis auf der Reihenfolge der Konjunkte eindeutige aussagenlogische Formel in konjunktiver Normalform bzgl. $A_1, \dots, A_n$, welche die Wahrheitswerte der gegebenen potentiellen Wahrheitstafel annimmt.

Beweis.

(a) Um zu zeigen, dass F die Wahrheitswerte der gegebenen potentiellen Wahrheitstafel annimmt, sei eine beliebige Interpretation $v_1 \dots v_n$ gegeben. Zunächst sei der $v_1 \dots v_n$ zugewiesene Wahrheitswert in der potentiellen Wahrheitstafel gleich 1, so dass $\mathrm{Dis}(v_1 \dots v_n)$ ein Disjunkt von F ist. Da der Wahrheitswert von $\mathrm{Dis}(v_1 \dots v_n)$ unter der Interpretation $v_1 \dots v_n$ nach Bemerkung (1.44) gleich 1 ist, gilt dies auch für die Disjunktion F. Im Folgenden sei also der $v_1 \dots v_n$ zugewiesene Wahrheitswert in der potentiellen Wahrheitstafel gleich 0. Dann ist $\mathrm{Dis}(v_1 \dots v_n)$ kein Disjunkt von F. Folglich ist jedes Disjunkt von F gleich $\mathrm{Dis}(w_1 \dots w_n)$ für eine Interpretation $w_1 \dots w_n$, für welche es eine natürliche Zahl j mit $1 \leq j \leq n$ und $w_j \neq v_j$ gibt. Da aber für jede solchen Interpretation $w_1 \dots w_n$ der Wahrheitswert von $\mathrm{Dis}(w_1 \dots w_n)$ unter der Interpretation $v_1 \dots v_n$ nach Bemerkung (1.44) gleich 0 ist, gilt dies auch für die Disjunktion F. Somit ist in jedem Fall der Wahrheitswert von F unter der Interpretation $v_1 \dots v_n$ gleich dem $v_1 \dots v_n$ zugewiesenen Wahrheitswert in der potentiellen Wahrheitstafel.

Umgekehrt sei G eine beliebige aussagenlogische Formel in disjunktiver Normalform derart, dass G die Wahrheitswerte der gegebenen potentiellen Wahrheitstafel annimmt. Dann gibt es eine nicht-negative ganze Zahl k und verschiedene aussagenlogische Formeln $G_1, \dots, G_k$ derart, dass $G = G_1 \vee \dots \vee G_k$, und so, dass für alle natürlichen Zahlen i mit $1 \leq i \leq k$ stets $G_i = X_{i,1} \wedge \dots \wedge X_{i,n}$ gilt, wobei $X_{i,j} = A_j$ oder $X_{i,j} = \neg A_j$ für alle natürlichen Zahlen j mit $1 \leq j \leq n$. Ferner sei eine Interpretation $v_1 \dots v_n$ gegeben.

Zunächst sei angenommen, dass der Wert von $v_1 \dots v_n$ in der potentiellen Wahrheitstafel gleich 1 ist. Da G die Wahrheitswerte der potentiellen Wahrheitstafel annimmt, ist somit auch der Wahrheitswert von G unter $v_1 \dots v_n$ gleich 1. Wegen $G = G_1 \vee \dots \vee G_k$ gibt es also eine natürliche Zahl i mit $1 \leq i \leq k$ und derart, dass G_i unter $v_1 \dots v_n$ den Wahrheitswert 1 annimmt. Für jede natürliche Zahl j mit $1 \leq j \leq n$ sei

$$w_j := \begin{cases} 1, & \text{falls } X_{i,j} = A_j, \\ 0, & \text{falls } X_{i,j} = \neg A_j. \end{cases}$$

Dann ist $G_i = X_{i,1} \wedge \dots \wedge X_{i,n} = \mathrm{Dis}(w_1 \dots w_n)$. Da aber der Wahrheitswert von G_i unter der Interpretation $v_1 \dots v_n$ gleich 1 ist, gilt $w_j = v_j$ für jede natürliche Zahl j mit $1 \leq j \leq n$ nach Bemerkung (1.44). Folglich ist $G_i = \mathrm{Dis}(w_1 \dots w_n) = \mathrm{Dis}(v_1 \dots v_n)$ ein Disjunkt von G.

Nun sei angenommen, dass der Wert von $v_1 \dots v_n$ in der potentiellen Wahrheitstafel gleich 0 ist. Da G die Wahrheitswerte der potentiellen Wahrheitstafel annimmt, ist somit auch der Wahrheitswert von G unter$v_1 \dots v_n$ gleich 0. Wegen $G = G_1 \vee \dots \vee G_k$ gilt somit für jede natürliche Zahl i mit $1 \leq i \leq k$, dass G_i unter $v_1 \dots v_n$ den Wahrheitswert 0 annimmt. Nach Bemerkung (1.44) ist aber der Wahrheitswert von $\mathrm{Dis}(v_1 \dots v_n)$ unter $v_1 \dots v_n$ gleich 1, so dass für jede natürliche Zahl i mit $1 \leq i \leq k$ also notwendigerweise $G_i \neq \mathrm{Dis}(v_1 \dots v_n)$ ist.

Insgesamt ist G eine Disjunktion über all diejenigen Disjunkte, welche zu Interpretationen gehören, die in der potentiellen Wahrheitstafel den Wahrheitswert 1 zugewiesen bekommen, d.h. es ist G bis auf Reihenfolge der Disjunkte gleich F.

(b) Dies lässt sich dual zu (a) beweisen. □

(1.46) Beispiel. Es sei die folgende potentielle Wahrheitstafel für die Aussagenvariablen A, B, C gegeben.

A	B	C	
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	1

(a) Eine aussagenlogische Formel in disjunktiver Normalform, welche die gegebene potentielle Wahrheitstafel als Wahrheitstafel hat, ist

$$A \wedge B \wedge C \vee A \wedge \neg B \wedge C \vee \neg A \wedge \neg B \wedge C \vee \neg A \wedge \neg B \wedge \neg C.$$

(b) Eine aussagenlogische Formel in konjunktiver Normalform, welche die gegebene potentielle Wahrheitstafel als Wahrheitstafel hat, ist

$$(\neg A \vee \neg B \vee C) \wedge (\neg A \vee B \vee C) \wedge (A \vee \neg B \vee \neg C) \wedge (A \vee \neg B \vee C).$$

Beweis.

(a) Nach Proposition (1.45)(a) ist

$$\begin{aligned}&\mathrm{Dis}(111) \vee \mathrm{Dis}(101) \vee \mathrm{Dis}(001) \vee \mathrm{Dis}(000)\\ &= A \wedge B \wedge C \vee A \wedge \neg B \wedge C \vee \neg A \wedge \neg B \wedge C \vee \neg A \wedge \neg B \wedge \neg C\end{aligned}$$

eine aussagenlogische Formel in disjunktiver Normalform, welche die gegebene potentielle Wahrheitstafel als Wahrheitstafel hat.

(b) Nach Proposition (1.45)(b) ist

$$\begin{aligned}&\mathrm{Con}(110) \wedge \mathrm{Con}(100) \wedge \mathrm{Con}(011) \wedge \mathrm{Con}(010)\\ &= (\neg A \vee \neg B \vee C) \wedge (\neg A \vee B \vee C) \wedge (A \vee \neg B \vee \neg C) \wedge (A \vee \neg B \vee C)\end{aligned}$$

eine aussagenlogische Formel in konjunktiver Normalform, welche die gegebene potentielle Wahrheitstafel als Wahrheitstafel hat. □

(1.47) Satz. Es sei eine nicht-negative ganze Zahl n gegeben.

(a) Jede aussagenlogische Formel in den Aussagenvariablen $A_1, \ldots, A_n$ ist bis auf Reihenfolge der Disjunkte zu genau einer aussagenlogischen Formel in disjunktiver Normalform bzgl. $A_1, \ldots, A_n$ logisch äquivalent.

(b) Jede aussagenlogische Formel in den Aussagenvariablen $A_1, \ldots, A_n$ ist bis auf Reihenfolge der Konjunkte zu genau einer aussagenlogischen Formel in konjunktiver Normalform bzgl. $A_1, \ldots, A_n$ logisch äquivalent.

Beweis.

(a) Nach Proposition (1.45)(a) gibt es für jede aussagenlogische Formel F bis auf Reihenfolge der Disjunkte genau eine aussagenlogische Formel in disjunktiver Normalform, welche die Wahrheitswerte der Wahrheitstafel von F annimmt, welche also zu F logisch äquivalent ist.

(b) Dies lässt sich dual zu (a) beweisen. □

(1.48) Beispiel.

(a) Eine zu $A \vee B \Rightarrow A \wedge C$ logisch äquivalente aussagenlogische Formel in disjunktiver Normalform ist durch

$$A \wedge B \wedge C \vee A \wedge \neg B \wedge C \vee \neg A \wedge \neg B \wedge C \vee \neg A \wedge \neg B \wedge \neg C.$$

gegeben.

(b) Eine zu $A \vee B \Rightarrow A \wedge C$ logisch äquivalente aussagenlogische Formel in konjunktiver Normalform ist durch

$$(\neg A \vee \neg B \vee C) \wedge (\neg A \vee B \vee C) \wedge (A \vee \neg B \vee \neg C) \wedge (A \vee \neg B \vee C).$$

gegeben.

Beweis. Es sei $F := (A \vee B \Rightarrow A \wedge C)$. Nach Beispiel (1.10)(a) sind die Wahrheitswerte von F wie folgt gegeben.

A	B	C	F
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	1

(a) Nach Beispiel (1.46)(a) ist

$$A \wedge B \wedge C \vee A \wedge \neg B \wedge C \vee \neg A \wedge \neg B \wedge C \vee \neg A \wedge \neg B \wedge \neg C$$

eine aussagenlogische Formel in disjunktiver Normalform, welche unter jeder Interpretation denselben Wahrheitswert wie F annimmt und damit zu F logisch äquivalent ist.

(b) Nach Beispiel (1.46)(b) ist

$$(\neg A \vee \neg B \vee C) \wedge (\neg A \vee B \vee C) \wedge (A \vee \neg B \vee \neg C) \wedge (A \vee \neg B \vee C).$$

eine aussagenlogische Formel in konjunktiver Normalform, welche unter jeder Interpretation denselben Wahrheitswert wie F annimmt und damit zu F logisch äquivalent ist. □

Alternativer Beweis. Nach Beispiel (1.10)(a) sind die Wahrheitswerte von $\neg F$ wie folgt gegeben.

A	B	C	$\neg F$
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	1
0	1	0	1
0	0	1	0
0	0	0	0

(a) Nach Proposition (1.45)(b) ist

$$(\neg A \vee \neg B \vee \neg C) \wedge (\neg A \vee B \vee \neg C) \wedge (A \vee B \vee \neg C) \wedge (A \vee B \vee C)$$

eine aussagenlogische Formel in konjunktiver Normalform, welche unter jeder Interpretation denselben Wahrheitswert wie $\neg F$ annimmt und damit zu $\neg F$ logisch äquivalent ist. Nach Beispiel (1.20) und den De Morganschen Gesetzen (1.21) folgt

$$\begin{aligned} F &\equiv \neg(\neg F) \equiv \neg((\neg A \vee \neg B \vee \neg C) \wedge (\neg A \vee B \vee \neg C) \wedge (A \vee B \vee \neg C) \wedge (A \vee B \vee C)) \\ &\equiv A \wedge B \wedge C \vee A \wedge \neg B \wedge C \vee \neg A \wedge \neg B \wedge C \vee \neg A \wedge \neg B \wedge \neg C. \end{aligned}$$

(b) Nach Proposition (1.45)(a) ist

$$A \wedge B \wedge \neg C \vee A \wedge \neg B \wedge \neg C \vee \neg A \wedge B \wedge C \vee \neg A \wedge B \wedge \neg C$$

eine aussagenlogische Formel in disjunktiver Normalform, welche unter jeder Interpretation denselben Wahrheitswert wie $\neg F$ annimmt und damit zu $\neg F$ logisch äquivalent ist. Nach Beispiel (1.20) und den De Morganschen Gesetzen (1.21) folgt

$$\begin{aligned} F &\equiv \neg(\neg F) \equiv \neg(A \wedge B \wedge \neg C \vee A \wedge \neg B \wedge \neg C \vee \neg A \wedge B \wedge C \vee \neg A \wedge B \wedge \neg C) \\ &\equiv (\neg A \vee \neg B \vee C) \wedge (\neg A \vee B \vee C) \wedge (A \vee \neg B \vee \neg C) \wedge (A \vee \neg B \vee C). \end{aligned}$$ □

Prädikate

Zum Abschluss dieses Abschnitts skizzieren wir noch einige Aspekte der Prädikatenlogik. Dabei werden wir diesen Kalkül noch knapper und informeller als den der Aussagenlogik behandeln, da eine weiterführende Formalisierung ohne Kenntnis einiger mathematischer Strukturen sehr abstrakt und nur schwer verständlich ist. ([14]) Der Zweck dieser kurzen Abhandlung ist es, eine intuitive Idee von Ausdrücken der Form $\exists x : P(x)$ zu bekommen.

Während die Aussagenlogik Modelle für Aussagen und deren logische Zusammensetzungen studiert, wird in der Prädikatenlogik auf die innere Struktur von Aussagen eingegangen. Anstelle von Aussagen betrachtet man nun Prädikate über einem zuvor festgelegten *Individuenbereich* (auch *Diskursuniversum* genannt). Ein *Prädikat*

[14] Weitergehende Präzisierungen werden in Vorlesungen zur *mathematischen Logik* vermittelt; an der RWTH Aachen üblicherweise im Rahmen des Kurses *Mathematische Logik* (etwa 4. Semester im Studiengang B.Sc. Informatik).

(manchmal etwas irreführend auch *Aussageform* genannt, vgl. Definition (1.1)(b)) ist hierbei eine „Eigenschaft“ oder eine „Beziehung“, welche für die Individuen aus dem zuvor festgelegten Bereich entweder gilt oder nicht. Betrachtet man ein Prädikat von konkreten Individuen, so erhält man eine Aussage.
Beispielsweise ist „Anne speist mit Christian.“ eine Aussage. Betrachten wir nun den Individuenbereich „Freundeskreis (des Dozenten)“, so sind „Anne“ und „Christian“ Individuen und es ist „... speist mit ...“ ein zweistelliges Prädikat über diesem Bereich (zweistellig, da das Prädikat zwei Individuen in Verbindung setzt).

Prädikatenlogische Formeln

So wie in der Aussagenlogik die Aussagen durch Aussagenvariablen abstrahiert werden, treten bei der Formalisierung der Prädikatenlogik nun *Individuenvariablen* an die Stelle von Individuen und *Prädikatvariablen* an die Stelle der Prädikate. So lässt sich oben genanntes Beispiel etwa durch $P(x, y)$ formalisieren, wobei „Anne“ durch x bzw. „Christian“ durch y sowie „... speist mit ...“ durch P ersetzt wird.
Desweiteren können in einer *prädikatenlogischen Formel* noch die aus der Aussagenlogik bekannten *Junktoren*, Hilfsklammern und die sogenannten *Quantoren* auftreten. Der *Existenzquantor* (Symbol $\exists$) formalisiert hierbei die Existenz eines Individuums, für welches ein gewisses Prädikat gilt, während der *Allquantor* (Symbol $\forall$) für die Allgemeingültigkeit des Prädikats für alle Individuen steht. Dabei wird $(\exists x)(P(x))$ als *es gibt ein x mit $P(x)$* und $(\forall x)(P(x))$ als *für alle x gilt $P(x)$* gelesen. Um die Bildung von Klammern zu reduzieren, schreiben wir meist $\exists x : P(x)$ statt $(\exists x)(P(x))$ sowie $\forall x : P(x)$ statt $(\forall x)(P(x))$.
Bei mehreren Individuenvariablen kommt es auf die Art und die Reihenfolge der Quantoren an. Wollen wir etwa die beiden in $P(x, y)$ vorkommenden *freien* Individuenvariablen x und y durch Quantoren *binden*, so haben wir die vier Möglichkeiten $\exists x : \exists y : P(x, y)$, $\exists x : \forall y : P(x, y)$, $\forall x : \exists y : P(x, y)$ und $\forall x : \forall y : P(x, y)$. Steht $P(x, y)$ wie oben für das Prädikat „... speist mit ...“, so steht $\exists x : \exists y : P(x, y)$ für die Aussage, dass es zwei nicht notwendigerweise verschiedene Individuen gibt ([15]), welche miteinander speisen („es gibt ein Paar von Individuen, welches miteinander speist“), während $\forall x : \forall y : P(x, y)$ der Aussage entspricht, dass jeder mit jedem speist. Die prädikatenlogische Formel $\exists x : \forall y : P(x, y)$ repräsentiert die Aussage, dass es ein Individuum gibt, welches mit allen (anderen und sich selbst) speist, während $\forall x : \exists y : P(x, y)$ die Existenz eines Tischpartners für jedes Individuum formalisiert.

Wahrheitswerte prädikatenlogischer Formeln

Bei einer *Interpretation* werden ein Individuenbereich, für jede Prädikatvariable ein Prädikat und für alle freien Individuenvariablen konkrete Individuen festgelegt. Interpretieren wir die Quantoren noch wie oben angedeutet, so ergibt sich bei einer gegebenen Interpretation der *Wahrheitswert* einer prädikatenlogischen Formel als Wahrheitswert der erhaltenen Aussage.
Oftmals stehen an Stelle der Prädikatvariablen bereits konkrete mathematische Symbole, welche aber erst durch Wahl des Individuenbereichs eine feste Bedeutung erhalten. Betrachten wir beispielsweise die prädikatenlogische Formel $x > 0$ in der Individuenvariablen x. Anstelle einer Prädikatvariablen $P(x)$ steht hier der Ausdruck $x > 0$. Hierbei handelt es sich *nicht* um ein Prädikat; wir haben es lediglich mit einer Aneinanderreihung von Symbolen zu tun, da wir für die einstellige Prädikatvariable > 0 noch keine inhaltliche Bedeutung zugewiesen haben. Dies geschieht erst bei einer Interpretation: Legen wir beispielsweise als Individuenbereich die natürlichen Zahlen fest und interpretieren wir > 0 wie üblich, also $>$ als die übliche Striktordnung auf den natürlichen Zahlen und 0 als die übliche ganze Zahl 0, so erhalten wir für jede mögliche Zuordnung eines Individuums aus dem gewählten Bereich eine wahre Aussage. Wählen wir hingegen als Individuenbereich die reellen Zahlen und interpretieren > 0 wie üblich, also $>$ als die übliche Striktordnung auf den reellen Zahlen und 0 als die übliche reelle Zahl 0, so gibt es Individuen, für welche wir eine wahre Aussage erhalten (etwa $\frac{1}{2}$), aber auch Individuen, für welche wir eine falsche Aussage erhalten (etwa $-\sqrt{2}$).
Während in der prädikatenlogischen Formel $F(x) = (x > 0)$ die Individuenvariable x frei ist und daher bei einer Interpretation durch ein konkretes Individuum des Individuenbereichs ersetzt wird, ist dies in $G = (\forall x : x > 0)$ und $H = (\exists x : x > 0)$ nicht der Fall. Wählen wir als Individuenbereich die natürlichen Zahlen, so erhalten wir für G und H jeweils den Wahrheitswert 1, während wir für den Individuenbereich der reellen Zahlen für G den Wahrheitswert 0 und für H den Wahrheitswert 1 erhalten.
Auch bei der Bestimmung des Wahrheitswerts einer prädikatenlogischen Formel bzgl. einer gegebenen Interpretation kommt es natürlich auf die Reihenfolge der Quantoren an. Betrachten wir hierzu beispielsweise die prädikatenlogischen Formeln $G = (\forall y : \exists x : y = x^2)$, $H = (\exists x : \forall y : y = x^2)$, $K = (\forall x : \exists y : y = x^2)$

[15] Der Existenzquantor formalisiert die Existenz *mindestens eines* Objekts.

und $L = (\exists y : \forall x : y = x^2)$. Bei einer Interpretation durch die reellen Zahlen liefern G, H und L jeweils den Wahrheitswert 0, während wir für K den Wahrheitswert 1 erhalten.

Logische Äquivalenz prädikatenlogischer Formeln

Wie in der Aussagenlogik lässt sich auch für prädikatenlogische Formeln ein Begriff der *logischen Äquivalenz* definieren. Für beliebige Prädikatvariablen $P(x)$ in der Individuenvariablen x sind dann $\neg(\forall x : P(x))$ und $\exists x : \neg P(x)$ sowie $\neg(\exists x : P(x))$ und $\forall x : \neg P(x)$ jeweils logisch äquivalente prädikatenlogische Formeln.

Zur Verwendung von logischen Symbolen

Wir werden das Studium der mathematischen Logik und insbesondere die Formalisierung logischer Strukturen nun beenden und verweisen auf weiterführende Vorlesungen. Da bereits die mathematischen Sachverhalte, über welche wir im Folgenden reden werden, formalisiert werden, unterhalten wir uns über diese in der Umgangssprache. Unsere Texte schreiben wir ebenfalls in dieser *Metasprache* auf, lediglich die Objekte (wie im nächsten Abschnitt Mengen, Elemente, etc.) werden formalisiert. Da die mathematische Logik nicht mehr Gegenstand unserer Untersuchungen ist, verzichten wir dementsprechend auch auf die Verwendung logischer Symbole. Hierdurch können wir eine Überformalisierung vermeiden und den Text lesbarer halten. Der Verzicht auf logische Symbole außerhalb der mathematischen Logik wird gemeinhin als guter Stil empfunden.
Man beachte, dass wir durch diese Regelung im weiteren Verlauf streng genommen nichts anderes machen werden als zuvor: Auch bisher haben wir logische Symbole nur in aussagen- und prädikatenlogischen Formeln benutzt, nicht jedoch bei den Aussagen selbst verwandt – und schon gar nicht in den Aussagen über die Aussagen bzw. den Aussagen über die aussagenlogischen Formeln. Logische Symbole sind Bestandteile der *Objektsprache*, d.h. der formalen Sprache, die wir in diesem Abschnitt studiert haben, und die uns als formales Modell für Aussagen und Prädikate dient.
Wir haben die Logik in diesem Abschnitt studiert, um die logischen Strukturen der im Folgenden auftauchenden Sätze besser verstehen und einordnen zu können. Ferner hilft uns das logische Verständnis beim Auffinden von Beweisen. Aus diesen Gründen wird von der oben getroffenen Konvention, auf logische Symbole zu verzichten, in Ausnahmesituationen Abstand genommen (auch wenn dies streng genommen wegen der Trennung von Objektsprache und Metasprache keinen Sinn macht); etwa wenn man bei umgangssprachlich vergleichsweise kompliziert auszudrückenden Sachverhalten die logische Struktur genauer präzisieren möchte. Ein Beispiel hierfür ist etwa die Definition der Konvergenz einer Folge in der Analysis, dessen prädikatenlogische Formalisierung vergleichsweise viele Quantoren beinhaltet, bei welchen es zudem auf die Reihenfolge ankommt.
Eine zweite Ausnahme von dieser Regelung ist der Anschrieb von Vorlesungsnotizen an einer Tafel oder ähnlichen Präsentationsgeräten wie einem Overheadprojektor: Da eine Vorlesung oder ein Vortrag durch die Verwendung der mündlichen Sprache einen anderen Charakter als ein geschriebener Text hat, werden logische Symbole hier gerne als Abkürzung genommen.

Sprachliche Konventionen

Wenn wir sagen, dass eine erste Aussage *oder* eine zweite Aussage gilt, so lassen wir damit stets zu, dass auch beide Aussagen gelten. Die aussagenlogische Formalisierung dieses umgangssprachlichen Konstrukts entspricht einer Disjunktion. Möchten wir darstellen, dass *entweder* die erste Aussage *oder* die zweite Aussage gilt, so sagen wir dies explizit. Analog bei mehr als zwei Aussagen.
Die Existenz *eines* Objektes bedeute stets die Existenz von *mindestens einem* Objekt. Bei einer Formalisierung im Sinne der Prädikatenlogik würden wir in diesem Fall einen Existenzquantor erhalten. Möchten wir die Existenz von *genau einem* Objekt ausdrücken, so sagen wir auch dies explizit dazu.
Wenn wir sagen, dass eine Eigenschaft *für* gewisse Objekte gilt, so meinen wir damit stets, dass die Eigenschaft *für alle* diese Objekte gilt. Eine prädikatenlogische Formalisierung würde in diesem Fall einen Allquantor ergeben. Möchten wir hingegen ausdrücken, dass die Eigenschaft *für eines* der Objekte gilt, dass es also ein Objekt (unter allen potentiellen Objekten) mit dieser Eigenschaft gibt, so sagen wir dies explizit dazu. Bei einer Formalisierung würden wir dann einen Existenzquantor erhalten.
Die Formulierung, dass ein (beliebiges) Objekt *gegeben sein* soll, bedeute, dass das danach Dargestellte *für jedes* solche Objekt gilt. Dieser Ausdruck entspricht bei einer Formalisierung einem Allquantor.
Wenn wir sagen, dass wir uns ein Objekt mit einer Eigenschaft *wählen*, so bedeute dies, dass ein Objekt mit dieser Eigenschaft *existiert* (per Definition oder nach einer vorher gezeigten Aussage). Formal entspricht dies

einem Existenzquantor.

Zusätzliche Konzepte

Im Folgenden geben wir einige zusätzliche Definitionen, deren Studium dem Leser zur Übung überlassen sei.

(1.49) Definition (Modell)**.** Es seien eine nicht-negative ganze Zahl n und eine aussagenlogische Formel F in den Aussagenvariablen $A_1, \ldots, A_n$ gegeben. Ein *Modell* für F ist eine Interpretation der Aussagenvariablen $A_1, \ldots, A_n$ derart, dass F unter dieser Interpretation den Wahrheitswert 1 annimmt.

(1.50) Definition (Erfüllbarkeit, Falsifizierbarkeit)**.** Es seien eine nicht-negative ganze Zahl n und eine aussagenlogische Formel F in den Aussagenvariablen $A_1, \ldots, A_n$ gegeben.

(a) Die aussagenlogische Formel F heißt *erfüllbar*, wenn es ein Modell für F gibt.

(b) Die aussagenlogische Formel F heißt *falsifizierbar*, wenn es eine Interpretation der Aussagenvariablen $A_1, \ldots, A_n$ gibt, welche kein Modell für F ist.

2 Mengen

Unser nächstes Ziel ist die Einführung von Mengen und einiger damit verbundener Konzepte wie Mengenoperationen. Hierbei wollen wir nicht genau sagen, was eine Menge ist, sondern lediglich, was wir uns hierunter vorstellen und wie wir mit Mengen umgehen. Um Mengen auf einer soliden mathematischen Basis einführen zu können, bedarf es weiterer Formalismen innerhalb der *mathematischen Logik*, welche den Rahmen unserer einführenden Veranstaltung sprengen würden. ([16]) Für das erfolgreiche Studium der meisten Gebiete der Informatik (und auch der Mathematik) genügt jedoch eine Kenntnis über Mengen im Umfang dieser Anfängervorlesung. Dafür ist es nicht wichtig, zu wissen, was eine Menge ist, sondern eine gewisse Vorstellung von Mengen zu entwickeln und den Umgang mit Mengen zu verinnerlichen.
Wir beginnen mit einer informellen Einführung des Mengenbegriffs und der Festlegung von Notationen zur Angabe von Mengen. Danach werden Teilmengen und die Potenzmenge eingeführt. Im Anschluss betrachten wir Tupel, Folgen und allgemeinere Familien. Es folgen innere und äußere Mengenoperationen sowie eine Illustration am Beispiel von Datenbanken. Der Abschnitt schließt mit der Behandlung von Matrizen als ein weiteres Beispiel für Familien.
Die durch Anführungsstriche markierten Wörter in diesem Abschnitt werden nicht genauer präzisiert.

Begriffsbildung

Wir beginnen mit der Beschreibung dessen, was wir uns unter einer Menge vorstellen wollen, sowie einigen sprachlichen Konventionen.

(2.1) Vorstellung (Menge; Cantor, 1895)**.**

(a) Unter einer *Menge* verstehen wir eine „Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen“.

(b) Es sei eine Menge X gegeben. Diejenigen Objekte, welche durch X zusammengefasst werden, bezeichnen wir als *Elemente* von X. Ist ein Objekt x ein Element von X, so schreiben wir $x \in X$, andernfalls $x \notin X$.

(c) Es seien Mengen X und Y gegeben. Die Mengen X und Y sind *gleich*, geschrieben $X = Y$, falls sie die gleichen Elemente enthalten, d.h. falls für jedes Objekt x genau dann $x \in X$ gilt, wenn $x \in Y$ gilt.

Nach (2.1)(a) ist eine Menge X allein durch ihren „Umfang“ bestimmt, d.h. durch ihre Elemente festgelegt (*Extensionalitätsprinzip*): Für ein gegebenes Objekt x gilt entweder $x \in X$ oder $x \notin X$. Demnach kann ein Objekt auch nicht „mehrfach“ als Element vorkommen und es gibt auch keine „Ordnung“ der Elemente.

[16] Eine mathematisch präzise Einführung von Mengen wird in Vorlesungen über *axiomatische Mengenlehre* vermittelt; an der RWTH Aachen üblicherweise im Rahmen des Kurses *Mathematische Logik II* (ab etwa 5. Semester im Studiengang B.Sc. Informatik).

Im Folgenden werden wir einige Notationen zur Beschreibung von Mengen angeben. In aller Regel erfolgt eine solche Beschreibung durch die Angabe einer „Eigenschaft“ ([17]), welche die Elemente einer Menge erfüllen, oder durch eine einfache „Aufzählung“ ihrer Elemente. Letzteres wird vor allem bei einer Menge mit „endlich“ vielen Elementen gemacht – etwas unpräzise aber auch bei „unendlich“ vielen Elementen, sofern aus dem Kontext klar ist (bzw. klar sein sollte), welche Objekte aufgezählt werden.

(2.2) Notation.

(a) Es seien eine Menge X und eine Eigenschaft φ so gegeben, dass für jedes Objekt x genau dann $x \in X$ gilt, wenn x die Eigenschaft φ erfüllt. Wir schreiben

$$\{x \mid x \text{ erfüllt } \varphi\} := X.$$

(b) Es sei eine Menge X gegeben. Für eine Eigenschaft φ schreiben wir

$$\{x \in X \mid x \text{ erfüllt } \varphi\} := \{x \mid x \in X \text{ und } x \text{ erfüllt } \varphi\}.$$

(c) Es seien Objekte $a_1, \ldots, a_n$ gegeben. Wir schreiben

$$\{a_1, \ldots, a_n\} := \{x \mid x = a_1 \text{ oder } \ldots \text{ oder } x = a_n\}.$$

(d) Für jede natürliche Zahl i sei ein Objekt a_i gegeben. Wir schreiben

$$\{a_1, a_2, a_3, \ldots\} := \{x \mid \text{es gibt eine natürliche Zahl } i \text{ mit } x = a_i\}.$$

Wir erinnern daran, dass das „oder“ in der Mathematik, siehe Notation (2.2)(c), gemäß der semantischen Interpretation des Junktors $\vee$ in Definition (1.7)(b) für ein *einschließendes oder* steht: Für Objekte x, a und b gilt also genau dann $x = a$ oder $x = b$, wenn $x = a$ und $x \neq b$, oder wenn $x \neq a$ und $x = b$, oder wenn $x = a$ und $x = b$ gilt, d.h. wenn das Objekt x gleich einem oder beiden der beiden Objekte a und b ist. ([18]) Wenn wir sagen möchten, dass das Objekt x identisch zu genau einem der beiden Objekte a und b ist, so betonen wir dies und sagen „entweder $x = a$ oder $x = b$“. Ähnlich für beliebig viele Objekte.
Entsprechend bedeutet die Existenz eines Objektes mit einer vorgegebenen Eigenschaft, vgl. Notation (2.2)(d), dass es *mindestens* ein Objekt mit dieser Eigenschaft gibt.
Obwohl es sehr natürlich scheint, Mengen durch Eigenschaften zu beschreiben, möchten wir betonen, dass *nicht* jede Eigenschaft eine Menge beschreibt. Beispielsweise ist es nicht möglich, $\{x \mid x \text{ ist eine Menge}\}$ zu bilden. Es ist jedoch stets möglich, Mengen wie in (2.2)(b) zu bilden, d.h. Mengen, deren Elemente alle in einer bereits gegebenen Menge X liegen und zusätzlich eine gegebene Eigenschaft φ erfüllen. (*Aussonderung*)

(2.3) Beispiel. Wir wollen davon ausgehen, dass wir wissen, was die folgenden Mengen sind. ([19])

(a) Die *Menge der natürlichen Zahlen* ist durch

$$\mathbb{N} = \{x \mid x = 1 \text{ oder es gibt ein } y \in \mathbb{N} \text{ mit } x = y + 1\} = \{1, 2, 3, \ldots\}$$

gegeben. Die *Menge der natürlichen Zahlen mit Null* ist durch

$$\mathbb{N}_0 = \{x \mid x \in \mathbb{N} \text{ oder } x = 0\}$$

gegeben.

(b) Die *Menge der ganzen Zahlen* ist durch

$$\mathbb{Z} = \{x \mid x \in \mathbb{N} \text{ oder } x = 0 \text{ oder es gibt ein } y \in \mathbb{N} \text{ mit } x = -y\}$$

gegeben.

[17] Die formale Behandlung einer axiomatischen Mengenlehre im Rahmen dieser Vorlesung scheitert unter anderem an der unzureichenden Behandlung der Prädikatenlogik in Abschnitt 1; Eigenschaften lassen sich als (1-stellige) Prädikate präzisieren.

[18] Tritt der Fall $x = a$ und $x \neq b$ oder der Fall $x \neq a$ und $x = b$ ein, so gilt notwendigerweise $a \neq b$; tritt der Fall $x = a$ und $x = b$ ein, so gilt notwendigerweise $a = b$. Wir haben aber weder vorausgesetzt, dass $a \neq b$ gilt, noch dass $a = b$ gilt. Durch die Verwendung des *einschließenden oder* ist es uns möglich, beide Fälle simultan zu betrachten.

[19] Man kann diese Mengen geeignet aus der leeren Menge, siehe Definition (2.8), konstruieren; dies wollen wir aber in diesem Kurs nicht machen. Um die meisten Konzepte der Mengenlehre einzuführen und die grundlegenden Aussagen zu beweisen, benötigen wir diese Mengen nicht. Sie helfen uns jedoch insofern, dass wir durch sie erläuternde Beispiele angeben können.

(c) Die *Menge der rationalen Zahlen* ist durch

$$\mathbb{Q} = \{x \mid \text{es gibt } p, q \in \mathbb{Z} \text{ mit } q \neq 0 \text{ und } x = \frac{p}{q}\}$$

gegeben.

(d) Die *Menge der reellen Zahlen* wird als $\mathbb{R}$ notiert.

(2.4) Beispiel.

(a) Es ist $\{x \mid x \text{ ist eine Primzahl}\}$ eine Menge.

(b) Es ist $\{x \in \mathbb{Z} \mid x \text{ ist gerade}\}$ eine Menge.

(c) Es ist $\{-3, 1, 19\}$ eine Menge.

(d) Es ist $\{1, 2, 4, 8, 16, 32, 64, \dots\}$ eine Menge.

Man beachte, dass Mengen beliebige Objekte zusammenfassen, also beispielsweise auch wieder Mengen:

(2.5) Beispiel. Es sind $\{1\}$, $\{\{1\}\}$ und $\{1, \{1\}\}$ Mengen.

Bei der Beschreibung einer Menge durch Aufzählung ihrer Elemente kommt es nach dem Extensionalitätsprinzip nur auf die Elemente selbst an, nicht auf die Reihenfolge und die Häufigkeit des Auftretens einzelner Elemente innerhalb der Aufzählung (vgl. Notation (2.2)(c), man beachte die einschließende Bedeutung von „oder“).

(2.6) Beispiel.

(a) Es ist $\{-3, 1, 19\} = \{1, 19, -3\} = \{1, 19, -3, 1\}$.

(b) Es ist $\{1\} = \{1, 1, 1\}$.

(c) Es ist $\{x \in \mathbb{R} \mid x^3 + 2x = 3x^2\} = \{0, 1, 2\}$.

(d) Es ist $\{1\} \neq \{1, 2\}$.

(e) Es ist $\{1\} \neq \{\{1\}\}$ und $\{1\} \neq \{1, \{1\}\}$ und $\{\{1\}\} \neq \{1, \{1\}\}$.

Wir können Mengen auch benutzen, um Zusammenfassungen des täglichen Lebens zu modellieren ([20]):

(2.7) Anwendungsbeispiel.

(a) Das lateinische Alphabet lässt sich als Menge $\{\mathrm{A}, \mathrm{B}, \dots, \mathrm{Z}\}$ auffassen.

(b) Eine Platzierung in der Tabelle der Fußball-Bundesliga lässt sich als ein Element der Menge $\{1, 2, \dots, 18\}$ auffassen.

(c) Eine Medaille bei den Olympischen Spielen lässt sich als ein Element der Menge $\{\text{gold}, \text{silber}, \text{bronze}\}$ auffassen.

(d) Eine Kartenfarbe lässt sich als ein Element der Menge $\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}$ auffassen.

(e) Eine Position in einer Reihe von Objekten lässt sich als ein Element von $\mathbb{N}$ auffassen.

(f) Die Anzahl der Objekte in einer Ansammlung lässt sich als ein Element von $\mathbb{N}$ auffassen.

Auf Grund des Extensionalitätsprinzips gibt es nur eine Menge, welche keine Elemente enthält. Wir benutzen folgende Bezeichnung:

[20] Bei einer axiomatischen Behandlung der Mengenlehre beinhalten Mengen nur „mathematische Objekte“, so dass erst mal nicht klar ist, was eine Menge der Form $\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}$ wie in Beispiel (2.7)(d) sein soll. Dies ist aber nicht weiter tragisch, da wir nicht sagen, was die Elemente dieser Menge sind. Zu Modellierungszwecken könnten wir etwa zuvor $\heartsuit := 0$, $\diamondsuit := 1$, $\spadesuit := 2$, $\clubsuit := 3$ setzen, oder aber $\heartsuit := \emptyset$ (siehe Definition (2.8)), $\diamondsuit := \{\emptyset\}$, $\spadesuit := \{\{\emptyset\}\}$, $\clubsuit := \{\{\{\emptyset\}\}\}$. Die präzise Definition dieser Elemente ist für Anwendungszwecke nicht relevant, weswegen wir in solchen Anwendungsbeispielen darauf verzichten werden – wichtig ist lediglich, dass die Elemente einer solchen Menge „wohlunterschieden“ sind.

(2.8) Definition (leere Menge)**.** Die Menge, welche keine Elemente enthält, heißt *leere Menge* und wird als $\emptyset$ notiert.

Im Folgenden werden wir des Öfteren Mengen bestehend aus endlich vielen aufeinanderfolgenden ganzen Zahlen betrachten. Aus diesem Grund führen wir folgende Schreibweise ein:

(2.9) Notation. Für $a, b \in \mathbb{Z}$ mit $a \leq b + 1$ schreiben wir

$$[a, b] := \{x \in \mathbb{Z} \mid a \leq x \leq b\}.$$

(2.10) Beispiel.

(a) Es ist $[1, 3] = \{1, 2, 3\}$.

(b) Es ist $[-2, 1] = \{-2, -1, 0, 1\}$.

(c) Es ist $[-1, -1] = \{-1\}$.

(d) Es ist $[2, 1] = \emptyset$.

Teilmengen

Wir wollen dem Konzept aus Notation (2.2)(b) einen Namen geben:

(2.11) Definition (Teilmenge)**.** Es sei eine Menge X gegeben. Eine *Teilmenge* von X ist eine Menge U derart, dass aus $u \in U$ stets $u \in X$ folgt.
Eine Teilmenge U von X heißt *echt* (oder *strikt*), falls $U \neq X$ gilt.
Es sei eine Menge U gegeben. Ist U eine Teilmenge von X, so schreiben wir $U \subseteq X$. Ist U keine Teilmenge von X, so schreiben wir $U \nsubseteq X$. Ist U eine echte Teilmenge von X, so schreiben wir $U \subset X$.

Die Teilmengennotation ist innerhalb der Mathematik nicht einheitlich: Manche Autoren schreiben $U \subset X$ anstatt $U \subseteq X$ und $U \subsetneq X$ anstatt $U \subset X$. Da Mathematik von Menschen gemacht wird, sind abweichende Notationen etwas ganz Normales und teilweise auch unvermeidbar. In vielen Bereichen haben sich jedoch Standardnotationen eingebürgert, und in aller Regel versucht man, sich auch an solche Standardnotationen zu halten. Es wäre zum Beispiel in einem vorliegenden mathematischen Text völlig korrekt, für „U ist eine Teilmenge von X“ stets $U \,\%\, X$ zu schreiben, sofern man sich in diesem Text vorher auf diese Notation festgelegt hat. Ein solcher Text wäre jedoch auch für einen geübten Mathematiker nur schwer lesbar. Wir werden im Folgenden meist nicht auf alternative Notationen anderer Autoren eingehen.

(2.12) Beispiel.

(a) Es ist $\{2, 3, 4, 7\}$ eine Teilmenge von $\{1, 2, 3, 4, 5, 6, 7\}$.

(b) Es ist $\{0, 3, 4, 7\}$ keine Teilmenge von $\{1, 2, 3, 4, 5, 6, 7\}$.

(c) Es gilt $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$, d.h. es ist $\mathbb{N}$ eine Teilmenge von $\mathbb{Z}$, es ist $\mathbb{Z}$ eine Teilmenge von $\mathbb{Q}$ und es ist $\mathbb{Q}$ eine Teilmenge von $\mathbb{R}$.

(2.13) Bemerkung (Gleichheitskriterium für Mengen)**.** Es seien Mengen X und Y gegeben. Genau dann ist $X = Y$, wenn $X \subseteq Y$ und $Y \subseteq X$ gilt.

Beweis. Genau dann gilt $X = Y$, wenn für jedes Objekt x genau dann $x \in X$ gilt, wenn $x \in Y$ gilt, d.h. falls aus $x \in X$ stets $x \in Y$ folgt und falls aus $x \in Y$ stets $x \in X$ folgt. Nun folgt aus $x \in X$ jedoch genau dann stets $x \in Y$, wenn $X \subseteq Y$ gilt, und entsprechend folgt aus $x \in Y$ genau dann stets $x \in X$, wenn $Y \subseteq X$ gilt. Insgesamt haben wir genau dann $X = Y$, wenn $X \subseteq Y$ und $Y \subseteq X$ gilt. □

Die Teilmengen einer gegebenen Menge X können wieder zu einer Menge zusammengefasst werden:

(2.14) Definition (Potenzmenge)**.** Es sei eine Menge X gegeben. Die *Potenzmenge* von X ist definiert als

$$\mathrm{Pot}(X) := \{U \mid U \text{ ist eine Teilmenge von } X\}.$$

(2.15) Beispiel.

(a) Es ist $\mathrm{Pot}(\{1\}) = \{\emptyset, \{1\}\}$.

(b) Es ist $\mathrm{Pot}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

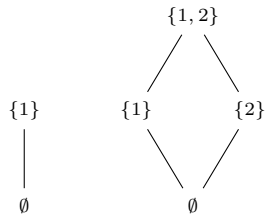


Abbildung 1: Teilmengen von $\{1\}$ und $\{1, 2\}$

Familien

Ein klassisches Beispiel für Mengen von Paaren geht zurück auf René Descartes (17. Jahrhundert): Durch Einführung eines Koordinatenkreuzes werden die Punkte der Anschauungsebene durch Paare reeller Zahlen modelliert; die Ebene entspricht dann

$$\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}.$$

Geometrische Objekte innerhalb der Ebene lassen sich durch diese Formalisierung analytisch beschreiben, zum Beispiel der Einheitskreis als

$$S = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$$

oder die Gerade durch $(3, 0)$ und $(0, 2)$ als

$$T = \{(x, y) \in \mathbb{R}^2 \mid 2x + 3y = 6\}.$$

Als Verallgemeinerung dieser Paare führen wir als nächstes Familien ein. Diese können wir uns als eine Art „beschriftete“ oder „parametrisierte Mengen“ vorstellen, an Stelle der Reihenfolge des Auftretens in einem Paar als erste bzw. zweite Komponente tritt hierbei die Parametrisierung durch die Elemente einer gegebenen Menge. Bei der Begriffsbildung verzichten wir auf eine formale Definition und geben lediglich eine charakterisierende Beschreibung von Familien über ein Gleichheitskriterium an, welches wir von einer parametrisierten Menge erwarten: zwei gegebene „beschriftete Mengen“ sind genau dann gleich, wenn die „Mengen der Beschriftungen“ gleich sind und für jede „Beschriftung“ die damit „beschrifteten Elemente“ gleich sind.

(2.16) Vorstellung (Familie)**.**

(a) Es sei eine Menge I gegeben. Eine *Familie* über I ist ein „Ausdruck“ der Form $x = (x_i)_{i \in I}$ für gewisse Objekte x_i für $i \in I$. Die Menge I wird *Indexmenge* von x genannt. Ein Element von I wird *Index* (oder *Stelle*) von x genannt. Für $i \in I$ wird x_i die *Komponente* (oder der *Eintrag*) von x an der Stelle i genannt.

(b) Es seien Mengen I und J, eine Familie $x = (x_i)_{i \in I}$ über I und eine Familie $y = (y_j)_{j \in J}$ über J gegeben. Die Familien $x = (x_i)_{i \in I}$ und $y = (y_j)_{j \in J}$ sind *gleich*, geschrieben $x = y$, wenn $I = J$ und für $i \in I$ stets $x_i = y_i$ gilt.

Eine Familie über einer gegebenen Indexmenge setzt sich nach (2.16)(a) also gewissermaßen aus ihren Komponenten zusammen und nach dem Gleichheitskriterium für Familien (2.16)(b) sind gegebene Familien über dieser Indexmenge genau dann gleich, wenn alle Komponenten jeweils gleich sind. Im Gegensatz zu den Elementen einer Menge sind die Komponenten einer Familie noch durch die Elemente der Indexmenge „gekennzeichnet“, so dass Komponenten zu verschiedenen Stellen einer gegebenen Familie gleich sein können.

(2.17) Beispiel.

(a) Es ist $x = (x_i)_{i \in \{1,2,3\}}$ gegeben durch $x_1 = 3$, $x_2 = -\frac{2}{5}$, $x_3 = \sqrt{7}$ eine Familie über $\{1, 2, 3\}$.

(b) Es ist $x = (x_i)_{i \in \mathbb{N}_0}$ gegeben durch $x_i = i^2 + 1$ für $i \in \mathbb{N}_0$ eine Familie über $\mathbb{N}_0$.

(c) Es ist $(i^2 - 1)_{i \in \mathbb{Z}}$ eine Familie über $\mathbb{Z}$.

(d) Es sei $I := \{\emptyset, \{1\}, \{1, 2\}\}$. Dann ist $x = (x_i)_{i \in I}$ gegeben durch $x_\emptyset = 0$, $x_{\{1\}} = \{\{1\}\}$, $x_{\{1,2\}} = \{3\}$ eine Familie über I.

(e) Es gibt keine Familie $x = (x_i)_{i\in\{2,5\}}$ über $\{2,5\}$ mit $x_2 = 0$ und $x_2 = 1$.

(2.18) Beispiel.

(a) Es sei eine Familie x über $\{-2,1,3\}$ gegeben durch $x_{-2} = 4$, $x_1 = 1$, $x_3 = 9$. Ferner sei eine Familie y über $\{-2,1,3\}$ gegeben durch $y = (i^2)_{i\in\{-2,1,3\}}$. Dann ist $x = y$.

(b) Es seien Familien x und y über $\{0,1\}$ gegeben durch $x_0 = 1$, $x_1 = 2$, $y_0 = 2$, $y_1 = 1$. Dann ist $x \neq y$.

(c) Es sei eine Familie x über $\{0,1\}$ gegeben durch $x_i = 0$ für $i \in \{0,1\}$. Ferner sei eine Familie y über $\{-1,0,1\}$ gegeben durch $y_j = 0$ für $j \in \{-1,0,1\}$. Dann ist $x \neq y$.

Beweis.

(a) Wegen

$$\begin{aligned} x_{-2} &= 4 = (-2)^2 = y_{-2}, \\ x_1 &= 1 = 1^2 = y_1, \\ x_3 &= 9 = 3^2 = y_3 \end{aligned}$$

gilt $x = y$.

(b) Wegen

$$x_0 = 1 \neq 2 = y_0$$

gilt $x \neq y$.

(c) Da x eine Familie über $\{0,1\}$ und y eine Familie über $\{-1,0,1\}$ ist und $\{0,1\} \neq \{-1,0,1\}$ gilt, ist $x \neq y$. □

(2.19) Anwendungsbeispiel.

(a) Eine Belegung einer Küche lässt sich als Familie über der „Menge der Küchenmöbel“ auffassen. Ist die Menge der Küchenmöbel K etwa modelliert durch

$$\begin{aligned} K = \{&\text{Hängeschrank}, \text{Bodenschrank}, \text{Schublade}, \text{Backofen}, \text{Kühlschrank}, \text{Kühltruhe}, \\ &\text{Waschmaschine}\}, \end{aligned}$$

so kann eine typische Belegung etwa modelliert werden durch eine Familie b über K gegeben durch

$$\begin{aligned} b_{\text{Hängeschrank}} &= \text{Geschirr}, \\ b_{\text{Bodenschrank}} &= \text{Töpfe}, \\ b_{\text{Schublade}} &= \text{Besteck}, \\ b_{\text{Backofen}} &= \text{Pizza}, \\ b_{\text{Kühlschrank}} &= \text{Bier}, \\ b_{\text{Kühltruhe}} &= \text{Pizza}, \\ b_{\text{Waschmaschine}} &= \text{Unterhosen}. \end{aligned}$$

(b) Ein 239-seitiges Buch mit sechsseitigem Vorwort lässt sich als Familie über der Menge

$$\{n \mid n \in \{\text{i}, \text{ii}, \text{iii}, \text{iv}, \text{v}, \text{vi}\} \text{ oder } n \in [1, 239]\}$$

auffassen.

(c) Ein Warenkatalog lässt sich als Familie über der „Menge der Artikelnummern“ des Katalogs auffassen.

(d) Eine (reale) Familie bestehend aus Vater, Mutter, einem Sohn und einer Tochter lässt sich als eine (formale) Familie über der Menge $R = \{\text{Vater}, \text{Mutter}, \text{Sohn}, \text{Tochter}\}$ auffassen. Eine typische Familie kann etwa modelliert werden als (formale) Familie Maier über R gegeben durch

$$\begin{aligned} \text{Maier}_{\text{Vater}} &= \text{Hans}, \\ \text{Maier}_{\text{Mutter}} &= \text{Katrin}, \\ \text{Maier}_{\text{Sohn}} &= \text{Uwe}, \\ \text{Maier}_{\text{Tochter}} &= \text{Chantal}. \end{aligned}$$

Wir bemerken, dass in unserem mathematischen Modell in Anwendungsbeispiel (2.19)(a) offenbar

$$b_{\text{Backofen}} = \text{Pizza} = b_{\text{Kühltruhe}}$$

gilt, während im wahren Leben die Pizzen im Backofen und in der Kühltruhe natürlich nicht identisch sind. Wollen wir diese unterscheiden, benötigen wir ein feineres Modell, etwa gegeben durch die Familie b' über K gegeben durch

$$b'_m = \begin{cases} \text{Pizza1}, & \text{für } m = \text{Backofen}, \\ \text{Pizza2}, & \text{für } m = \text{Kühltruhe}, \\ b_m, & \text{für } m \in K \text{ mit } m \neq \text{Backofen und } m \neq \text{Kühltruhe}. \end{cases}$$

Eine weitere Familie c über K ist etwa gegeben durch $c_m = \text{Bier}$ für jedes $m \in K$; ein theoretisch mögliches mathematisches Modell muss also keiner sinnvollen Belegung im wahren Leben entsprechen.
Oft liegen die Komponenten einer Familie in einer gegebenen Menge. Wir vereinbaren hierfür folgende Sprachregelung:

(2.20) Definition (Familie)**.** Es seien eine Menge X und eine Menge I gegeben. Die *Menge der Familien* in X über I ist definiert als

$$X^I := \{x \mid x \text{ ist eine Familie über } I \text{ mit } x_i \in X \text{ für } i \in I\}.$$

Ein Element von X^I wird eine *Familie* in X über I genannt.

(2.21) Beispiel. Es sei $I := \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$ und es sei eine Familie x über I gegeben durch $x_\emptyset = 0$, $x_{\{1\}} = 1$, $x_{\{2\}} = 1$, $x_{\{1,2\}} = 0$.

(a) Es ist x eine Familie in $\mathbb{Z}$.

(b) Es ist x eine Familie in $\mathbb{Q}$.

(c) Es ist x eine Familie in $\{0, 1\}$.

Beweis.

(a) Wegen $x_\emptyset, x_{\{1\}}, x_{\{2\}}, x_{\{1,2\}} \in \mathbb{Z}$ ist x eine Familie in $\mathbb{Z}$.

(b) Wegen $x_\emptyset, x_{\{1\}}, x_{\{2\}}, x_{\{1,2\}} \in \mathbb{Q}$ ist x eine Familie in $\mathbb{Q}$.

(c) Wegen $x_\emptyset, x_{\{1\}}, x_{\{2\}}, x_{\{1,2\}} \in \{0, 1\}$ ist x eine Familie in $\{0, 1\}$. □

(2.22) Beispiel. Es seien Familien a, b, c, d, e, f, g, h in $\{-1, 1\}$ über $\{-2, 1, 5\}$ gegeben durch

$$\begin{array}{lll} a_{-2} = -1, & a_1 = -1, & a_5 = -1, \\ b_{-2} = 1, & b_1 = -1, & b_5 = -1, \\ c_{-2} = -1, & c_1 = 1, & c_5 = -1, \\ d_{-2} = 1, & d_1 = 1, & d_5 = -1, \\ e_{-2} = -1, & e_1 = -1, & e_5 = 1, \\ f_{-2} = 1, & f_1 = -1, & f_5 = 1, \\ g_{-2} = -1, & g_1 = 1, & g_5 = 1, \\ h_{-2} = 1, & h_1 = 1, & h_5 = 1. \end{array}$$

Dann ist

$$\{-1, 1\}^{\{-2,1,5\}} = \{a, b, c, d, e, f, g, h\}.$$

(2.23) Notation. Es seien eine Menge I und eine Eigenschaft φ mit $I = \{i \mid i \text{ erfüllt } \varphi\}$ gegeben. Für eine Familie x über I schreiben wir

$$\{x_i \mid i \text{ erfüllt } \varphi\} := \{z \mid \text{es gibt ein } i \in I \text{ mit } z = x_i\}.$$

Da für jede Menge I insbesondere $I = \{i \mid i \in I\}$ gilt, haben wir nach Notation (2.23) für jede Familie x über I stets

$$\{x_i \mid i \in I\} = \{z \mid \text{es gibt ein } i \in I \text{ mit } z = x_i\}.$$

Diese Menge fasst die Komponenten der Familie x zusammen. Die Schreibweise stellt eine Verallgemeinerung der Beschreibung aus Notation (2.2)(c), (d) dar, vgl. Definition (2.26) und Definition (2.33), an Stelle der Aufzählung tritt eine Parametrisierung durch die Elemente der Indexmenge I.
Umgekehrt lässt sich wie folgt zu jeder Menge eine Familie konstruieren:

(2.24) Bemerkung. Für jede Menge X haben wir die Familie $(x)_{x \in X}$ über X.

(2.25) Definition (leere Familie)**.** Die Familie über der leeren Menge $\emptyset$ wird *leere Familie* genannt und als $( )$ notiert.

Tupel

Die häufigsten Varianten von Familien tragen eigene Namen und Schreibweisen. Als nächstes betrachten wir Familien über einem „Anfangsstück“ der natürlichen Zahlen. Die „Anordnung“ dieser natürlichen Zahlen liefert eine naheliegende aufzählende Notation für solche Familien:

(2.26) Definition (Tupel)**.** Es sei $n \in \mathbb{N}_0$ gegeben.

(a) Ein *n-Tupel* ist eine Familie x über $[1, n]$. ([21]) Die nicht-negative ganze Zahl n wird *Länge* von x genannt. Für ein n-Tupel x schreiben wir auch

$$(x_1, \ldots, x_n) := x.$$

(b) Es sei eine Menge X gegeben. Die *Menge der n-Tupel* in X ist definiert als

$$X^n := X^{[1,n]}.$$

Ein Element von X^n wird *n-Tupel* in X genannt.

(2.27) Definition (leeres Tupel, Paar, Tripel, Quadrupel, Quintupel)**.**

(a) Das 0-Tupel wird auch das *leere Tupel* genannt.

(b) Ein 1-Tupel wird auch *Single* genannt.

(c) Ein 2-Tupel wird auch *Paar* genannt.

(d) Ein 3-Tupel wird auch *Tripel* genannt.

(e) Ein 4-Tupel wird auch *Quadrupel* genannt.

(f) Ein 5-Tupel wird auch *Quintupel* genannt.

(2.28) Beispiel.

(a) Es ist $(1, 2, 4)$ ein Tripel.

(b) Es ist $x = (x_i)_{i \in [1,9]}$ gegeben durch $x_i = i - i^2$ für $i \in [1, 9]$ ein 9-Tupel.

(c) Es ist $(\{1\}, \{2\})$ ein Paar.

[21] In manchen Texten werden auch Familien über $[0, n-1]$ als n-Tupel bezeichnet. Allgemeiner: Für $k \in \mathbb{Z}$ wird eine Familie über $[k+1, k+n]$ auch ein *durch* $[k+1, k+n]$ *indiziertes n-Tupel* genannt.

(d) Es gibt kein Quadrupel x in $\mathbb{Z}$ mit $x_2 = 0$ und $x_2 = 1$.

(2.29) Beispiel.

(a) Es sei ein Quadrupel x gegeben durch

$$x = (i^3)_{i\in[1,4]}.$$

Dann ist $x = (1, 8, 27, 64)$.

(b) Es ist $(3, \{4\}) \neq (\{4\}, 3)$.

(c) Es ist $(1, 2, 3) \neq (1, 2, 3, 2)$.

Beweis.

(a) Es ist

$$x = (i^3)_{i\in[1,4]} = (1^3, 2^3, 3^3, 4^3) = (1, 8, 27, 64).$$

(b) Es seien $x := (3, \{4\})$ und $y := (\{4\}, 3)$. Wegen

$$x_1 = 3 \neq \{4\} = y_1$$

gilt $x \neq y$.

(c) Es seien $x := (1, 2, 3)$ und $y := (1, 2, 3, 2)$. Da x ein Tripel, d.h. eine Familie über $[1, 3]$, und y ein Quadrupel, d.h. eine Familie über $[1, 4]$, ist und $[1, 3] \neq [1, 4]$ gilt, ist $x \neq y$. □

(2.30) Beispiel. Es ist

$$\{-1, 1\}^3 = \{(-1, -1, -1), (1, -1, -1), (-1, 1, -1), (1, 1, -1), (-1, -1, 1), (1, -1, 1), (-1, 1, 1), (1, 1, 1)\}.$$

(2.31) Anwendungsbeispiel.

(a) Eine (einfache) Belegung einer TV-Fernbedienung lässt sich als 9-Tupel auffassen. In Deutschland wird eine typische Belegung etwa durch das 9-Tupel

$$(\text{DasErste}, \text{ZDF}, \text{RTL}, \text{Sat1}, \text{ProSieben}, \text{RTL2}, \text{kabeleins}, \text{VOX}, \text{3sat})$$

modelliert.

(b) Ein Fotoalbum mit 64 Fotos lässt sich als 64-Tupel auffassen.

(c) Eine Beamerpräsentation mit 23 Folien lässt sich als 23-Tupel auffassen.

(d) Ein Speicher mit 256 Speicherplätzen lässt sich als 256-Tupel auffassen. ([22])

(e) Eine Ziehung der Lottozahlen lässt sich als 49-Tupel in $\{\text{gezogen}, \text{nicht gezogen}\}$ auffassen.

(2.32) Anwendungsbeispiel. Es sei $n \in \mathbb{N}_0$ gegeben. Eine Interpretation der Aussagenvariablen $A_1, \ldots, A_n$ lässt sich als n-Tupel in $\{0, 1\}$ modellieren. ([23])

Folgen

Bei diskreter Zeitmodellierung spielen Familien über den natürlichen Zahlen eine Rolle. Für diese führen wir nun eine eigene Terminologie ein:

(2.33) Definition (Folge)**.** Eine *Folge* ist eine Familie über $\mathbb{N}$. ([24])
Für eine Folge x schreiben wir auch

$$(x_1, x_2, x_3, \ldots) := x.$$

(2.34) Beispiel. Es ist $(2i)_{i\in\mathbb{N}} = (2, 4, 6, \ldots)$ eine Folge.

[22] In der Informatik würde man die Komponenten üblicherweise mit Elementen der Menge $[0, 255]$ indizieren und damit einen solchen Speicher eher als Familie über $[0, 255]$ auffassen.

[23] Die vereinbarte Notation aus Definition (1.7)(a) entspricht dann der Notation für Strings aus Definition (10.2).

[24] Gelegentlich werden auch Familien über $\mathbb{N}_0$ als Folgen bezeichnet. Allgemeiner: Für $a \in \mathbb{Z}$ seien $\mathbb{Z}_{\geq a} := \{x \in \mathbb{Z} \mid x \geq a\}$ und $\mathbb{Z}_{\leq a} := \{x \in \mathbb{Z} \mid x \leq a\}$. Eine Familie über $\mathbb{Z}_{\geq a}$ wird dann auch eine *durch* $\mathbb{Z}_{\geq a}$ *indizierte Folge* und eine Familie über $\mathbb{Z}_{\leq a}$ auch eine *durch* $\mathbb{Z}_{\leq a}$ *indizierte Folge* genannt.

Innere Mengenoperationen

Wir betrachten Mengenoperationen, d.h. Methoden, um Mengen aus gegebenen Mengen zu bilden. Hierbei beschränken wir uns in diesem Abschnitt auf sogenannte innere Mengenoperationen, d.h. solche, welche angewandt auf die Elemente einer Potenzmenge wieder ein Element dieser Potenzmenge ergeben.

(2.35) Definition (Differenz)**.** Es seien Mengen X und Y gegeben. Die Menge

$$X \setminus Y := \{x \mid x \in X \text{ und } x \notin Y\}$$

heißt *Differenz* (oder *Mengendifferenz*) von X und Y.

(2.36) Beispiel. Es ist

$$\{1,2,3\} \setminus \{2,4\} = \{1,3\},$$
$$\{2,4\} \setminus \{1,2,3\} = \{4\}.$$

(2.37) Definition (Schnitt, Vereinigung)**.**

(a) (i) Es seien eine nicht-leere Menge I und eine Familie von Mengen $X = (X_i)_{i \in I}$ über I ([25]) gegeben. Die Menge

$$\bigcap X = \bigcap_{i \in I} X_i := \{x \mid x \in X_i \text{ für } i \in I\}$$

heißt *Schnitt* (oder *Durchschnitt*) von X.

(ii) Es seien $n \in \mathbb{N}$ und ein n-Tupel von Mengen $(X_1, \ldots, X_n)$ gegeben. Wir schreiben auch

$$X_1 \cap \ldots \cap X_n := \bigcap X.$$

(iii) Es seien Mengen X und Y gegeben. Der Schnitt $X \cap Y$ von (X, Y) wird auch *Schnitt* (oder *Durchschnitt*) von X und Y genannt.

(b) (i) Es seien eine Menge I und eine Familie von Mengen $X = (X_i)_{i \in I}$ über I gegeben. Die Menge

$$\bigcup X = \bigcup_{i \in I} X_i := \{x \mid \text{es gibt ein } i \in I \text{ mit } x \in X_i\}$$

heißt *Vereinigung* von X.

(ii) Es seien $n \in \mathbb{N}_0$ und ein n-Tupel von Mengen $(X_1, \ldots, X_n)$ gegeben. Wir schreiben auch

$$X_1 \cup \ldots \cup X_n := \bigcup X.$$

(iii) Es seien Mengen X und Y gegeben. Die Vereinigung $X \cup Y$ von (X, Y) wird auch *Vereinigung* von X und Y genannt.

(2.38) Beispiel.

(a) (i) Es ist

$$\{1,2,3\} \cap \{2,4\} = \{2\}.$$

(ii) Es ist

$$\bigcap_{i \in \mathbb{N}} \{qi \mid q \in \mathbb{Z}\} = \{0\}.$$

(b) (i) Es ist

$$\{1,2,3\} \cup \{2,4\} = \{1,2,3,4\}.$$

[25] Wir nehmen also an, dass X_i für $i \in I$ stets eine Menge ist.

(ii) Es ist

$$\bigcup_{i\in\mathbb{N}} \{qi \mid q \in \mathbb{Z}\} = \mathbb{Z}.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(2.39) Bemerkung. Es seien $n \in \mathbb{N}_0$ und ein n-Tupel von Mengen $(X_1, \ldots, X_n)$ gegeben.

(a) Es sei $n \neq 0$. Dann ist

$$X_1 \cap \ldots \cap X_n = \{x \mid x \in X_1 \text{ und } \ldots \text{ und } x \in X_n\}.$$

(b) Es ist

$$X_1 \cup \ldots \cup X_n = \{x \mid x \in X_1 \text{ oder } \ldots \text{ oder } x \in X_n\}.$$

Im Folgenden studieren wir einige Verträglichkeiten von Schnitt- und Vereinigungsoperation untereinander.

(2.40) Bemerkung.

(a) (i) *Assoziativität des Schnitts.* Für alle Mengen X, Y, Z ist $X \cap (Y \cap Z) = (X \cap Y) \cap Z$.
(ii) *Assoziativität der Vereinigung.* Für alle Mengen X, Y, Z ist $X \cup (Y \cup Z) = (X \cup Y) \cup Z$.

(b) (i) *Neutrales Element des Schnitts von Teilmengen.* Für jede Menge X und jede Teilmenge U von X ist $U \cap X = U$.
(ii) *Neutrales Element der Vereinigung.* Für jede Menge X ist $X \cup \emptyset = X$.

(c) (i) *Kommutativität des Schnitts.* Für alle Mengen X, Y ist $X \cap Y = Y \cap X$.
(ii) *Kommutativität der Vereinigung.* Für alle Mengen X, Y ist $X \cup Y = Y \cup X$.

(d) (i) *Idempotenz des Schnitts.* Für jede Menge X ist $X \cap X = X$.
(ii) *Idempotenz der Vereinigung.* Für jede Menge X ist $X \cup X = X$.

(e) (i) *Distributivität.* Für alle Mengen X, Y, Z ist $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.
(ii) *Distributivität.* Für alle Mengen X, Y, Z ist $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$.

(f) (i) *Absorption.* Für alle Mengen X, Y ist $X \cap (X \cup Y) = X$.
(ii) *Absorption.* Für alle Mengen X, Y ist $X \cup (X \cap Y) = X$.

Beweis. Dies sei dem Leser zur Übung überlassen. Wir begnügen uns hier mit dem Beweis von (e)(i).

(e) (i) Für alle Mengen X, Y, Z ist

$$\begin{aligned} X \cap (Y \cup Z) &= \{x \mid x \in X \text{ und } x \in Y \cup Z\} = \{x \mid x \in X \text{ und } (x \in Y \text{ oder } x \in Z)\} \\ &= \{x \mid (x \in X \text{ und } x \in Y) \text{ oder } (x \in X \text{ und } x \in Z)\} \\ &= \{x \mid x \in X \cap Y \text{ oder } x \in X \cap Z\} = (X \cap Y) \cup (X \cap Z). \end{aligned}$$

□

(2.41) Definition (Disjunktheit)**.**

(a) Es seien eine Menge I und eine Familie von Mengen $X = (X_i)_{i\in I}$ über I gegeben. Wir sagen, dass X *disjunkt* ist, falls für $i, j \in I$ mit $i \neq j$ stets $X_i \cap X_j = \emptyset$ gilt.

(b) Es seien Mengen X und Y gegeben. Wir sagen, dass X und Y *disjunkt* sind, falls (X, Y) disjunkt ist.

(2.42) Beispiel. Es seien $X := \{1, 2, 4\}$, $Y := \{3, 6\}$, $Z := \{5, 6\}$.

(a) Die Menge X und Y sind disjunkt.

(b) Die Menge X und Z sind disjunkt.

(c) Die Mengen Y und Z sind nicht disjunkt.

Beweis.

(a) Es ist $\{1,2,4\} \cap \{3,6\} = \emptyset$.

(b) Es ist $\{1,2,4\} \cap \{5,6\} = \emptyset$.

(c) Es ist $\{3,6\} \cap \{5,6\} = \{6\} \neq \emptyset$. □

(2.43) Definition ((innere) disjunkte Vereinigung)**.**

(a) Es seien eine Menge I und eine Familie von Mengen $X = (X_i)_{i \in I}$ über I gegeben. Wenn X disjunkt ist, so sagen wir, dass $\bigcup X$ eine (*innere*) *disjunkte Vereinigung* von X ist, und schreiben

$$\dot{\bigcup} X = \dot{\bigcup_{i \in I}} X_i := \bigcup X.$$

(b) Es seien $n \in \mathbb{N}_0$ und ein disjunktes n-Tupel von Mengen $(X_1, \ldots, X_n)$ gegeben. Wir schreiben auch

$$X_1 \mathbin{\dot{\cup}} \cdots \mathbin{\dot{\cup}} X_n := \dot{\bigcup} X.$$

(c) Es seien disjunkte Mengen X und Y gegeben. Die disjunkte Vereinigung $X \mathbin{\dot{\cup}} Y$ von (X, Y) wird auch (*innere*) *disjunkte Vereinigung* von X und Y genannt.

(2.44) Beispiel. Es ist

$$\mathbb{N} = \{n \in \mathbb{N} \mid n \text{ ist gerade}\} \mathbin{\dot{\cup}} \{n \in \mathbb{N} \mid n \text{ ist ungerade}\}.$$

(2.45) Bemerkung. Für alle Mengen X und Y sind $X \setminus Y$ und $Y \setminus X$ disjunkt.

Beweis. Es seien Mengen X und Y gegeben. Für alle $x \in X \setminus Y$ gilt $x \notin Y$, also insbesondere auch $x \notin Y \setminus X$. Folglich ist $(X \setminus Y) \cap (Y \setminus X) = \emptyset$, d.h. $X \setminus Y$ und $Y \setminus X$ sind disjunkt. □

(2.46) Definition (symmetrische Differenz)**.** Es seien Mengen X und Y gegeben. Die Menge

$$X \mathbin{\triangle} Y := (X \setminus Y) \mathbin{\dot{\cup}} (Y \setminus X)$$

heißt *symmetrische Differenz* von X und Y.

(2.47) Beispiel. Es ist

$$\{1,2,3\} \mathbin{\triangle} \{1,4\} = \{2,3,4\}.$$

Beweis. Es ist

$$\{1,2,3\} \mathbin{\triangle} \{1,4\} = (\{1,2,3\} \setminus \{1,4\}) \mathbin{\dot{\cup}} (\{1,4\} \setminus \{1,2,3\}) = \{2,3\} \mathbin{\dot{\cup}} \{4\} = \{2,3,4\}.$$ □

Äußere Mengenoperationen

Schließlich führen wir das kartesische Produkt und die (äußere) disjunkte Vereinigung ein. Informell gesprochen stellt letztere eine Methode dar, um nicht disjunkte Mengen künstlich disjunkt zu machen.

(2.48) Definition (kartesisches Produkt, disjunkte Vereinigung)**.**

(a) (i) Es seien eine Menge I und eine Familie von Mengen $X = (X_i)_{i \in I}$ über I gegeben. Die Menge

$$\bigtimes X = \bigtimes_{i \in I} X_i := \{x \mid x = (x_i)_{i \in I} \text{ ist eine Familie über } I \text{ mit } x_i \in X_i \text{ für } i \in I\}$$

heißt *kartesisches Produkt* (oder *Mengenprodukt* oder *Produkt*) von X.

(ii) Es seien $n \in \mathbb{N}_0$ und ein n-Tupel von Mengen $(X_1, \ldots, X_n)$ gegeben. Wir schreiben auch

$$X_1 \times \ldots \times X_n := \bigtimes_{i \in [1,n]} X_i.$$

(iii) Es seien Mengen X und Y gegeben. Das kartesische Produkt $X \times Y$ von (X, Y) wird auch *kartesisches Produkt* (oder *Mengenprodukt* oder *Produkt*) von X und Y genannt.

(b) (i) Es seien eine Menge I und eine Familie von Mengen $X = (X_i)_{i \in I}$ über I gegeben. Die Menge

$$\bigsqcup X = \bigsqcup_{i \in I} X_i := \dot{\bigcup_{i \in I}} (X_i \times \{i\})$$

heißt *disjunkte Vereinigung* (oder *äußere disjunkte Vereinigung* oder *Mengenkoprodukt* oder *Koprodukt*) von X.

(ii) Es seien $n \in \mathbb{N}_0$ und ein n-Tupel von Mengen $(X_1, \ldots, X_n)$ gegeben. Wir schreiben auch

$$X_1 \sqcup \ldots \sqcup X_n := \bigsqcup_{i \in [1,n]} X_i.$$

(iii) Es seien Mengen X und Y gegeben. Die disjunkte Vereinigung $X \sqcup Y$ von (X, Y) wird auch *disjunkte Vereinigung* (oder *äußere disjunkte Vereinigung* oder *Mengenkoprodukt* oder *Koprodukt*) von X und Y genannt.

(2.49) Beispiel.

(a) Es ist

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

(b) Es ist

$$\{1,3,5,7,9\} \sqcup \{2,3,5,7\} = \{(1,1),(3,1),(5,1),(7,1),(9,1),(2,2),(3,2),(5,2),(7,2)\}.$$

Beweis.

(a) Es ist

$$\{1,2\} \times \{3,4,5\} = \{(x,y) \mid x \in \{1,2\} \text{ und } y \in \{3,4,5\}\} = \{(1,3),(1,4),(1,5),(2,3),(2,4),(2,5)\}.$$

(b) Es ist

$$\begin{aligned} \{1,3,5,7,9\} \sqcup \{2,3,5,7\} &= (\{1,3,5,7,9\} \times \{1\}) \,\dot\cup\, (\{2,3,5,7\} \times \{2\}) \\ &= \{(1,1),(3,1),(5,1),(7,1),(9,1)\} \,\dot\cup\, \{(2,2),(3,2),(5,2),(7,2)\} \\ &= \{(1,1),(3,1),(5,1),(7,1),(9,1),(2,2),(3,2),(5,2),(7,2)\}. \end{aligned}$$

□

Anwendung: Datenbanken

Als Anwendung der Konzepte einer Familie und eines kartesischen Produkts präsentieren wir ein mathematisches Modell für Datenbanken. ([26])

(2.50) Definition (Datenbank)**.** Es seien eine Menge A und eine Familie $(X_a)_{a \in A}$ von Mengen gegeben. Eine *Datenbank* mit Werten in $(X_a)_{a \in A}$ ist eine Teilmenge von $\bigtimes_{a \in A} X_a$.
Es sei eine Datenbank D mit Werten in $(X_a)_{a \in A}$ gegeben. Die Menge A wird *Attributmenge* von D genannt. Ein Element von A wird *Attribut* von D genannt. Für $a \in A$ wird X_a die *Domäne* (oder der *Wertebereich*) von D zum Attribut a genannt. Ein Element von D wird *Datensatz* von D genannt. Für $a \in A$, $x \in D$ wird x_a der *Attributwert* von x zum Attribut a genannt.

[26] Datenbanken werden an der RWTH Aachen im Rahmen des Kurses *Datenbanken und Informationssysteme* (etwa 4. Semester im Studiengang B.Sc. Informatik) studiert.

(2.51) Anwendungsbeispiel. Die Datenbank einer Vorlesung *Diskrete Strukturen* lässt sich als (formale) Datenbank mit der Attributmenge

$$A = \{\text{Matrikelnummer}, \text{Nachname}, \text{Vorname}, \text{Studiengang}, \text{Semester}, \text{E-Mail}, \text{Passwort}\}$$

und den Domänen

$$\begin{aligned}
X_{\text{Matrikelnummer}} &= [1, 999999],\\
X_{\text{Nachname}} &= \text{Strings},\\
X_{\text{Vorname}} &= \text{Strings},\\
X_{\text{Studiengang}} &= \{\texttt{Informatik (B.Sc.)}, \texttt{Informatik (LAB-GyGe)},\\
&\qquad \texttt{Informatik (M.Sc. Auflagenfach)}, \texttt{Technik-Kommunikation (B.Sc.)},\\
&\qquad \texttt{Computational Engineering Science (M.Sc.)}, \texttt{Verfahrenstechnik (M.Sc.)},\\
&\qquad \texttt{Schülerstudium}, \texttt{Sonstiges}\},\\
X_{\text{Semester}} &= [1, 99],\\
X_{\text{E-Mail}} &= \text{Strings},\\
X_{\text{Passwort}} &= \text{Strings}.
\end{aligned}$$

auffassen, wobei Strings ein Modell für die „Menge der Strings“ darstelle ([27]). Ein typischer Datensatz ist dann etwa gegeben durch

$$\begin{aligned}
x_{\text{Matrikelnummer}} &= 123456,\\
x_{\text{Nachname}} &= \texttt{Mustermann},\\
x_{\text{Vorname}} &= \texttt{Max},\\
x_{\text{Studiengang}} &= \texttt{Informatik (B.Sc.)},\\
x_{\text{Semester}} &= 1,\\
x_{\text{E-Mail}} &= \texttt{max.mustermann@rwth-aachen.de},\\
x_{\text{Passwort}} &= \texttt{qV8atM/dMY22g}.
\end{aligned}$$

Matrizen

Das binäre kartesische Produkt liefert eine neue Sorte von Familien, welche unter einem eigenen Namen bekannt sind:

(2.52) Definition (Matrix)**.** Es seien $m, n \in \mathbb{N}_0$ gegeben.

(a) Eine $(m \times n)$-*Matrix* (oder (m, n)-*Matrix*) ist eine Familie x über $[1, m] \times [1, n]$. Das Paar (m, n) wird *Format* von x genannt.

Für eine $(m \times n)$-Matrix x schreiben wir auch

$$\begin{pmatrix} x_{1,1} & \dots & x_{1,n} \\ \vdots & & \vdots \\ x_{m,1} & \dots & x_{m,n} \end{pmatrix} := (x_{i,j})_{i \in [1,m], j \in [1,n]} := x.$$

(b) Es sei eine Menge X gegeben. Die *Menge der* $(m \times n)$-*Matrizen* in X ist definiert als

$$X^{m \times n} := X^{[1,m] \times [1,n]}.$$

Ein Element von $X^{m \times n}$ wird $(m \times n)$-*Matrix* in X (oder $(m \times n)$-*Matrix* über X) genannt.

[27] Für eine mögliche Formalisierung siehe Definition (10.2).

(2.53) Beispiel.

(a) Es ist

$$\begin{pmatrix} -1 & 3 & 1 & 2 \\ 2 & 2 & -5 & 0 \\ 1 & 2 & 3 & 1 \end{pmatrix}$$

eine (3×4)-Matrix.

(b) Es ist $x = (x_{i,j})_{i \in [1,8], j \in [1,3]}$ gegeben durch

$$x_{i,j} = i^3 j^2$$

für $i \in [1,8]$, $j \in [1,3]$ eine (8×3)-Matrix in $\mathbb{N}$.

(c) Es ist

$$\begin{pmatrix} \{1\} & \{\{\emptyset\}\} \\ \sqrt{3} & (-2)^5 \end{pmatrix}$$

eine (2×2)-Matrix.

(2.54) Beispiel.

(a) Es sei eine (3×2)-Matrix x gegeben durch

$$x = (ij - j)_{i \in [1,3], j \in [1,2]}.$$

Dann ist

$$x = \begin{pmatrix} 0 & 0 \\ 1 & 2 \\ 2 & 4 \end{pmatrix}.$$

(b) Es ist

$$\begin{pmatrix} 1 \\ -2 \end{pmatrix} \neq \begin{pmatrix} -2 \\ 1 \end{pmatrix}.$$

(c) Es ist

$$\begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \end{pmatrix} \neq \begin{pmatrix} 2 & 2 \\ 2 & 2 \\ 2 & 2 \end{pmatrix}.$$

Beweis.

(a) Es ist

$$x = (ij - j)_{i \in [1,3], j \in [1,2]} = \begin{pmatrix} 1 \cdot 1 - 1 & 1 \cdot 2 - 2 \\ 2 \cdot 1 - 1 & 2 \cdot 2 - 2 \\ 3 \cdot 1 - 1 & 3 \cdot 2 - 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 2 \\ 2 & 4 \end{pmatrix}.$$

(b) Es seien

$$x := \begin{pmatrix} 1 \\ -2 \end{pmatrix}, \; y := \begin{pmatrix} -2 \\ 1 \end{pmatrix}.$$

Wegen

$$x_{1,1} = 1 \neq -2 = y_{1,1}$$

gilt $x \neq y$.

(c) Es seien

$$x := \begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \end{pmatrix}, \; y := \begin{pmatrix} 2 & 2 \\ 2 & 2 \\ 2 & 2 \end{pmatrix}.$$

Da x eine (2×3)-Matrix, d.h. eine Familie über $[1,2] \times [1,3]$, und y eine (3×2)-Matrix, d.h. eine Familie über $[1,3] \times [1,2]$, ist und $[1,2] \times [1,3] \neq [1,3] \times [1,2]$ gilt, ist $x \neq y$. □

(2.55) Beispiel. Es ist

$$\begin{aligned} \{1,3\}^{2\times 2} = \{&\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}, \\ &\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}\}. \end{aligned}$$

(2.56) Anwendungsbeispiel. Eine Situation in einem Schachspiel lässt sich als (8×8)-Matrix auffassen. Die Anfangssituation wird etwa durch die (8×8)-Matrix

$$\begin{pmatrix} \text{WT} & \text{WS} & \text{WL} & \text{WD} & \text{WK} & \text{WL} & \text{WS} & \text{WT} \\ \text{WB} & \text{WB} & \text{WB} & \text{WB} & \text{WB} & \text{WB} & \text{WB} & \text{WB} \\ \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} \\ \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} \\ \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} \\ \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} & \text{leer} \\ \text{SB} & \text{SB} & \text{SB} & \text{SB} & \text{SB} & \text{SB} & \text{SB} & \text{SB} \\ \text{ST} & \text{SS} & \text{SL} & \text{SD} & \text{SK} & \text{SL} & \text{SS} & \text{ST} \end{pmatrix}$$

modelliert. ([28])

Matrizen werden unter anderem zur knappen Beschreibung linearer Gleichungssysteme genutzt, siehe Abschnitt 16. Allgemeiner dienen Matrizen und die in Abschnitt 15 einzuführende Arithmetik der Beschreibung von Homomorphismen zwischen endlichdimensionalen Vektorräumen [18, Abschn. 3]. ([29])
Bei Matrizen, welche nur aus genau einer Zeile oder genau einer Spalte bestehen, lassen wir unter Missbrauch von Notationen den jeweils zweiten Index für die Einträge weg:

(2.57) Notation. Es sei $n \in \mathbb{N}_0$ gegeben.

(a) Es sei eine $(n \times 1)$-Matrix x gegeben. Wir schreiben $x_i := x_{i,1}$ für $i \in [1,n]$ sowie

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := (x_i)_{i\in[1,n]} := x.$$

(b) Es sei eine $(1 \times n)$-Matrix x gegeben. Wir schreiben $x_i := x_{1,i}$ für $i \in [1,n]$ sowie

$$\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix} := (x_i)_{i\in[1,n]} := x.$$

(2.58) Definition (Zeile, Spalte)**.** Es seien $m, n \in \mathbb{N}_0$ und eine $(m \times n)$-Matrix x gegeben.

(a) Für $i \in [1,m]$ heißt die $(1 \times n)$-Matrix $x_{i,-}$ gegeben durch

$$x_{i,-} = (x_{i,j})_{j\in[1,n]}$$

die *i-te Zeile* von x.

[28] Die bildliche Darstellung hier ist anders als bei einem klassischen Schachbrett, da in einer Matrix die Zeilen „von oben nach unten“ nummeriert sind, während die Nummerierung auf einem Schachbrett „von unten nach oben“ erfolgt. Die weiße Dame steht zu Beginn auf der Position d1, also in der Spalte mit der Beschriftung d und der Zeile mit der Beschriftung 1. Unter der kanonischen Abzählung $[1,8] \to \{\text{a}, \dots, \text{h}\}$, $1 \mapsto \text{a}$, $\dots$, $8 \mapsto \text{h}$, siehe Definition (3.41)(b), entspricht dies der Stelle $(1,4)$.

[29] Vektorräume und ihre Homomorphismen werden in Vorlesungen über *lineare Algebra* behandelt; an der RWTH Aachen bspw. im Kurs *Lineare Algebra für Informatiker* (etwa 2. Semester im Studiengang B.Sc. Informatik).

(b) Für $j \in [1,n]$ heißt die $(m \times 1)$-Matrix $x_{-,j}$ gegeben durch

$$x_{-,j} = (x_{i,j})_{i \in [1,m]}$$

die *j-te Spalte* von x.

(2.59) Beispiel. Es sei

$$x := \begin{pmatrix} 1 & 0 & -2 \\ 2 & -1 & 3 \end{pmatrix}.$$

(a) Es ist

$$x_{1,-} = \begin{pmatrix} 1 & 0 & -2 \end{pmatrix},\ x_{2,-} = \begin{pmatrix} 2 & -1 & 3 \end{pmatrix}.$$

(b) Es ist

$$x_{-,1} = \begin{pmatrix} 1 \\ 2 \end{pmatrix},\ x_{-,2} = \begin{pmatrix} 0 \\ -1 \end{pmatrix},\ x_{-,3} = \begin{pmatrix} -2 \\ 3 \end{pmatrix}.$$

Schließlich legen wir noch eine einfache Notation für „aneinandergehängte“ Matrizen fest:

(2.60) Notation. Es seien $m, n, p, q \in \mathbb{N}_0$ und eine $(m \times n)$-Matrix a, eine $(m \times q)$-Matrix b, eine $(p \times n)$-Matrix c und eine $(p \times q)$-Matrix d gegeben. Die $((m+p) \times (n+q))$-Matrix x gegeben durch

$$x_{i,j} = \begin{cases} a_{i,j} & \text{für } (i,j) \in [1,m] \times [1,n], \\ b_{i,j-n} & \text{für } (i,j) \in [1,m] \times [n+1, n+q], \\ c_{i-m,j} & \text{für } (i,j) \in [m+1, m+p] \times [1,n], \\ d_{i-m,j-n} & \text{für } (i,j) \in [m+1, m+p] \times [n+1, n+q], \end{cases}$$

notieren wir als

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \left(\begin{array}{c|c} a & b \\ \hline c & d \end{array}\right) := x.$$

Ähnlich für andere Zusammensetzungen.

3 Abbildungen

In diesem Abschnitt führen wir Abbildungen zwischen Mengen ein. Während Mengen von der Vorstellung her starre Gebilde sind, stellen wir uns unter einer Abbildung eine „Vorschrift“ vor, welche die Elemente einer Menge eindeutig auf gewisse Elemente einer anderen Menge „abbildet“.
Der Abschnitt beginnt mit der Definition einer Abbildung, zugehörigen Notationen und Beispielen sowie dem Zusammenhang zwischen Abbildungen und Familien. Danach werden zunächst die algebraischen Konzepte von Komposition und Invertierbarkeit und danach die mengentheoretisch, qualitativ beschreibenden Konzepte der Injektivität und Surjektivität sowie des Bildes und Urbildes von Teilmengen behandelt. Das wichtigste Resultat ist Satz (3.29), welcher einen Zusammenhang zwischen den Konzepten liefert. Im Anschluss werden Abbildungskonzepte im Zusammenhang mit Teilmengen wie Restriktion und Indikatorabbildungen eingeführt. Zum Schluss des Abschnitts werden schließlich die Endlichkeit und die Kardinalität von Mengen studiert.

Begriffsbildung

In der Mathematik ist es allgemein üblich, neue Begriffe auf bereits bekannte Begriffe zurückzuführen. Auch wenn wir uns unter einer Abbildung etwas anderes vorstellen werden als unter einer Menge, werden wir nun zunächst den Abbildungsbegriff mit Hilfe des Mengenbegriffs definieren. Oder anders ausgedrückt: wir wollen unsere intuitive Vorstellung von einer Abbildung mit Hilfe von Mengen „modellieren“. Dies hätten wir bereits beim Konzept einer Familie, siehe (2.16), machen können; allerdings ist hierbei die Formalisierung auf den ersten Blick weniger einsichtig.
Aus der Schule sind uns Funktionen von $\mathbb{R}$ nach $\mathbb{R}$ vertraut. Diese veranschaulichen wir anhand eines „Graphen“, welchen wir als Teilmenge der Ebene $\mathbb{R} \times \mathbb{R}$ auffassen können. Für eine allgemeine Abbildung ersetzen wir nun $\mathbb{R}$ durch beliebige Mengen und nehmen die beschreibende Teilmenge als Bestandteil der Definition:

(3.1) Definition (Abbildung)**.**

(a) Eine *Abbildung* (oder *Funktion*) besteht aus Mengen X und Y zusammen mit einer Teilmenge f von $X \times Y$ so, dass es für jedes $x \in X$ genau ein $y \in Y$ mit $(x, y) \in f$ gibt. Unter Missbrauch der Notation bezeichnen wir sowohl die besagte Abbildung als auch die Teilmenge von $X \times Y$ mit f. Die Menge X wird *Startmenge* (oder *Definitionsbereich*) von f genannt. Ein Element von X wird *Argument* von f genannt. Die Menge Y wird *Zielmenge* (oder *Wertebereich*) von f genannt. Ein Element von Y wird *Zielwert* (oder *Zielelement*) von f genannt.

Für eine Abbildung f mit Startmenge X und Zielmenge Y schreiben wir $\operatorname{Source} f := X$ und $\operatorname{Target} f := Y$. Für $x \in X$ heißt das Element $y \in Y$ mit $(x, y) \in f$ das *Bild* (oder *Bildelement*) von x unter f, wir schreiben $f(x) := y$. Für $y \in Y$, $x \in X$ mit $y = f(x)$ wird x ein *Urbild* (oder *Urbildelement*) von y unter f genannt.

(b) Es seien Mengen X und Y gegeben. Die *Menge der Abbildungen* von X nach Y ist definiert als

$$\operatorname{Map}(X, Y) := \{f \mid f \text{ ist eine Abbildung mit } \operatorname{Source} f = X \text{ und } \operatorname{Target} f = Y\}.$$

Ein Element von $\operatorname{Map}(X, Y)$ wird *Abbildung* von X nach Y genannt; wir schreiben $f\colon X \to Y$ sowie $f\colon X \to Y$, $x \mapsto f(x)$ für $f \in \operatorname{Map}(X, Y)$.

Wir betonen, dass in der vorangegangenen Definition $f \neq f(x)$ ist. Während f eine Abbildung angibt, bezeichnet $f(x)$ für $x \in X$ das Bildelement von x unter f, also ein Element von Y.

(3.2) Beispiel.

(a) Es ist $\{1, 2, 3\} \to \{4, 5, 6\}$, $1 \mapsto 4$, $2 \mapsto 5$, $3 \mapsto 4$ eine Abbildung.

(b) Es ist $\mathbb{Z} \to \mathbb{Q}$, $x \mapsto 2x^2$ eine Abbildung.

(c) Es gibt keine Abbildung $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(x) = \sqrt{x}$ für alle $x \in \mathbb{N}$.

(d) Es gibt keine Abbildung $f\colon \{-2, 3, \sqrt{61}\} \to \mathbb{Q}$ mit $f(3) = -5$ und $f(3) = \frac{2}{7}$.

(e) Die Teilmenge $\{(x, \frac{1}{x}) \mid x \in \mathbb{R} \setminus \{0\}\}$ von $\mathbb{R} \times \mathbb{R}$ liefert keine Abbildung von $\mathbb{R}$ nach $\mathbb{R}$.

(f) Es ist $f\colon \mathbb{R} \to \mathbb{R}$ gegeben durch

$$f(x) = \begin{cases} \frac{1}{x}, & \text{für } x \in \mathbb{R} \setminus \{0\}, \\ 0, & \text{für } x = 0 \end{cases}$$

eine Abbildung.

Beweis.

(c) Es ist etwa $\sqrt{2} \notin \mathbb{N}$.

(d) Es ist $-5 \neq \frac{2}{7}$ in $\mathbb{Q}$. □

In den Fällen von Beispiel (3.2)(c), (d) sagen wir auch, dass solche Abbildungen nicht *wohldefiniert* wären.

(3.3) Beispiel. Es ist

$$\begin{aligned}\operatorname{Map}(\{1, 2\}, \{3, 4, 5\}) = \{&(1 \mapsto 3, 2 \mapsto 3), (1 \mapsto 3, 2 \mapsto 4), (1 \mapsto 3, 2 \mapsto 5), (1 \mapsto 4, 2 \mapsto 3), (1 \mapsto 4, 2 \mapsto 4), \\ &(1 \mapsto 4, 2 \mapsto 5), (1 \mapsto 5, 2 \mapsto 3), (1 \mapsto 5, 2 \mapsto 4), (1 \mapsto 5, 2 \mapsto 5)\},\end{aligned}$$

wobei wir etwa $(1 \mapsto 3, 2 \mapsto 3)$ als Kurzschreibweise für die Abbildung $\{1, 2\} \to \{3, 4, 5\}$, $1 \mapsto 3$, $2 \mapsto 3$ verwendet haben. ([30])

Wir betrachten noch einige Modellierungen von alltäglichen Zuordnungen:

[30] Start- und Zielmenge der jeweiligen Abbildungen sind bereits durch die Bezeichnung $\operatorname{Map}(\{1, 2\}, \{3, 4, 5\})$ festgelegt. Würden wir eine Menge betrachten, deren Elemente Abbildungen mit verschieden Start- und/oder Zielmengen sind, so müssten wir die jeweiligen Start- und Zielmengen der Elemente natürlich angeben.

(3.4) Anwendungsbeispiel.

(a) Der Briefpostversand der Aachener Post (an einem festgelegten Tag) lässt sich als Abbildung auffassen, bei der die Elemente der Startmenge die abgegebenen Briefe und die Elemente der Zielmenge die Postadressen modellieren.

(b) Eine Nachrichtenverschlüsselung lässt sich als Abbildung auffassen, bei der die Elemente der Startmenge die Klartexte und die Elemente der Zielmenge die Geheimtexte modellieren. Eine Nachrichtenentschlüsselung lässt sich als Abbildung auffassen, bei der die Elemente der Startmenge die Geheimtexte und die Elemente der Zielmenge die Klartexte modellieren.

(c) Ein Ticketverkauf zu einer Filmvorstellung lässt sich als Abbildung auffassen, bei der die Elemente der Startmenge die Sitzplätze und die Elemente der Zielmenge die Menschen modellieren.

(3.5) Anwendungsbeispiel. Es sei $n \in \mathbb{N}_0$ gegeben. Eine potentielle Wahrheitstafel für die Aussagenvariablen $A_1, \ldots, A_n$ lässt sich als Abbildung von $\{0,1\}^n$ nach $\{0,1\}$ ([31]) modellieren.

(3.6) Bemerkung (Gleichheitskriterium für Abbildungen)**.** Es seien Abbildungen $f\colon X \to Y$ und $f'\colon X' \to Y'$ gegeben. Genau dann gilt $f = f'$, wenn $X = X'$, $Y = Y'$ und $f(x) = f'(x)$ in Y für alle $x \in X$ ist.

Beweis. Als Teilmenge von $X \times Y$ ist $f = \{(x, f(x)) \mid x \in X\} := \{z \mid \text{es gibt ein } x \in X \text{ mit } z = (x, f(x))\}$, und als Teilmenge von $X' \times Y'$ ist $f' = \{(x', f'(x')) \mid x' \in X'\}$. Nun gilt $f = f'$ als Abbildungen genau dann, wenn $X = X'$, $Y = Y'$ und $f = f'$ als Teilmenge von $X \times Y = X' \times Y'$ ist. Letzteres ist aber äquivalent zu $\{(x, f(x)) \mid x \in X\} = \{(x', f'(x')) \mid x' \in X'\} = \{(x, f'(x)) \mid x \in X\}$. Schließlich sind diese Mengen genau dann gleich, wenn für $x \in X$ stets $f(x) = f'(x)$ gilt. □

(3.7) Beispiel.

(a) Es seien $f\colon \{1,2,3\} \to \mathbb{N}$, $x \mapsto x+2$ und $f'\colon \{1,2,3\} \to \mathbb{N}$, $1 \mapsto 3$, $2 \mapsto 4$, $3 \mapsto 5$. Dann ist $f = f'$.

(b) Es sei eine Abbildung $f\colon \mathbb{R} \to \mathbb{R}$ gegeben durch

$$f(x) = \begin{cases} \frac{1}{x+1}, & \text{für } x \in \mathbb{R} \setminus \{-1\}, \\ 0, & \text{für } x = -1. \end{cases}$$

Ferner sei eine Abbildung $f'\colon \mathbb{R} \to \mathbb{R}$ gegeben durch

$$f'(x) = \begin{cases} \frac{1}{x+1}, & \text{für } x \in \mathbb{R} \setminus \{-1\}, \\ -1, & \text{für } x = -1. \end{cases}$$

Dann ist $f \neq f'$.

(c) Es seien $f\colon \mathbb{N}_0 \to \mathbb{N}_0$, $x \mapsto x^2$ und $f'\colon \mathbb{Z} \to \mathbb{N}_0$, $x \mapsto x^2$. Dann ist $f \neq f'$.

(d) Es seien $f\colon \mathbb{N}_0 \to \mathbb{N}$, $x \mapsto x+1$ und $f'\colon \mathbb{N}_0 \to \mathbb{Z}$, $x \mapsto x+1$. Dann ist $f \neq f'$.

Beweis.

(a) Es ist $\operatorname{Source} f = \{1,2,3\} = \operatorname{Source} f'$ und $\operatorname{Target} f = \mathbb{N} = \operatorname{Target} f'$. Wegen

$$\begin{aligned} f(1) &= 1+2 = 3 = f'(1), \\ f(2) &= 2+2 = 4 = f'(2), \\ f(3) &= 3+2 = 5 = f'(3) \end{aligned}$$

ist daher $f = f'$ nach dem Gleichheitskriterium für Abbildungen (3.6).

(b) Wegen

$$f(-1) = 0 \neq -1 = f(-1)$$

ist $f \neq f'$ nach dem Gleichheitskriterium für Abbildungen (3.6).

[31] Eine solche Abbildung wird auch *Boolesche Funktion* genannt.

(c) Wegen

$$\text{Source } f = \mathbb{N}_0 \neq \mathbb{Z} = \text{Source } f'$$

ist $f \neq f'$ nach dem Gleichheitskriterium für Abbildungen (3.6).

(d) Wegen

$$\text{Target } f = \mathbb{N} \neq \mathbb{Z} = \text{Target } f'$$

ist $f \neq f'$ nach dem Gleichheitskriterium für Abbildungen (3.6). □

Zusammenhang zu Familien

Zwischen Abbildungen und Familien besteht ein enger Zusammenhang:

(3.8) Bemerkung. Es seien Mengen X und I gegeben.

(a) Es sei eine Familie x in X über I gegeben. Dann ist $I \to X$, $i \mapsto x_i$ eine Abbildung.

(b) Es sei eine Abbildung $f\colon I \to X$ gegeben. Dann ist $(f(i))_{i\in I}$ eine Familie.

Obwohl es einen formalen Unterschied zwischen Abbildungen und Familien gibt (insbesondere gehören Start- und Zielmenge zu einer gegebenen Abbildung, die Menge in welcher die Einträge einer Familie liegen jedoch nicht zu einer Familie), fassen wir Familien hin und wieder als Abbildungen auf, und umgekehrt ebenso.

(3.9) Konvention. Es seien Mengen X und I gegeben.

(a) Es sei eine Familie x in X über I gegeben. Unter Missbrauch der Notation bezeichnen wir die Abbildung $I \to X$, $i \mapsto x_i$ wieder als x.

(b) Es sei eine Abbildung $f\colon I \to X$ gegeben. Unter Missbrauch der Notation bezeichnen wir die Familie $(f(i))_{i\in I}$ wieder als f.

Komposition von Abbildungen

Als nächstes wollen wir gleich mehrere Abbildungen auf einmal betrachten. Haben wir Abbildungen f und g so gegeben, dass die Zielmenge von f gleich der Startmenge von g ist, so können wir diese Abbildungen nacheinander ausführen, d.h. wir können sie komponieren:

(3.10) Definition (Kompositum)**.** Es seien Abbildungen $f\colon X \to Y$ und $g\colon Y \to Z$ gegeben. Die Abbildung

$$g \circ f\colon X \to Z,\ x \mapsto g(f(x))$$

heißt *Kompositum* von f und g.

(3.11) Beispiel. Es seien $f\colon \mathbb{N} \to \mathbb{Z}$, $x \mapsto x+1$ und $g\colon \mathbb{Z} \to \mathbb{Q}$, $y \mapsto 2y^2$. Dann ist $g \circ f\colon \mathbb{N} \to \mathbb{Q}$, $x \mapsto 2(x+1)^2$.

Beweis. Für $x \in \mathbb{N}$ ist

$$g(f(x)) = g(x+1) = 2(x+1)^2.$$ □

(3.12) Bemerkung. Es seien Abbildungen $f\colon X \to Y$, $g\colon Y \to Z$, $h\colon Z \to A$ gegeben. Dann gilt

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

Beweis. Es sind $h \circ (g \circ f)$ und $(h \circ g) \circ f$ Abbildungen von X nach A. Für alle $x \in X$ gilt außerdem

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

Nach dem Gleichheitskriterium für Abbildungen (3.6) haben wir daher $h \circ (g \circ f) = (h \circ g) \circ f$. □

(3.13) Konvention. Da es nach Bemerkung (3.12) bei der iterierten Bildung von Komposita nicht auf die Klammerung ankommt, lassen wir die Klammern im Folgenden meist weg.

Wir werden nun sehen, dass es möglich ist, für jede Menge X mindestens eine Abbildung $X \to X$ hinzuschreiben, egal welche Elemente X besitzt.

(3.14) Definition (Identität)**.** Es sei eine Menge X gegeben. Die Abbildung

$$\mathrm{id} = \mathrm{id}_X \colon X \to X,\ x \mapsto x$$

heißt *Identität* (oder *identische Abbildung*) auf X.

(3.15) Beispiel. Die Identität auf $\{1,2,3\}$ ist gegeben durch

$$\mathrm{id}_{\{1,2,3\}} \colon \{1,2,3\} \to \{1,2,3\},\ 1 \mapsto 1,\ 2 \mapsto 2,\ 3 \mapsto 3.$$

(3.16) Bemerkung. Für jede Abbildung $f \colon X \to Y$ gilt

$$f \circ \mathrm{id}_X = \mathrm{id}_Y \circ f = f.$$

Beweis. Es sei eine Abbildung $f \colon X \to Y$ gegeben. Dann sind $f \circ \mathrm{id}_X$ und $\mathrm{id}_Y \circ f$ auch Abbildungen von X nach Y. Für alle $x \in X$ gilt außerdem

$$(f \circ \mathrm{id}_X)(x) = f(\mathrm{id}_X(x)) = f(x),$$
$$(\mathrm{id}_Y \circ f)(x) = \mathrm{id}_Y(f(x)) = f(x).$$

Nach dem Gleichheitskriterium für Abbildungen (3.6) gilt daher $f \circ \mathrm{id}_X = f$ und $\mathrm{id}_Y \circ f = f$. □

Schließlich wollen wir zu einer gegebenen Abbildung f solche Abbildungen g betrachten, welche durch Komposition mit f eine Identität liefern. Da die Identität einer Menge, anschaulich gesprochen, mit den Elementen dieser Menge nichts macht, macht g also die Abbildung f „rückgängig“ und umgekehrt.

(3.17) Definition (Invertierbarkeit von Abbildungen)**.** Es sei eine Abbildung $f \colon X \to Y$ gegeben.

(a) Eine *Inverse* (oder *inverse Abbildung* oder *Umkehrabbildung*) zu f ist eine Abbildung $g \colon Y \to X$ derart, dass $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$ gilt.

(b) Die Abbildung f heißt *invertierbar*, falls es eine Inverse zu f gibt.

(3.18) Beispiel. Es seien $\mathbb{Q}_{>0} := \{x \in \mathbb{Q} \mid x > 0\}$ und $\mathbb{Q}_{<0} := \{x \in \mathbb{Q} \mid x < 0\}$.

(a) Es seien $f \colon \mathbb{Q}_{>0} \to \mathbb{Q}_{<0},\ x \mapsto -2x$ und $g \colon \mathbb{Q}_{<0} \to \mathbb{Q}_{>0},\ y \mapsto -\frac{1}{2}y$. Dann ist g eine zu f inverse Abbildung.

(b) Es seien $h \colon \mathbb{Q}_{>0} \to \mathbb{Q}_{<0},\ x \mapsto -x$ und $k \colon \mathbb{Q}_{<0} \to \mathbb{Q}_{>0},\ y \mapsto -y$. Dann ist k eine zu h inverse Abbildung.

(c) Die Abbildung $l \colon \mathbb{Q} \to \mathbb{Q},\ x \mapsto -x$ ist zu sich selbst invers.

Beweis.

(a) Für $x \in \mathbb{Q}_{>0}$ ist

$$g(f(x)) = g(-2x) = -\frac{1}{2}(-2x) = x,$$

und für $y \in \mathbb{Q}_{<0}$ ist

$$f(g(y)) = f(-\frac{1}{2}y) = -2(-\frac{1}{2}y) = y.$$

Nach dem Gleichheitskriterium für Abbildungen (3.6) gilt daher $g \circ f = \mathrm{id}_{\mathbb{Q}_{>0}}$ und $f \circ g = \mathrm{id}_{\mathbb{Q}_{<0}}$, d.h. es ist g eine zu f inverse Abbildung. □

(3.19) Bemerkung. Es sei eine Abbildung $f \colon X \to Y$ gegeben. Dann gibt es höchstens eine Inverse zu f.

Beweis. Es seien $g \colon Y \to X$ und $g' \colon Y \to X$ zu f inverse Abbildungen. Nach Bemerkung (3.16) gilt dann

$$g = g \circ \mathrm{id}_Y = g \circ f \circ g' = \mathrm{id}_X \circ g' = g'.$$ □

Da wir nun wissen, dass die zu einer gegebenen Abbildung f inverse Abbildung, sofern sie existiert, eindeutig durch f festgelegt ist, können wir ihr eine feste Bezeichnung (in Abhängigkeit von f) geben:

(3.20) Notation. Die zu einer invertierbaren Abbildung $f\colon X \to Y$ gegebene inverse Abbildung notieren wir als $f^{-1}\colon Y \to X$.

(3.21) Proposition.

(a) Es seien invertierbare Abbildungen $f\colon X \to Y$ und $g\colon Y \to Z$ gegeben. Dann ist auch $g \circ f\colon X \to Z$ invertierbar mit

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

(b) Es sei eine Menge X gegeben. Die Identität $\mathrm{id}_X\colon X \to X$ ist eine invertierbare Abbildung mit

$$\mathrm{id}_X^{-1} = \mathrm{id}_X.$$

(c) Es sei eine invertierbare Abbildung $f\colon X \to Y$ gegeben. Dann ist auch $f^{-1}\colon Y \to X$ invertierbar mit

$$(f^{-1})^{-1} = f.$$

Beweis.

(a) Da f invertierbar ist, gilt $f^{-1} \circ f = \mathrm{id}_X$ und $f \circ f^{-1} = \mathrm{id}_Y$. Ferner, da g invertierbar ist, gilt $g^{-1} \circ g = \mathrm{id}_Y$ und $g \circ g^{-1} = \mathrm{id}_Z$. Nach Bemerkung (3.16) ist also

$$f^{-1} \circ g^{-1} \circ g \circ f = f^{-1} \circ \mathrm{id}_Y \circ f = f^{-1} \circ f = \mathrm{id}_X,$$
$$g \circ f \circ f^{-1} \circ g^{-1} = g \circ \mathrm{id}_Y \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_Z.$$

Somit ist $g \circ f$ invertierbar mit $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

(b) Nach Bemerkung (3.16) gilt $\mathrm{id}_X \circ \mathrm{id}_X = \mathrm{id}_X$. Folglich ist id_X invertierbar mit $\mathrm{id}_X^{-1} = \mathrm{id}_X$.

(c) Da $f^{-1}\colon Y \to X$ zu f invers ist, gilt $f^{-1} \circ f = \mathrm{id}_X$ und $f \circ f^{-1} = \mathrm{id}_Y$. Dann ist aber auch $f \circ f^{-1} = \mathrm{id}_Y$ und $f^{-1} \circ f = \mathrm{id}_X$, d.h. es ist f^{-1} invertierbar mit $(f^{-1})^{-1} = f$. □

Für iterierte Komposita verwenden wir folgende vereinfachte Schreibweise. ([32])

(3.22) Notation. Es sei eine Abbildung $f\colon X \to X$ gegeben. Für $k \in \mathbb{N}_0$ setzen wir

$$f^k := \begin{cases} \mathrm{id}_X, & \text{falls } k = 0, \\ f \circ f^{k-1}, & \text{falls } k > 0. \end{cases}$$

Wenn f invertierbar ist, so setzen wir

$$f^{-k} := (f^{-1})^k$$

für $k \in \mathbb{N}$.

Injektivität und Surjektivität

Bisher haben wir Abbildungen unter algebraischen Gesichtspunkten studiert, d.h. wir haben Abbildungen komponiert und Eigenschaften der Komposition und der damit verwandten Begriffe wie Identität und Inverse betrachtet. Als nächstes wollen wir Abbildungen mehr unter qualitativen, rein mengentheoretischen Gesichtspunkten verstehen. Wir wollen also Fragen nach dem „Aussehen“ einer Abbildung, d.h. nach ihrem Verhalten gegenüber den Elementen und Teilmengen von Start- und Zielmenge, untersuchen. Der Höhepunkt wird schließlich Satz (3.29) sein, welcher die algebraische und die mengentheoretische Sichtweise miteinander verknüpft.

[32] Bzgl. Komposition wird für jede Menge X die Menge der Abbildungen $\mathrm{Map}(X, X)$ ein Monoid, siehe Bemerkung (6.22) und Definition (6.17). Die Potenznotation in (3.22) entspricht dann gerade der Potenznotation in abstrakten (multiplikativ geschriebenen) Monoiden, siehe Notation (9.13)(a). Insbesondere handelt es sich um eine rekursive Definition, vgl. den Rekursionssatz (9.5).

(3.23) Definition (injektiv, surjektiv)**.** Es seien Mengen X und Y gegeben.

(a) Die *Menge der injektiven Abbildungen* von X nach Y ist definiert als

$$\mathrm{Map}_{\mathrm{inj}}(X,Y) := \{f \in \mathrm{Map}(X,Y) \mid \text{für } x,x' \in X \text{ folgt aus } f(x) = f(x') \text{ stets } x = x'\}.$$

Ein Element von $\mathrm{Map}_{\mathrm{inj}}(X,Y)$ wird *injektive* Abbildung von X nach Y genannt.

(b) Die *Menge der surjektiven Abbildungen* von X nach Y ist definiert als

$$\mathrm{Map}_{\mathrm{surj}}(X,Y) := \{f \in \mathrm{Map}(X,Y) \mid \text{für } y \in Y \text{ gibt es ein } x \in X \text{ mit } y = f(x)\}.$$

Ein Element von $\mathrm{Map}_{\mathrm{surj}}(X,Y)$ wird *surjektive* Abbildung von X nach Y genannt.

(c) Die *Menge der bijektiven Abbildungen* von X nach Y ist definiert als

$$\mathrm{Map}_{\mathrm{bij}}(X,Y) := \mathrm{Map}_{\mathrm{inj}}(X,Y) \cap \mathrm{Map}_{\mathrm{surj}}(X,Y).$$

Ein Element von $\mathrm{Map}_{\mathrm{bij}}(X,Y)$ wird *bijektive* Abbildung von X nach Y genannt.

Eine Abbildung $f\colon X \to Y$ ist also injektiv, wenn sie verschiedene Elemente in X stets auf verschiedene Elemente in Y abbildet; surjektiv, wenn jedes Element aus Y das Bild eines Elements aus X unter f ist; und bijektiv, wenn sie sowohl injektiv als auch surjektiv ist.

(3.24) Beispiel.

(a) Die Abbildung $\{1,2,3\} \to \{4,5\}$, $1 \mapsto 4$, $2 \mapsto 4$, $3 \mapsto 5$ ist surjektiv, aber nicht injektiv.

(b) Die Abbildung $\{1,2\} \to \{4,5,6\}$, $1 \mapsto 4$, $2 \mapsto 5$ ist injektiv, aber nicht surjektiv.

(c) Die Abbildung $\{1,2,3\} \to \{4,5,6\}$, $1 \mapsto 5$, $2 \mapsto 6$, $3 \mapsto 4$ ist bijektiv.

(d) Die Abbildung $\{1,2,3\} \to \{4,5,6\}$, $1 \mapsto 5$, $2 \mapsto 6$, $3 \mapsto 5$ ist weder injektiv noch surjektiv.

(3.25) Beispiel. Die Abbildung $f\colon \mathbb{Q} \to \mathbb{Q}$, $x \mapsto -2x + 3$ ist eine Bijektion.

Beweis. Für $x, x' \in \mathbb{Q}$ mit $f(x) = f(x')$ gilt $-2x + 3 = -2x' + 3$, folglich $-2x = -2x'$ und damit $x = x'$. Somit ist f injektiv.
Für $y \in \mathbb{Q}$ gilt

$$f(-\frac{1}{2}y + \frac{3}{2}) = -2(-\frac{1}{2}y + \frac{3}{2}) + 3 = y - 3 + 3 = y.$$

Somit ist f surjektiv.
Insgesamt ist f bijektiv. □

Zum Beweis der Surjektivität in Beispiel (3.25) haben wir für jedes $y \in \mathbb{Q}$ ein $x \in \mathbb{Q}$ mit $y = f(x)$ angegeben, nämlich $x = -\frac{1}{2}y + \frac{3}{2}$. Hierbei ist es nicht entscheidend, wie man auf diese Formel gekommen ist, wichtig ist allein, dass für jedes $y \in \mathbb{Q}$ die Gleichung $y = f(x)$ gilt.
Nichtsdestotrotz stellt sich die Frage nach einer systematischen Methode zur Bestimmung eines solchen $x \in \mathbb{Q}$ für gegebenes $y \in \mathbb{Q}$. Hierzu können wir in diesem Fall eine *Analyse* verwenden: Wir nehmen an, dass wir ein $x \in \mathbb{Q}$ mit $y = f(x)$ gegeben haben. Dann gilt nämlich $y = f(x) = -2x + 3$, also $y - 3 = -2x$ und damit

$$x = -\frac{1}{2}(y - 3) = -\frac{1}{2}y + \frac{3}{2}.$$

Die Analyse ersetzt hierbei nicht den Beweis der Surjektivität und aus der Surjektivität folgt umgekehrt auch nicht die Aussage der Analyse: Bei der Analyse folgern wir für gegebenes $x \in \mathbb{Q}$ aus der Aussage $y = f(x)$ die Aussage $x = -\frac{1}{2}y + \frac{3}{2}$ (also die genaue Gestalt von x), während wir im Beweis der Surjektivität aus der Aussage $x = -\frac{1}{2}y + \frac{3}{2}$ die Aussage $y = f(x)$ folgern.

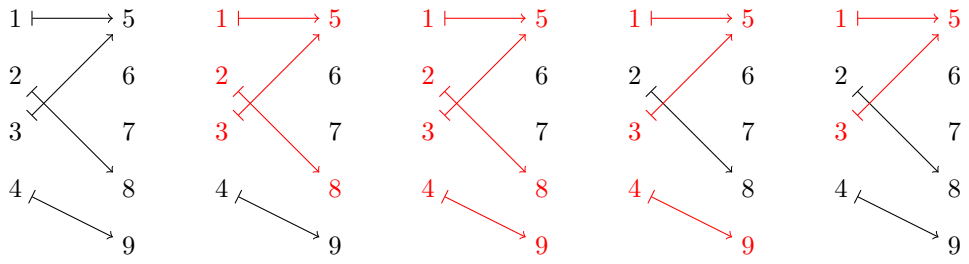


Abbildung 2: Bild und Urbild

(3.26) Beispiel.

(a) Es ist

$$\mathrm{Map}_{\mathrm{inj}}(\{1,2\},\{3,4,5\}) = \{(1\mapsto 3, 2\mapsto 4), (1\mapsto 3, 2\mapsto 5), (1\mapsto 4, 2\mapsto 3), (1\mapsto 4, 2\mapsto 5),\\ (1\mapsto 5, 2\mapsto 3), (1\mapsto 5, 2\mapsto 4)\}.$$

(b) Es ist

$$\mathrm{Map}_{\mathrm{surj}}(\{1,2,3\},\{4,5\}) = \{(1\mapsto 4, 2\mapsto 4, 3\mapsto 5), (1\mapsto 4, 2\mapsto 5, 3\mapsto 4), (1\mapsto 4, 2\mapsto 5, 3\mapsto 5),\\ (1\mapsto 5, 2\mapsto 4, 3\mapsto 4), (1\mapsto 5, 2\mapsto 4, 3\mapsto 5), (1\mapsto 5, 2\mapsto 5, 3\mapsto 4)\}.$$

(c) Es ist

$$\mathrm{Map}_{\mathrm{bij}}(\{1,2,3\},\{4,5,6\}) = \{(1\mapsto 4, 2\mapsto 5, 3\mapsto 6), (1\mapsto 4, 2\mapsto 6, 3\mapsto 5), (1\mapsto 5, 2\mapsto 4, 3\mapsto 6),\\ (1\mapsto 5, 2\mapsto 6, 3\mapsto 4), (1\mapsto 6, 2\mapsto 4, 3\mapsto 5), (1\mapsto 6, 2\mapsto 5, 3\mapsto 4)\}.$$

(3.27) Definition (Bild, Urbild)**.** Es sei eine Abbildung $f\colon X \to Y$ gegeben.

(a) Für eine Teilmenge U von X heißt

$$f(U) := \{f(u) \mid u \in U\} := \{y \in Y \mid \text{es gibt ein } u \in U \text{ mit } y = f(u)\}$$

das *Bild* von U unter f. Ferner heißt $\operatorname{Im} f := f(X)$ das *Bild* von f.

(b) Für eine Teilmenge V von Y heißt

$$f^{-1}(V) := \{x \in X \mid f(x) \in V\}$$

das *Urbild* von V unter f. Für $y \in Y$ heißt $f^{-1}(\{y\})$ die *Faser* von f über y.

Wir betonen, dass die Notation von Urbild und Faser nicht die Existenz einer inversen Abbildung voraussetzt; stattdessen haben wir es mit einer mehrdeutigen Schreibweise zu tun.

(3.28) Beispiel. Es sei $f\colon \{1,2,3,4\} \to \{5,6,7,8,9\}$, $1\mapsto 5$, $2\mapsto 8$, $3\mapsto 5$, $4\mapsto 9$. Dann ist $f(\{1,2,3\}) = \{5,8\}$, $\operatorname{Im} f = \{5,8,9\}$, $f^{-1}(\{5,9\}) = \{1,3,4\}$, $f^{-1}(\{5\}) = \{1,3\}$.

Beweis. Es gilt

$$f(\{1,2,3\}) = \{f(u) \mid u \in \{1,2,3\}\} = \{f(1), f(2), f(3)\} = \{5,8,5\} = \{5,8\},$$
$$\operatorname{Im} f = f(\{1,2,3,4\}) = \{f(u) \mid u \in \{1,2,3,4\}\} = \{f(1), f(2), f(3), f(4)\} = \{5,8,5,9\} = \{5,8,9\},$$
$$f^{-1}(\{5,9\}) = \{x \in \{1,2,3,4\} \mid f(x) \in \{5,9\}\} = \{x \in \{1,2,3,4\} \mid f(x) = 5 \text{ oder } f(x) = 9\} = \{1,3,4\},$$
$$f^{-1}(\{5\}) = \{x \in \{1,2,3,4\} \mid f(x) \in \{5\}\} = \{x \in \{1,2,3,4\} \mid f(x) = 5\} = \{1,3\}.$$ □

(3.29) Satz. Es sei eine Abbildung $f\colon X \to Y$ gegeben.

(a) Die folgenden Aussagen sind äquivalent.

(i) Die Abbildung f ist injektiv.

(ii) Jede Faser von f besitzt höchstens ein Element.

(iii) Es ist $X = \emptyset$ oder es gibt eine Abbildung $g\colon Y \to X$ mit $g \circ f = \mathrm{id}_X$.

(b) Die folgenden Aussagen sind äquivalent.

(i) Die Abbildung f ist surjektiv.

(ii) Jede Faser von f besitzt mindestens ein Element.

(iii) Es gibt eine Abbildung $g\colon Y \to X$ mit $f \circ g = \mathrm{id}_Y$.

(c) Die folgenden Aussagen sind äquivalent.

(i) Die Abbildung f ist bijektiv.

(ii) Jede Faser von f besitzt genau ein Element.

(iii) Die Abbildung f ist invertierbar.

Beweis.

(a) Zuerst zeigen wir die Äquivalenz von Bedingung (i) und Bedingung (ii), danach die Äquivalenz von Bedingung (i) und Bedingung (iii).

Zunächst gelte Bedingung (i), d.h. f sei injektiv. Für $y \in Y$, $x, x' \in f^{-1}(\{y\})$ gilt $f(x) = y = f(x')$, wegen der Injektivität von f also $x = x'$. Folglich ist $f^{-1}(\{y\})$ für $y \in Y$ entweder leer oder enthält genau ein Element, d.h. es gilt Bedingung (ii).

Nun sei umgekehrt angenommen, dass Bedingung (ii) gilt, d.h. dass jede Faser von f höchstens ein Element enthält. Außerdem seien $x, x' \in X$ mit $f(x) = f(x')$ gegeben. Dann ist $x \in f^{-1}(\{f(x)\})$ und $x' \in f^{-1}(\{f(x')\})$, wegen $f(x) = f(x')$ also $x, x' \in f^{-1}(\{f(x)\}) = f^{-1}(\{f(x')\})$. Nach unserer Voraussetzung enthält $f^{-1}(\{f(x)\}) = f^{-1}(\{f(x')\})$ jedoch höchstens ein Element, so dass $x = x'$ folgt. Somit ist f injektiv, d.h. es gilt Bedingung (i).

Folglich sind Bedingung (i) und Bedingung (ii) äquivalent.

Als nächstes gelte wieder Bedingung (i), d.h. f sei injektiv. Ferner nehmen wir an, dass $X \neq \emptyset$ ist. Da mit Bedingung (i) auch Bedingung (ii) gilt, enthält jede Faser von f höchstens ein Element. Die Faser von f unter jedem $y \in \operatorname{Im} f$ ist nach Definition von $\operatorname{Im} f$ jedoch auch nicht leer, d.h. sie enthält also genau ein Element. Mit anderen Worten: Für jedes $y \in \operatorname{Im} f$ gibt es genau ein $x \in X$ mit $f(x) = y$. Dies definiert eine Abbildung $g'\colon \operatorname{Im} f \to X$ mit $f(g'(y)) = y$ für $y \in \operatorname{Im} f$. Wegen $X \neq \emptyset$ gibt es ferner eine Abbildung $g''\colon Y \setminus \operatorname{Im} f \to X$. Wir definieren $g\colon Y \to X$ durch

$$g(y) := \begin{cases} g'(y) & \text{für } y \in \operatorname{Im} f, \\ g''(y) & \text{für } y \in Y \setminus \operatorname{Im} f. \end{cases}$$

Es ergibt sich $f(g(f(x))) = f(g'(f(x))) = f(x)$ und somit $g(f(x)) = x$ für $x \in X$ wegen der Injektivät von f. Also ist $g \circ f = \mathrm{id}_X$, d.h. es gilt Bedingung (iii).

Schließlich gelte Bedingung (iii), d.h. es sei $X = \emptyset$ oder es existiere eine Abbildung $g\colon Y \to X$ mit $g \circ f = \mathrm{id}_X$. Für $x, x' \in X$ mit $f(x) = f(x')$ folgt dann

$$x = g(f(x)) = g(f(x')) = x'.$$

Somit ist f injektiv, d.h. es gilt Bedingung (i).

Folglich sind auch Bedingung (i) und Bedingung (iii) äquivalent.

Insgesamt sind Bedingung (i), Bedingung (ii) und Bedingung (iii) äquivalent.

(b) Wir führen einen Ringschluss, d.h. wir zeigen, dass Bedingung (i) Bedingung (ii) impliziert, dass Bedingung (ii) Bedingung (iii) impliziert, und dass Bedingung (iii) Bedingung (i) impliziert.

Zunächst gelte Bedingung (i), d.h. f sei surjektiv. Ferner sei $y \in Y$ beliebig gegeben. Da f surjektiv ist, gibt es ein $x \in X$ mit $y = f(x)$, d.h. mit $x \in f^{-1}(\{y\})$. Folglich ist $f^{-1}(\{y\})$ nicht leer. Da $y \in Y$ beliebig war, gilt also Bedingung (ii).

Als nächstes sei angenommen, dass Bedingung (ii) gilt, d.h. dass jede Faser von f mindestens ein Element enthält. Dann gibt es für jedes $y \in Y$ ein $x \in X$ mit $x \in f^{-1}(\{y\})$. Wir wählen uns für jedes $y \in Y$ ein $g(y) \in f^{-1}(\{y\})$ und erhalten so eine Abbildung $g\colon Y \to X$ mit $f(g(y)) = y$ für $y \in Y$. Somit ist $f \circ g = \mathrm{id}_Y$, d.h. es gilt Bedingung (iii).

Schließlich gelte Bedingung (iii), d.h. es existiere eine Abbildung $g\colon Y \to X$ mit $f \circ g = \mathrm{id}_Y$. Für alle $y \in Y$ ist dann $f(g(y)) = y$, d.h. $g(y)$ ist ein Urbild von y unter f. Also ist f surjektiv, d.h. es gilt Bedingung (i).

Insgesamt sind Bedingung (i), Bedingung (ii) und Bedingung (iii) äquivalent.

(c) Dies sei dem Leser zur Übung überlassen. □

(3.30) Beispiel.

(a) Es sei $f\colon \{1,2\} \to \{4,5,6\}$, $1 \mapsto 4$, $2 \mapsto 5$. Dann ist

$$\{g \in \mathrm{Map}(\{4,5,6\},\{1,2\}) \mid g \circ f = \mathrm{id}_{\{1,2\}}\} = \{(4 \mapsto 1, 5 \mapsto 2, 6 \mapsto 1), (4 \mapsto 1, 5 \mapsto 2, 6 \mapsto 2)\}.$$

(b) Es sei $f\colon \{1,2,3\} \to \{4,5\}$, $1 \mapsto 4$, $2 \mapsto 4$, $3 \mapsto 5$. Dann ist

$$\{g \in \mathrm{Map}(\{4,5\},\{1,2,3\}) \mid f \circ g = \mathrm{id}_{\{4,5\}}\} = \{(4 \mapsto 1, 5 \mapsto 3), (4 \mapsto 2, 5 \mapsto 3)\}.$$

(c) Es sei $f\colon \{1,2,3\} \to \{4,5,6\}$, $1 \mapsto 5$, $2 \mapsto 6$, $3 \mapsto 4$. Dann ist

$$\{g \in \mathrm{Map}(\{4,5,6\},\{1,2,3\}) \mid g \circ f = \mathrm{id}_{\{1,2,3\}},\ f \circ g = \mathrm{id}_{\{4,5,6\}}\} = \{(4 \mapsto 3, 5 \mapsto 1, 6 \mapsto 2)\}.$$

Beweis.

(a) Es ist

$$\begin{aligned}
&\{g \in \mathrm{Map}(\{4,5,6\},\{1,2\}) \mid g \circ f = \mathrm{id}_{\{1,2\}}\} \\
&= \{g \in \mathrm{Map}(\{4,5,6\},\{1,2\}) \mid (g \circ f)(x) = \mathrm{id}_{\{1,2\}}(x) \text{ für } x \in \{1,2\}\} \\
&= \{g \in \mathrm{Map}(\{4,5,6\},\{1,2\}) \mid g(f(x)) = x \text{ für } x \in \{1,2\}\} \\
&= \{g \in \mathrm{Map}(\{4,5,6\},\{1,2\}) \mid g(f(1)) = 1,\ g(f(2)) = 2\} \\
&= \{g \in \mathrm{Map}(\{4,5,6\},\{1,2\}) \mid g(4) = 1,\ g(5) = 2\} \\
&= \{(4 \mapsto 1, 5 \mapsto 2, 6 \mapsto 1), (4 \mapsto 1, 5 \mapsto 2, 6 \mapsto 2)\}.
\end{aligned}$$

(b) Es ist

$$\begin{aligned}
&\{g \in \mathrm{Map}(\{4,5\},\{1,2,3\}) \mid f \circ g = \mathrm{id}_{\{4,5\}}\} \\
&= \{g \in \mathrm{Map}(\{4,5\},\{1,2,3\}) \mid (f \circ g)(y) = \mathrm{id}_{\{4,5\}}(y) \text{ für } y \in \{4,5\}\} \\
&= \{g \in \mathrm{Map}(\{4,5\},\{1,2,3\}) \mid f(g(y)) = y \text{ für } y \in \{4,5\}\} \\
&= \{g \in \mathrm{Map}(\{4,5\},\{1,2,3\}) \mid g(y) \in f^{-1}(\{y\}) \text{ für } y \in \{4,5\}\} \\
&= \{g \in \mathrm{Map}(\{4,5\},\{1,2,3\}) \mid g(4) \in f^{-1}(\{4\}),\ g(5) \in f^{-1}(\{5\})\} \\
&= \{g \in \mathrm{Map}(\{4,5\},\{1,2,3\}) \mid g(4) \in \{1,2\},\ g(5) \in \{3\}\} \\
&= \{(4 \mapsto 1, 5 \mapsto 3), (4 \mapsto 2, 5 \mapsto 3)\}.
\end{aligned}$$

(c) Es ist

$$\begin{aligned}
&\{g \in \mathrm{Map}(\{4,5,6\},\{1,2,3\}) \mid g \circ f = \mathrm{id}_{\{1,2,3\}},\ f \circ g = \mathrm{id}_{\{4,5,6\}}\} \\
&= \{g \in \mathrm{Map}(\{4,5,6\},\{1,2,3\}) \mid (g \circ f)(x) = \mathrm{id}_{\{1,2,3\}}(x) \text{ für } x \in \{1,2,3\},
\end{aligned}$$

$$
\begin{aligned}
&(f \circ g)(y) = \mathrm{id}_{\{4,5,6\}}(y) \text{ für } y \in \{4,5,6\}\} \\
&= \{g \in \mathrm{Map}(\{4,5,6\},\{1,2,3\}) \mid g(f(x)) = x \text{ für } x \in \{1,2,3\},\ f(g(y)) = y \text{ für } y \in \{4,5,6\}\} \\
&= \{g \in \mathrm{Map}(\{4,5,6\},\{1,2,3\}) \mid g(f(1)) = 1,\ g(f(2)) = 2,\ g(f(3)) = 3, \\
&\quad f(g(4)) = 4,\ f(g(5)) = 5,\ f(g(6)) = 6\} \\
&= \{g \in \mathrm{Map}(\{4,5,6\},\{1,2,3\}) \mid g(5) = 1,\ g(6) = 2,\ g(4) = 3, \\
&\quad f(g(4)) = 4,\ f(g(5)) = 5,\ f(g(6)) = 6\} \\
&= \{g \in \mathrm{Map}(\{4,5,6\},\{1,2,3\}) \mid g(5) = 1,\ g(6) = 2,\ g(4) = 3,\ f(3) = 4,\ f(1) = 5,\ f(2) = 6\} \\
&= \{g \in \mathrm{Map}(\{4,5,6\},\{1,2,3\}) \mid g(5) = 1,\ g(6) = 2,\ g(4) = 3\} \\
&= \{(4 \mapsto 3, 5 \mapsto 1, 6 \mapsto 2)\}.
\end{aligned}
$$

□

Restriktion von Abbildungen

Als nächstes werden wir kurz aufzeigen, dass Teilmengen Anlass zu Abbildungen geben.

(3.31) Definition (Restriktion)**.** Es seien eine Abbildung $f\colon X \to Y$, eine Teilmenge U von X und eine Teilmenge V von Y mit $f(U) \subseteq V$ gegeben. Die Abbildung

$$f|_U^V\colon U \to V,\ u \mapsto f(u)$$

wird *Restriktion* (oder *Einschränkung*) von f bzgl. U und V genannt.
Für $U \subseteq X$ setzen wir

$$f|_U := f|_U^Y.$$

Für $V \subseteq Y$ mit $\operatorname{Im} f \subseteq V$ setzen wir

$$f|^V := f|_X^V.$$

(3.32) Beispiel. Es sei $f\colon \{2,3,5,7,11\} \to \{0,1,2,3\}$, $2 \mapsto 2$, $3 \mapsto 3$, $5 \mapsto 1$, $7 \mapsto 3$, $11 \mapsto 3$.

(a) Es ist

$$f|_{\{3,7,11\}}^{\{0,1,3\}}\colon \{3,7,11\} \to \{0,1,3\},\ 3 \mapsto 3,\ 7 \mapsto 3,\ 11 \mapsto 3.$$

(b) Es ist

$$f|_{\{2,7,11\}}\colon \{2,7,11\} \to \{0,1,2,3\},\ 2 \mapsto 2,\ 7 \mapsto 3,\ 11 \mapsto 3.$$

(c) Es ist

$$f|^{\{1,2,3\}}\colon \{2,3,5,7,11\} \to \{1,2,3\},\ 2 \mapsto 2,\ 3 \mapsto 3,\ 5 \mapsto 1,\ 7 \mapsto 3,\ 11 \mapsto 3.$$

(3.33) Definition (Inklusion)**.** Es seien eine Menge X und eine Teilmenge U von X gegeben. Die Abbildung

$$\mathrm{inc} = \mathrm{inc}^U := \mathrm{id}_X|_U\colon U \to X$$

heißt *Inklusion* (oder *Inklusionsabbildung*) von U in X.

(3.34) Beispiel. Die Inklusion von $\{2,5,7\}$ in $\{2,3,5,7,11\}$ ist gegeben durch

$$\mathrm{inc}\colon \{2,5,7\} \to \{2,3,5,7,11\},\ 2 \mapsto 2,\ 5 \mapsto 5,\ 7 \mapsto 7.$$

Indikatorfunktion

Ein Zusammenhang zwischen Teilmengen und Abbildungen ist durch die Indikatorfunktion gegeben, welche eine Bijektion zwischen der Potenzmenge einer gegebenen Menge und den Abbildungen von dieser Menge in eine zweielementige Menge liefert, siehe Satz (3.37).

(3.35) Definition (Indikatorfunktion)**.** Es seien eine Menge X und eine Teilmenge U von X gegeben. Die Abbildung $\chi_U\colon X \to \{0,1\}$ gegeben durch

$$\chi_U(x) = \begin{cases} 1, & \text{für } x \in U, \\ 0, & \text{für } x \in X \setminus U, \end{cases}$$

heißt *Indikatorfunktion* (oder *charakteristische Funktion*) von U in X.

Gemäß Konvention (3.9) fassen wir eine Indikatorfunktion ggf. auch als Familie auf und sprechen dann von einer *Indikatorfamilie* bzw. in den Spezialfällen von einem *Indikatortupel* bzw. einer *Indikatorfolge* bzw. einer *Indikatormatrix*. Notieren wir ein Indikatortupel als String, vgl. Definition (10.2), so sprechen wir entsprechend von einem *Indikatorstring*.

(3.36) Beispiel.

(a) Die Indikatorfunktion von $\{2,5,7\}$ in $\{2,3,5,7,11\}$ ist gegeben durch

$$\chi_{\{2,5,7\}}\colon \{2,3,5,7,11\} \to \{0,1\},\ 2 \mapsto 1,\ 3 \mapsto 0,\ 5 \mapsto 1,\ 7 \mapsto 1,\ 11 \mapsto 0.$$

(b) Das Indikatortupel von $\{2,3,4,7\}$ in $[1,7]$ ist gegeben durch

$$\chi_{\{2,3,4,7\}} = (0,1,1,1,0,0,1).$$

(3.37) Satz. Es sei eine Menge X gegeben. Die Abbildungen

$$\mathrm{Pot}(X) \to \mathrm{Map}(X,\{0,1\}),\ U \mapsto \chi_U,$$
$$\mathrm{Map}(X,\{0,1\}) \to \mathrm{Pot}(X),\ f \mapsto f^{-1}(\{1\})$$

sind zueinander invers.

Beweis. Für den Zweck dieses Beweises sei

$$\mathrm{U}_f := f^{-1}(\{1\}) = \{x \in X \mid f(x) = 1\}$$

für $f \in \mathrm{Map}(X,\{0,1\})$. Wir wollen zeigen, dass sich die Abbildungen

$$\chi_-\colon \mathrm{Pot}(X) \to \mathrm{Map}(X,\{0,1\}),\ U \mapsto \chi_U,$$
$$\mathrm{U}_-\colon \mathrm{Map}(X,\{0,1\}) \to \mathrm{Pot}(X),\ f \mapsto \mathrm{U}_f$$

gegenseitig invertieren. Für $U \in \mathrm{Pot}(X)$ ist

$$(\mathrm{U}_- \circ \chi_-)(U) = \mathrm{U}_{\chi_U} = \chi_U^{-1}(\{1\}) = U = \mathrm{id}_{\mathrm{Pot}(U)}(U).$$

Nach dem Gleichheitskriterium für Abbildungen (3.6) gilt folglich $\mathrm{U}_- \circ \chi_- = \mathrm{id}_{\mathrm{Pot}(U)}$. Für $f \in \mathrm{Map}(X,\{0,1\})$ gilt umgekehrt

$$\chi_{\mathrm{U}_f}(x) = \begin{Bmatrix} 1, & \text{falls } x \in \mathrm{U}_f, \\ 0, & \text{falls } x \notin \mathrm{U}_f \end{Bmatrix} = \begin{Bmatrix} 1, & \text{falls } x \in f^{-1}(\{1\}), \\ 0, & \text{falls } x \notin f^{-1}(\{1\}) \end{Bmatrix} = \begin{Bmatrix} 1, & \text{falls } f(x) = 1, \\ 0, & \text{falls } f(x) \neq 1 \end{Bmatrix} = f(x)$$

für $x \in X$, also $(\chi_- \circ \mathrm{U}_-)(f) = \chi_{\mathrm{U}_f} = f = \mathrm{id}_{\mathrm{Map}(X,\{0,1\})}(f)$ nach dem Gleichheitskriterium für Abbildungen (3.6). Somit gilt auch $\chi_- \circ \mathrm{U}_- = \mathrm{id}_{\mathrm{Map}(X,\{0,1\})}$ nach dem Gleichheitskriterium für Abbildungen (3.6). Insgesamt sind χ_- und U_- zueinander inverse Abbildungen. □

(3.38) Beispiel. Wir haben folgende Bijektion.

$$\begin{aligned}
\mathrm{Pot}([1,3]) &\to \{0,1\}^3,\\
\emptyset &\mapsto (0,0,0),\\
\{1\} &\mapsto (1,0,0),\\
\{2\} &\mapsto (0,1,0),\\
\{3\} &\mapsto (0,0,1),\\
\{1,2\} &\mapsto (1,1,0),\\
\{1,3\} &\mapsto (1,0,1),\\
\{2,3\} &\mapsto (0,1,1),\\
\{1,2,3\} &\mapsto (1,1,1).
\end{aligned}$$

Endlichkeit und Kardinalität

Zum Schluss dieses Abschnitts betrachten wir noch das Konzept der Kardinalität einer endlichen Menge.

(3.39) Definition (Gleichmächtigkeit)**.** Es seien Mengen X und Y gegeben. Wir sagen, dass X *gleichmächtig* zu Y ist, falls es eine Bijektion von X nach Y gibt.

(3.40) Beispiel.

(a) Die Menge $\{1,2,3\}$ ist gleichmächtig zur Menge $\{4,5,6\}$.

(b) Die Menge $\mathbb{N}$ ist gleichmächtig zu $\mathbb{Z}$.

Beweisskizze.

(a) Die Abbildung $\{1,2,3\} \to \{4,5,6\}$, $x \mapsto x+3$ ist eine Bijektion.

(b) Die Abbildung $f\colon \mathbb{N} \to \mathbb{Z}$ gegeben durch

$$f(x) = \begin{cases} \frac{x}{2}, & \text{für } x \in \mathbb{N} \text{ gerade},\\ \frac{1-x}{2}, & \text{für } x \in \mathbb{N} \text{ ungerade}, \end{cases}$$

ist eine Bijektion. □

(3.41) Definition ((un)endliche Menge)**.** Es sei eine Menge X gegeben.

(a) Wir sagen, dass X *endlich* ist, falls es ein $n \in \mathbb{N}_0$ derart gibt, dass X gleichmächtig zu $[1,n]$ ist, und ansonsten, dass X *unendlich* ist.

(b) Es seien ein $n \in \mathbb{N}_0$ und eine Menge X gegeben. Eine Bijektion von $[1,n]$ nach X wird *Abzählung* von X genannt.

(3.42) Beispiel.

(a) Die Menge $\{1,3,17\}$ ist endlich.

(b) Die Mengen $\mathbb{N}$ und $\{x \in \mathbb{N} \mid x \text{ gerade}\}$ sind unendlich.

(c) Die leere Menge ist endlich.

(d) Die Menge $\{x \in \mathbb{R} \mid x^3 + 2x = 3x^2\}$ ist endlich.

Es lässt sich zeigen, dass es für jede endliche Menge X genau ein $n \in \mathbb{N}_0$ derart gibt, dass X gleichmächtig zu $[1,n]$ ist.

(3.43) Definition (Kardinalität)**.** Es seien eine endliche Menge X und $n \in \mathbb{N}_0$ derart gegeben, dass X gleichmächtig zu $[1,n]$ ist. Wir nennen

$$|X| := n$$

die *Kardinalität* (oder *Mächtigkeit*) von X. Wir sagen auch, dass X eine *n-elementige* Menge ist.

(3.44) Beispiel.

(a) Es ist $|\{1, 3, 17\}| = 3$.

(b) Es ist $|\{1, 1, 1\}| = 1$.

(c) Es ist $|\{\{1\}\}| = 1$.

(d) Es ist $|\{1, \{1\}\}| = 2$.

4 Relationen

Als nächstes widmen wir uns Relationen auf einer gegebenen Menge; ein Konzept, welches Beziehungen zwischen den Elementen dieser Menge formalisiert. Hierbei beschränken wir uns auf binäre Relationen, d.h. die betrachteten Beziehungen bestehen zwischen Paaren von Elementen der Menge.
Nach der Definition einer Relation studieren wir Eigenschaften von allgemeinen (binären) Relationen sowie Abschlüsse unter einiger dieser Eigenschaften. Zum Schluss geben wir mit der Indikatormatrix eine Methode an, wie sich Relationen auf einer endlichen Menge mit Hilfe einer Matrix darstellen lassen.

Begriffsbildung

Wir beginnen mit der Definition einer Relation.

(4.1) Definition (Relation)**.**

(a) Eine *Relation* (genauer *binäre Relation*) besteht aus einer Menge X zusammen mit einer Teilmenge r von $X \times X$. Unter Missbrauch der Notation bezeichnen wir sowohl die besagte Relation als auch die Teilmenge von $X \times X$ mit r. Die Menge X wird *Grundmenge* von r genannt.

Es seien eine Relation r mit Grundmenge X und $x, y \in X$ gegeben. Falls $(x, y) \in r$ ist, so sagen wir, dass x bzgl. r in *Relation* zu y *steht* und schreiben $x\ r\ y$.

(b) Es sei eine Menge X gegeben. Die *Menge der Relationen* auf X ist definiert als

$$\mathrm{Rel}(X) := \{r \mid r \text{ ist eine Relation mit Grundmenge } X\}.$$

Ein Element von $\mathrm{Rel}(X)$ wird *Relation* auf X genannt.

Etwas allgemeiner lässt sich für Mengen X und Y eine *Relation* zwischen X und Y als Gesamtheit aus X, Y und einer Teilmenge von $X \times Y$ definieren. Wir werden dieses Konzept in dieser Veranstaltung nicht weiter verfolgen.

(4.2) Beispiel.

(a) Es ist $<$ eine Relation auf $\mathbb{N}$. Die zur Relation $<$ gehörige Teilmenge von $\mathbb{N} \times \mathbb{N}$ ist gegeben durch

$$< = \{(m, n) \in \mathbb{N} \times \mathbb{N} \mid \text{es gibt ein } p \in \mathbb{N} \text{ mit } n = p + m\}.$$

(b) Es sei eine Menge X gegeben. Dann ist $\subseteq$ eine Relation auf $\mathrm{Pot}(X)$. ([33]) Die zur Relation $\subseteq$ gehörige Teilmenge von $\mathrm{Pot}(X) \times \mathrm{Pot}(X)$ ist gegeben durch

$$\subseteq = \{(U, V) \in \mathrm{Pot}(X) \times \mathrm{Pot}(X) \mid \text{für } x \in U \text{ gilt } x \in V\}.$$

(c) Es sei eine Menge X gegeben. Dann ist $=$ eine Relation auf X. Wir nennen $=$ die *Gleichheitsrelation* (oder *Gleichheit*) auf X. Die zur Relation $=$ gehörige Teilmenge von $X \times X$ ist gegeben durch

$$= = \{(x, x) \mid x \in X\}.$$

(d) Es sei eine Menge X gegeben. Dann wird $X \times X = \{(x, y) \mid x, y \in X\}$ zu einer Relation auf X, die *Allrelation* auf $X \times X$.

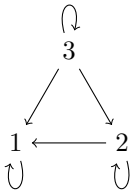


Abbildung 3: Relation auf $\{1, 2, 3\}$

(e) Es wird $\{(1, 1), (2, 1), (2, 2), (3, 1), (3, 2), (3, 3)\}$ zu einer Relation auf $\{1, 2, 3\}$.

Wie in Beispiel (4.2)(a), (b), (c) schon angedeutet, ist es üblich, Relationen durch Angabe der Eigenschaft, welche für die in Relation stehenden Elemente erfüllt ist, zu definieren. Dies ist äquivalent zur Angabe der Teilmenge des kartesischen Produkts und meistens etwas leserlicher.
Wir geben noch einige Modellierungen von Beziehungen aus dem täglichen Leben durch Relationen an:

(4.3) Anwendungsbeispiel.

(a) Die Einwohner von Aachen seien als Elemente einer Menge A modelliert. Für $a, b \in A$ gelte genau dann $a\ n\ b$, wenn der durch a modellierte Einwohner ein Nachkomme des durch b modellierten Einwohners ist. Dann ist n eine Relation auf A.

(b) Die Studierenden des Moduls *Diskrete Strukturen* seien als Elemente einer Menge D modelliert. Für $s, t \in D$ gelte genau dann $s\ e\ t$, wenn der oder die durch s modellierte Studierende die gleichen Eltern wie der oder die durch t modellierte Studierende hat. Für $s, t \in D$ gelte genau dann $s\ g\ t$, wenn der oder die durch s modellierte Studierende den gleichen Geburtstag wie der oder die durch t modellierte Studierende hat. Dann sind e und g Relationen auf D.

(c) Die Stichwörter in einem Lexikon seien als Elemente einer Menge L modelliert. Für $v, w \in L$ gelte genau dann $v\ a\ w$, wenn das durch v modellierte Stichwort den gleichen Anfangsbuchstaben wie das durch w modellierte Stichwort hat. Für $v, w \in L$ gelte genau dann $v\ o\ w$, wenn das durch v modellierte Stichwort einen Anfangsbuchstaben hat, welcher im Alphabet vorm Anfangsbuchstaben des durch w modellierten Stichworts vorkommt. Dann sind a und o Relationen auf L.

(d) Farbige Glasperlen in einer Dose seien als Elemente einer Menge P modelliert. Für $p, q \in P$ gelte genau dann $p\ f\ q$, wenn die durch p modellierte Glasperle die gleiche Farbe wie die durch q modellierte Glasperle hat. Dann ist f eine Relation auf P.

Eigenschaften

Wir betrachten einige potentielle Eigenschaften von Relationen.

(4.4) Definition (Transitivität, Reflexivität, Symmetrie, Antisymmetrie, Vollständigkeit)**.** Es seien eine Menge X und eine Relation r auf X gegeben.

(a) Wir sagen, dass r *transitiv* ist, falls für $x, y, z \in X$ aus $x\ r\ y$ und $y\ r\ z$ stets $x\ r\ z$ folgt.

(b) Wir sagen, dass r *reflexiv* (auf X) ist, falls für $x \in X$ stets $x\ r\ x$ gilt.

(c) Wir sagen, dass r *symmetrisch* ist, falls für $x, y \in X$ aus $x\ r\ y$ stets $y\ r\ x$ folgt.

(d) Wir sagen, dass r *antisymmetrisch* ist, falls für $x, y \in X$ aus $x\ r\ y$ und $y\ r\ x$ stets $x = y$ folgt.

(e) Wir sagen, dass r *vollständig* (auf X) ist, falls für $x, y \in X$ stets $x\ r\ y$ oder $y\ r\ x$ gilt.

(4.5) Beispiel. Die Relation $<$ auf $\mathbb{N}$ ist transitiv und antisymmetrisch, aber nicht reflexiv, nicht symmetrisch und nicht vollständig.

[33] Wir nennen $\subseteq$ die *Teilmengenrelation* (oder *Inklusionsrelation* oder *Inklusion*) auf $\mathrm{Pot}(X)$.

Beweis. Es seien $m, n, p \in \mathbb{N}$ mit $m < n$ und $n < p$ gegeben. Dann gibt es $q, r \in \mathbb{N}$ mit $n = q + m$ und $p = r + n$. Es folgt $p = r + n = r + q + m$, also $m < p$. Folglich ist $<$ transitiv.
Es gibt keine $m, n \in \mathbb{N}$ mit $m < n$ und $n < m$. Folglich ist $<$ antisymmetrisch.
Es gibt keine $m, p \in \mathbb{N}$ mit $m = p + m$. Somit gibt es kein $m \in \mathbb{N}$ mit $m < m$. Insbesondere ist $<$ nicht reflexiv und nicht vollständig.
Es seien $m, n \in \mathbb{N}$ mit $m < n$ gegeben. Dann gibt es ein $p \in \mathbb{N}$ mit $n = p + m$. Gäbe es ein $q \in \mathbb{N}$ mit $m = q + n$, so wäre $m = q + n = q + p + m$ und damit $q + p = 0$. Da mit $p, q \in \mathbb{N}$ dann aber auch $0 = q + p \in \mathbb{N}$ sein müsste, ist dies ein Widerspruch. Folglich gilt $n < m$ nicht. Insbesondere ist $<$ nicht symmetrisch. □

Vorsicht sind bei den Begriffen der Reflexivität und der Vollständigkeit geboten, da diese von der unterliegende Menge abhängig sind.

(4.6) Beispiel.

(a) Es sei r die Relation auf $\{1\}$ gegeben durch $r = \{(1, 1)\}$. Dann ist r reflexiv.

(b) Es sei r die Relation auf $\{1, 2\}$ gegeben durch $r = \{(1, 1)\}$. Dann ist r nicht reflexiv.

Beweis.

(a) Wegen $1\ r\ 1$ gilt $x\ r\ x$ für alle $x \in \{1\}$. Folglich ist r reflexiv.

(b) Da $2\ r\ 2$ nicht gilt, gibt es ein $x \in \{1, 2\}$ so, dass $x\ r\ x$ nicht gilt. Folglich ist r nicht reflexiv. □

(4.7) Bemerkung. Es seien eine Menge X, eine nicht leere Menge I und eine Familie $(r_i)_{i \in I}$ von Relationen auf X gegeben. Für $x, y \in X$ gelte genau dann $x\ r\ y$, wenn für $i \in I$ stets $x\ r_i\ y$ gilt.

(a) Wenn r_i für jedes $i \in I$ transitiv ist, dann ist r auch transitiv.

(b) Wenn r_i für jedes $i \in I$ reflexiv ist, dann ist r auch reflexiv.

(c) Wenn r_i für jedes $i \in I$ symmetrisch ist, dann ist r auch symmetrisch.

(d) Wenn es ein $i \in I$ derart gibt, dass r_i antisymmetrisch ist, dann ist r auch antisymmetrisch.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(4.8) Beispiel. Es seien r' und r'' die Relationen auf $\{1, 2\}$ gegeben durch

$$r' = \{(1, 1), (2, 2), (1, 2)\},$$
$$r'' = \{(1, 1), (2, 2), (2, 1)\}.$$

Für $x, y \in \{1, 2\}$ gelte genau dann $x\ r\ y$, wenn $x\ r'\ y$ und $x\ r''\ y$ gilt. Dann sind r' und r'' vollständig auf $\{1, 2\}$, aber r ist nicht vollständig auf $\{1, 2\}$.

Beweis. Wegen $1\ r'\ 1$, $2\ r'\ 2$ und $1\ r'\ 2$ ist r' vollständig.
Wegen $1\ r''\ 1$, $2\ r''\ 2$ und $2\ r''\ 1$ ist r'' vollständig.
Da $1\ r''\ 2$ nicht gilt, gilt auch $1\ r\ 2$ nicht. Da $2\ r'\ 1$ nicht gilt, gilt auch $2\ r\ 1$ nicht. Folglich ist r nicht vollständig. □

Abschlüsse

Der Abschluss einer gegebenen Relation unter einer Eigenschaft ist die kleinste Relation, welche zum einen die gegebene Relation als Teilmenge enthält und zum anderen die gegebene Eigenschaft erfüllt:

(4.9) Definition (transitiver Abschluss, reflexiver Abschluss, transitiv-reflexiver Abschluss, symmetrischer Abschluss)**.** Es seien eine Menge X und eine Relation r auf X gegeben.

(a) Ein *transitiver Abschluss* (oder eine *transitive Hülle*) von r ist eine transitive Relation s auf X mit $r \subseteq s$ und so, dass für jede transitive Relation t auf X mit $r \subseteq t$ stets $s \subseteq t$ folgt.

(b) Ein *reflexiver Abschluss* (oder eine *reflexive Hülle*) von r ist eine reflexive Relation s auf X mit $r \subseteq s$ und so, dass für jede reflexive Relation t auf X mit $r \subseteq t$ stets $s \subseteq t$ folgt.

Abbildung 4: Abschlüsse

(c) Ein *transitiv-reflexiver Abschluss* (oder eine *transitiv-reflexive Hülle*) von r ist eine transitive, reflexive Relation s auf X mit $r \subseteq s$ und so, dass für jede transitive, reflexive Relation t auf X mit $r \subseteq t$ stets $s \subseteq t$ folgt.

(d) Ein *symmetrischer Abschluss* (oder eine *symmetrische Hülle*) von r ist eine symmetrische Relation s auf X mit $r \subseteq s$ und so, dass für jede symmetrische Relation t auf X mit $r \subseteq t$ stets $s \subseteq t$ folgt.

(4.10) Beispiel. Es sei r die Relation auf $\{1,2,3\}$ gegeben durch $r = \{(1,2),(2,3)\}$.

(a) Die Relation s auf $\{1,2,3\}$ gegeben durch

$$s = \{(1,2),(1,3),(2,3)\}$$

ist ein transitiver Abschluss von r.

(b) Die Relation s auf $\{1,2,3\}$ gegeben durch

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

ist ein reflexiver Abschluss von r.

(c) Die Relation s auf $\{1,2,3\}$ gegeben durch

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

ist ein transitiv-reflexiver Abschluss von r.

(d) Die Relation s auf $\{1,2,3\}$ gegeben durch

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

ist ein symmetrischer Abschluss von r.

Beweis.

(a) Um zu zeigen, dass s transitiv ist, seien $x,y,z \in \{1,2,3\}$ mit $x\ s\ y$ und $y\ s\ z$ gegeben. Nach Definition von s gilt dann notwendigerweise $(x,y) = (1,2)$ und $(y,z) = (2,3)$, also $x = 1$, $y = 2$, $z = 3$. Dann gilt aber auch $x = 1\ s\ 3 = z$. Folglich ist s transitiv.

Für $x,y \in \{1,2,3\}$ mit $x\ r\ y$ gilt entweder $(x,y) = (1,2)$ und damit $x\ s\ y$, oder es gilt $(x,y) = (2,3)$ und damit $x\ s\ y$. Folglich gilt $r \subseteq s$.

Schließlich sei eine beliebige transitive Relation t auf $\{1,2,3\}$ mit $r \subseteq t$ gegeben. Wegen $1\ r\ 2$ gilt $1\ t\ 2$ und wegen $2\ r\ 3$ gilt $2\ t\ 3$. Aus $1\ t\ 2$ und $2\ t\ 3$ folgt $1\ t\ 3$ auf Grund der Transitivität von t. Insgesamt gilt $1\ t\ 2$, $1\ t\ 3$ und $2\ t\ 3$, d.h. für alle $x,y \in \{1,2,3\}$ mit $x\ s\ y$ gilt $x\ t\ y$. Folglich gilt $s \subseteq t$.

Insgesamt ist s ein transitiver Abschluss von r auf $\{1,2,3\}$.

(b) Dies sei dem Leser zur Übung überlassen.

(c) Dies sei dem Leser zur Übung überlassen.

(d) Dies sei dem Leser zur Übung überlassen. □

(4.11) Proposition. Es seien eine Menge X und eine Relation r auf X gegeben.

(a) Es gibt genau einen transitiven Abschluss von r. Der transitive Abschluss s von r ist wie folgt gegeben: Für $x, y \in X$ gilt genau dann $x\ s\ y$, wenn es ein $n \in \mathbb{N}$ und $x_0, \ldots, x_n \in X$ mit $x_i\ r\ x_{i+1}$ für $i \in [0, n-1]$ und $x_0 = x$, $x_n = y$ gibt.

$$x = x_0\ r\ x_1\ r\ \ldots\ r\ x_n = y$$

(b) Es gibt genau einen reflexiven Abschluss von r. Der reflexive Abschluss s von r ist wie folgt gegeben: Für $x, y \in X$ gilt genau dann $x\ s\ y$, wenn $x\ r\ y$ oder $x = y$ gilt.

(c) Es gibt genau einen transitiv-reflexiven Abschluss von r. Der transitiv-reflexive Abschluss s von r ist wie folgt gegeben: Für $x, y \in X$ gilt genau dann $x\ s\ y$, wenn es ein $n \in \mathbb{N}_0$ und $x_0, \ldots, x_n \in X$ mit $x_i\ r\ x_{i+1}$ für $i \in [0, n-1]$ und $x_0 = x$, $x_n = y$ gibt.

$$x = x_0\ r\ x_1\ r\ \ldots\ r\ x_n = y$$

(d) Es gibt genau einen symmetrischen Abschluss von r. Der symmetrische Abschluss s von r ist wie folgt gegeben: Für $x, y \in X$ gilt genau dann $x\ s\ y$, wenn $x\ r\ y$ oder $y\ r\ x$ gilt.

Beweis. Dies sei dem Leser zur Übung überlassen. □

Indikatormatrix

Es sei $n \in \mathbb{N}_0$ gegeben. Eine Relation r auf $[1, n]$ ist eine Teilmenge von $[1, n] \times [1, n]$. Die Indikatormatrix, vgl. Definition (3.35), liefert eine Verbildlichung einer solchen Relation.
Durch Wahl einer Abzählung, vgl. Definition (3.41)(b), lässt sich das Konzept auf Relationen auf beliebigen endlichen Mengen verallgemeinern:

(4.12) Definition (Indikatormatrix)**.** Es seien $n \in \mathbb{N}_0$, eine Menge X, eine Abzählung e von X und eine Relation r auf X gegeben. Die $(n \times n)$-Matrix $\chi_{r,e}$ in $\{0, 1\}$ gegeben durch

$$\chi_{r,e} = ((\chi_r)_{e(i),e(j)})_{i,j \in [1,n]}$$

wird *Indikatormatrix* von r bzgl. e genannt.

(4.13) Beispiel.

(a) Es sei eine Relation r auf $\{1, 2, 3\}$ gegeben durch

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

Die Indikatormatrix von r ist gegeben durch

$$\chi_r = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

(b) Es sei eine Relation r auf $\{-1, 0, 1\}$ gegeben durch

$$r = \{(-1,-1), (1,1), (-1,1), (1,-1)\}.$$

Die Indikatormatrix von r bzgl. der Abzählung $e\colon [1, 3] \to \{-1, 0, 1\}$, $1 \mapsto -1$, $2 \mapsto 0$, $3 \mapsto 1$ ist gegeben durch

$$\chi_{r,e} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Etwas informeller lässt sich die Indikatormatrix in Beispiel (4.13)(b) durch Beschriftung mit den abgezählten Elementen in einer *Indikatortafel* darstellen:

r	-1	0	1
-1	1	0	1
0	0	0	0
1	1	0	1

5 Äquivalenzrelationen und Quotientenmengen

Ziel dieses Abschnitts ist es, den Begriff der (absoluten) Gleichheit von Objekten abzuschwächen und zu formalisieren, was wir unter einer „Gleichheit unter einem gewissen Gesichtspunkt“ verstehen. Hierzu dient der Begriff der Äquivalenzrelation. Fassen wir die bzgl. einer Äquivalenzrelation in Relation stehenden Objekte auf geeignete Art und Weise zusammen, so erhalten wir eine neue Menge, die sogenannte Quotientenmenge, wo dann tatsächliche Gleichheit herrscht.
Wir beginnen mit der Einführung des Begriffs der Äquivalenzrelation und des Konzepts der Quotientenmenge modulo einer Äquivalenzrelation. Danach studieren wir mit der Bildgleichheit eine durch eine gegebene Abbildung induzierte Äquivalenzrelation, welche zum Homomorphiesatz für Mengen (5.15) führt. Am Ende des Abschnitts zeigen wir im Hauptsatz über Äquivalenzrelationen (5.20), dass Äquivalenzrelationen auf einer gegebenen Menge in Bijektion zu sogenannten Partitionen dieser Menge sind.

Äquivalenzrelationen

Eine Äquivalenzrelation ist eine Relation, siehe Definition (4.1), welche drei der in Definition (4.4) eingeführten Eigenschaften erfüllt:

(5.1) Definition (Äquivalenzrelation)**.** Es sei eine Menge X gegeben. Eine *Äquivalenzrelation* auf X ist eine Relation auf X, welche transitiv, reflexiv und symmetrisch ist.

(5.2) Beispiel.

(a) Für $x, y \in \mathbb{R}$ gelte genau dann $x \; c \; y$, wenn $x = y$ oder $x = -y$ ist. Dann ist c eine Äquivalenzrelation auf $\mathbb{R}$.

(b) Für $x, y \in \mathbb{Z}$ gelte genau dann $x \equiv_2 y$, wenn x und y entweder beide gerade oder beide ungerade sind. Dann ist $\equiv_2$ eine Äquivalenzrelation auf $\mathbb{Z}$.

(c) Es sei c die Relation auf $\{1, 2, 3, 4\}$ gegeben durch

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

Dann ist c eine Äquivalenzrelation auf $\{1, 2, 3, 4\}$.

(d) Für jede Menge X ist die Gleichheitsrelation $=$ auf X eine Äquivalenzrelation auf X.

Beweis.

(a) Es seien $x, y, z \in \mathbb{R}$ mit $x \; c \; y$ und $y \; c \; z$ gegeben. Dann gilt $x = y$ oder $x = -y$, sowie $y = z$ oder $y = -z$. Wir erhalten

$$x = \left\{ \begin{matrix} y, & \text{falls } x = y, \\ -y, & \text{falls } x = -y \end{matrix} \right\} = \left\{ \begin{matrix} z, & \text{falls } x = y,\ y = z, \\ -z, & \text{falls } x = y,\ y = -z, \\ -z, & \text{falls } x = -y,\ y = z, \\ -(-z), & \text{falls } x = -y,\ y = -z \end{matrix} \right\}$$

$$= \begin{cases} z, & \text{falls } x = y,\ y = z \text{ oder } x = -y,\ y = -z, \\ -z, & \text{falls } x = y,\ y = -z \text{ oder } x = -y,\ y = z. \end{cases}$$

Also ist $x = z$ oder $x = -z$, und damit $x \; c \; z$. Folglich ist c transitiv.

Da für alle $x \in \mathbb{R}$ wegen $x = x$ auch $x \; c \; x$ gilt, ist c reflexiv.

Es seien $x, y \in \mathbb{R}$ mit $x \; c \; y$ gegeben. Dann gilt $x = y$ oder $x = -y$, also auch $y = x$ oder $y = -x$ und damit $y \; c \; x$. Folglich ist c symmetrisch.

Insgesamt ist c eine Äquivalenzrelation auf $\mathbb{R}$.

(b) Es seien $x, y, z \in \mathbb{Z}$ mit $x \equiv_2 y$ und $y \equiv_2 z$ gegeben. Wenn x gerade ist, dann ist wegen $x \equiv_2 y$ auch y gerade und wegen $y \equiv_2 z$ dann auch z gerade. Wenn x ungerade ist, dann ist wegen $x \equiv_2 y$ auch y ungerade und wegen $y \equiv_2 z$ dann auch z ungerade. Also sind x und z entweder beide gerade oder beide ungerade, d.h. es gilt $x \equiv_2 z$. Folglich ist $\equiv_2$ transitiv.

Da x entweder gerade oder ungerade ist, ist $\equiv_2$ reflexiv.

Die Symmetrie von $\equiv_2$ folgt aus der symmetrischen Definition von $\equiv_2$.

Insgesamt ist $\equiv_2$ eine Äquivalenzrelation auf $\mathbb{Z}$. □

(5.3) Anwendungsbeispiel.

(a) Die Studierenden des Moduls *Diskrete Strukturen* seien als Elemente einer Menge D modelliert. Für $s, t \in D$ gelte genau dann $s\ e\ t$, wenn der oder die durch s modellierte Studierende die gleichen Eltern wie der oder die durch t modellierte Studierende hat. Für $s, t \in D$ gelte genau dann $s\ g\ t$, wenn der oder die durch s modellierte Studierende den gleichen Geburtstag wie der oder die durch t modellierte Studierende hat. Dann sind e und g Äquivalenzrelationen auf D.

(b) Die Stichwörter in einem Lexikon seien als Elemente einer Menge L modelliert. Für $v, w \in L$ gelte genau dann $v\ a\ w$, wenn das durch v modellierte Stichwort den gleichen Anfangsbuchstaben wie das durch w modellierte Stichwort hat. Dann ist a eine Äquivalenzrelation auf L.

(c) Farbige Glasperlen in einer Dose seien als Elemente einer Menge P modelliert. Für $p, q \in P$ gelte genau dann $p\ f\ q$, wenn die durch p modellierte Glasperle die gleiche Farbe wie die durch q modellierte Glasperle hat. Dann ist f eine Äquivalenzrelation auf P.

(5.4) Bemerkung. Es seien eine Menge X, eine nicht leere Menge I und eine Familie $(c_i)_{i \in I}$ von Äquivalenzrelationen auf X gegeben. Für $x, y \in X$ gelte genau dann $x\ c\ y$, wenn für $i \in I$ stets $x\ c_i\ y$ gilt. Dann ist c eine Äquivalenzrelation auf X.

Beweis. Dies sei dem Leser zur Übung überlassen. □

Quotientenmengen

Die bzgl. einer Äquivalenzrelation in Relation stehenden Elemente wollen wir nun zu Teilmengen zusammenfassen:

(5.5) Definition (Äquivalenzklasse)**.** Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Für $x \in X$ heißt

$$[x] = [x]_c := \{\tilde{x} \in X \mid \tilde{x}\ c\ x\}$$

die *Äquivalenzklasse* von x in X bzgl. c, und es heißt x ein *Repräsentant* von $[x]_c$.

Wir greifen die Beispiele aus (5.2) noch einmal auf:

(5.6) Beispiel.

(a) Für $x, y \in \mathbb{R}$ gelte genau dann $x\ c\ y$, wenn $x = y$ oder $x = -y$ ist. Dann ist

$$[x]_c = \{x, -x\}$$

für $x \in \mathbb{R}$.

(b) Für $x, y \in \mathbb{Z}$ gelte genau dann $x \equiv_2 y$, wenn x und y entweder beide gerade oder beide ungerade sind. Dann ist

$$[0]_{\equiv_2} = 2\mathbb{Z} = \{2q \mid q \in \mathbb{Z}\},$$
$$[1]_{\equiv_2} = 2\mathbb{Z} + 1 = \{2q + 1 \mid q \in \mathbb{Z}\}$$

(c) Es sei c die Äquivalenzrelation auf $\{1,2,3,4\}$ gegeben durch

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

Dann ist

$$[1]_c = [2]_c = [4]_c = \{1,2,4\},$$
$$[3]_c = \{3\}.$$

(d) Es sei eine Menge X gegeben. Dann ist

$$[x]_= = \{x\}$$

für alle $x \in X$.

(5.7) Proposition. Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben.

(a) Für $x \in X$ ist $x \in [x]_c$.

(b) Für $x, y \in X$ sind die folgenden Bedingungen äquivalent:

(i) Es ist $[x]_c = [y]_c$.
(ii) Es ist $[x]_c \subseteq [y]_c$.
(iii) Es gilt $x \; c \; y$.

Beweis.

(a) Da c reflexiv ist, haben wir $x \; c \; x$ und damit $x \in [x]$ für alle $x \in X$.

(b) Es seien $x, y \in X$ gegeben.

Wenn $[x] \subseteq [y]$ gilt, dann haben wir $x \in [x] \subseteq [y]$ nach (a) und somit $x \; c \; y$. Es sei also umgekehrt angenommen, dass $x \; c \; y$ gilt. Für alle $\tilde{x} \in [x]$ haben wir $\tilde{x} \; c \; x$, die Transitivität von c liefert also $\tilde{x} \; c \; y$, d.h. $\tilde{x} \in [y]$. Folglich ist $[x] \subseteq [y]$.

Somit gilt genau dann $[x] \subseteq [y]$, wenn $x \; c \; y$ ist; wir haben also die Äquivalenz von Bedingung (ii) und Bedingung (iii) gezeigt. Nun ist aber c symmetrisch, d.h. aus $x \; c \; y$ folgt $y \; c \; x$. Folglich impliziert $[x] \subseteq [y]$ bereits $[y] \subseteq [x]$ und damit $[x] = [y]$. Da $[x] = [y]$ aber stets $[x] \subseteq [y]$ impliziert, sind auch Bedingung (i) und Bedingung (ii) äquivalent.

Insgesamt sind Bedingung (i), Bedingung (ii) und Bedingung (iii) äquivalent. □

Als nächstes wollen wir die Äquivalenzklassen bzgl. einer Äquivalenzrelation wieder zu einer Menge zusammenfassen:

(5.8) Definition (Quotientenmenge)**.** Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Die Menge

$$X/c := \{[x]_c \mid x \in X\}$$

heißt *Quotientenmenge* (oder *Quotient*) von X modulo c. Die Abbildung

$$\mathrm{quo} = \mathrm{quo}^{X/c} \colon X \to X/c,\ x \mapsto [x]_c$$

wird *Quotientenabbildung* von X/c genannt.

Wir bestimmen die Quotientenmenge im Fall von Beispiel (5.2)(c):

(5.9) Beispiel. Es sei c die Äquivalenzrelation auf $\{1,2,3,4\}$ gegeben durch

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

Dann ist

$$\{1,2,3,4\}/c = \{[1]_c, [3]_c\}.$$

Beweis. Nach Beispiel (5.6)(c) ist $[1] = [2] = [4]$ und damit

$$\{1,2,3,4\}/c = \{[1],[2],[3],[4]\} = \{[1],[3]\}.$$ □

Unter der Quotientenmenge einer Menge X bzgl. einer Äquivalenzrelation c auf X stellen wir uns eine „Vergröberung" der Menge X vor. Diejenigen Elemente in X, welche in X nur äquivalent bzgl. c sind, werden über die Quotientenabbildung zu gleichen Elementen in der Quotientenmenge.

(5.10) Definition (Transversale)**.** Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Eine *Transversale* (oder ein *Repräsentantensystem*) von X bzgl. c (oder eine *Transversale* von X/c) ist eine Teilmenge T von X so, dass es für jedes $K \in X/c$ genau ein $t \in T$ mit $K = [t]_c$ gibt.

Wir bestimmen einige Transversalen für die Äquivalenzrelationen aus Beispiel (5.2):

(5.11) Beispiel.

(a) Für $x, y \in \mathbb{R}$ gelte genau dann $x\ c\ y$, wenn $x = y$ oder $x = -y$ ist. Dann sind $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} \mid x \geq 0\}$, $\mathbb{R}_{\leq 0} = \{x \in \mathbb{R} \mid x \leq 0\}$ und $\{x \in \mathbb{R} \mid x < -2 \text{ oder } 0 \leq x \leq 2\}$ Transversalen von $\mathbb{R}$ bzgl. c.

(b) Für $x, y \in \mathbb{Z}$ gelte genau dann $x \equiv_2 y$, wenn x und y entweder beide gerade oder beide ungerade sind. Dann sind $\{0,1\}$, $\{1,2\}$, $\{-3,88\}$ Transversalen von $\mathbb{Z}$ bzgl. $\equiv_2$.

(c) Es sei c die Äquivalenzrelation auf $\{1,2,3,4\}$ gegeben durch

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

Dann sind $\{1,3\}$, $\{2,3\}$, $\{3,4\}$ Transversalen von $\{1,2,3,4\}$ bzgl. c.

(d) Es sei eine Menge X gegeben. Dann ist X die einzige Transversale von X bzgl. $=$.

Der Homomorphiesatz für Mengen

Wir werden nun sehen, dass jede Abbildung Anlass zu einer Äquivalenzrelation gibt, welche schließlich zu einer Bijektion führt.

(5.12) Definition (Bildgleichheit)**.** Es sei eine Abbildung $f\colon X \to Y$ gegeben. Für $x, \tilde{x} \in X$ gelte genau dann $x =_f \tilde{x}$, wenn $f(x) = f(\tilde{x})$ ist. Die Relation $=_f$ auf X heißt *Bildgleichheit* bzgl. f.

(5.13) Beispiel. Es sei $f\colon \{1,2,3,4\} \to \mathbb{Z}$, $1 \mapsto 1$, $2 \mapsto 1$, $3 \mapsto 3$, $4 \mapsto 1$. Die Bildgleichheit $=_f$ ist gegeben durch

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

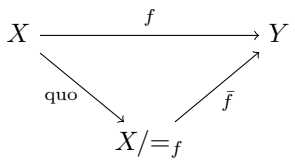
(5.14) Bemerkung. Für jede Abbildung $f\colon X \to Y$ ist $=_f$ eine Äquivalenzrelation auf X.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(5.15) Satz (Homomorphiesatz für Mengen)**.** Es sei eine Abbildung $f\colon X \to Y$ gegeben. Dann haben wir eine induzierte Abbildung $\bar{f}\colon X/{=_f} \to Y$, $[x] \mapsto f(x)$, welche $f = \bar{f} \circ \mathrm{quo}$ erfüllt. Es ist $\bar{f}$ injektiv und $\operatorname{Im} \bar{f} = \operatorname{Im} f$. Insbesondere ist

$$\bar{f}|^{\operatorname{Im} f}\colon X/{=_f} \to \operatorname{Im} f$$

eine Bijektion.



Beweis. Für $x, x' \in X$ ist nach Proposition (5.7)(b) genau dann $[x] = [x']$ in $X/{=_f}$, wenn $x =_f x'$ in X gilt, und dies ist nach Definition von $=_f$ äquivalent zu $f(x) = f(x')$ in Y. Folglich ist $\bar{f}\colon X/{=_f} \to Y$, $[x] \mapsto f(x)$ eine wohldefinierte, injektive Abbildung. Da für $x \in X$ stets

$$\bar{f}(\mathrm{quo}(x)) = \bar{f}([x]) = f(x)$$

ist, gilt $f = \bar{f} \circ \mathrm{quo}$. Ferner ist

$$\mathrm{Im}\, \bar{f} = \{\bar{f}(K) \mid K \in X/c\} = \{\bar{f}([x]) \mid x \in X\} = \{f(x) \mid x \in X\} = \mathrm{Im}\, f. \qquad \square$$

(5.16) Beispiel. Es sei $f\colon \{1,2,3,4\} \to \mathbb{Z}$, $1 \mapsto 1$, $2 \mapsto 1$, $3 \mapsto 3$, $4 \mapsto 1$. Dann ist $\{1,2,3,4\}/{=_f} = \{[1],[3]\}$ und es gilt $f = \bar{f} \circ \mathrm{quo}$ mit $\bar{f}\colon \{1,2,3,4\}/{=_f} \to \mathbb{Z}$, $[1] \mapsto 1$, $[3] \mapsto 3$.

Wir erläutern den Homomorphiesatz für Mengen (5.15) auch noch an einem Beispiel aus dem täglichen Leben:

(5.17) Anwendungsbeispiel. Farbige Glasperlen in einer Dose seien als Elemente einer Menge P modelliert. Farben seien als Elemente einer Menge C modelliert. Die Zuordnung der zugehörigen Farbe zu jeder Glasperle sei als Abbildung $a\colon P \to C$ modelliert. Für $p, q \in P$ gilt genau dann $p =_a q$, wenn die durch p modellierte Glasperle die gleiche Farbe wie die durch q modellierte Glasperle hat. Eine Äquivalenzklasse bzgl. $=_a$ entspricht der Gesamtheit aller Glasperlen einer Farbe. Die Quotientenmenge $P/{=_a}$ entspricht einer „Sortierung“ aller Glasperlen nach Farben; die Quotientenabbildung $\mathrm{quo}\colon P \to P/{=_a}$ entspricht der Zuordnung jeder Perle zu ihrem „Farbhäufchen“; und die induzierte Abbildung $\bar{a}\colon P/{=_a} \to C$ entspricht der Zuordnung jedes Häufchens zu „seiner“ Farbe.

Partitionen

Zum Abschluss beleuchten wir noch den mengentheoretischen Aspekt von Quotientenmengen etwas genauer: Jede Äquivalenzrelation c auf einer Menge X partitioniert (also unterteilt) via X/c die Menge X in Teilmengen, nämlich in die Elemente von X/c. Gehen wir umgekehrt von einer Unterteilung von X in Teilmengen aus, so liefert uns dies wiederum eine Äquivalenzrelation, indem wir zwei Elemente als äquivalent betrachten, wenn sie im gleichen Teil der Unterteilung liegen. Es lässt sich zeigen, dass sich diese Konstruktionen gegenseitig umkehren, siehe den Hauptsatz über Äquivalenzrelationen (5.20).
Zunächst präzisieren wir, was wir unter einer Unterteilung einer Menge verstehen wollen:

(5.18) Definition (Partition)**.** Es sei eine Menge X gegeben. Eine *Partition* (genauer *Mengenpartition*) von X ist eine Teilmenge $\mathcal{P}$ von $\mathrm{Pot}(X)$ so, dass $\emptyset \notin \mathcal{P}$ und

$$X = \dot{\bigcup_{P \in \mathcal{P}}} P.$$

Für $x \in X$ heißt das eindeutige $P \in \mathcal{P}$ mit $x \in P$ der *Teil* von x in $\mathcal{P}$.

(5.19) Beispiel. Es ist $\{\{1,2,4\},\{3\}\}$ eine Partition von $\{1,2,3,4\}$.

(5.20) Satz (Hauptsatz über Äquivalenzrelationen)**.** Es sei eine Menge X gegeben. Wir haben eine wohldefinierte Bijektion

$$X/{-}\colon \{c \mid c \text{ ist Äquivalenzrelation auf } X\} \to \{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } X\},\ c \mapsto X/c.$$

Für jede Partition $\mathcal{P}$ von X ist die eindeutige Äquivalenzrelation c auf X mit $\mathcal{P} = X/c$ wie folgt gegeben: Für $x, y \in X$ gilt genau dann $x\, c\, y$, wenn es ein $P \in \mathcal{P}$ mit $x \in P$ und $y \in P$ gibt.

Beweis. Zunächst sei eine Äquivalenzrelation c gegeben. Dann ist $X/c = \{[x]_c \mid x \in X\}$. Für alle $K \in X/c$ gibt es also ein $x \in X$ mit $K = [x]_c$, und mit Proposition (5.7)(a) folgt $x \in [x]_c = K$. Insbesondere ist $K \neq \emptyset$ für alle $K \in X/c$ und damit $\emptyset \notin X/c$. Für $x \in X$ gilt ferner

$$x \in [x]_c \subseteq \bigcup_{y \in X} [y]_c = \bigcup_{K \in X/c} K,$$

es ist also $X = \bigcup_{K \in X/c} K$. Um die Disjunktheit von $(K)_{K \in X/c}$ zu zeigen, seien $K, L \in X/c$ mit $K \cap L \neq \emptyset$ gegeben. Ferner seien $x, y, z \in X$ mit $K = [x]_c$, $L = [y]_c$ und $z \in K \cap L$ gegeben. Wegen $z \in K = [x]_c$

gilt $z\ c\ x$ und wegen $z \in L = [y]_c$ gilt $z\ c\ y$. Wir erhalten also $x\ c\ y$ und somit $K = [x]_c = [y]_c = L$ nach Proposition (5.7)(b). Insgesamt ist X/c eine Partition von X.
Somit haben wir eine wohldefinierte Abbildung

$$X/{-}\colon \{c \mid c \text{ ist Äquivalenzrelation auf } X\} \to \{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } X\},\ c \mapsto X/c.$$

Umgekehrt sei eine Partition $\mathcal{P}$ von X gegeben. Da $(P)_{P\in\mathcal{P}}$ disjunkt ist, gibt es für jedes $x \in X$ genau ein $P \in \mathcal{P}$ mit $x \in P$. Somit haben wir eine Abbildung $q_{\mathcal{P}}\colon X \to \mathcal{P}$ mit $x \in q_{\mathcal{P}}(x)$. Die Bildgleichheit $=_{q_{\mathcal{P}}}$ ist nach Bemerkung (5.14) eine Äquivalenzrelation auf X.
Folglich haben wir auch eine wohldefinierte Abbildung

$$=_{q_-}\colon \{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } X\} \to \{c \mid c \text{ ist Äquivalenzrelation auf } X\},\ \mathcal{P} \mapsto =_{q_{\mathcal{P}}}.$$

Wir wollen zeigen, dass sich die Abbildungen $X/-$ und $=_{q_-}$ gegenseitig invertieren. Für jede Äquivalenzrelation c auf X gilt

$$\begin{aligned} =_{q_{X/c}} &= \{(x,y) \in X \times X \mid q_{X/c}(x) = q_{X/c}(y)\} = \{(x,y) \in X \times X \mid [x]_c = [y]_c\} \\ &= \{(x,y) \in X \times X \mid x\ c\ y\} = c \end{aligned}$$

nach Proposition (5.7)(b). Folglich ist $=_{q_-} \circ X/- = \mathrm{id}_{\{c \mid c \text{ ist Äquivalenzrelation auf } X\}}$ nach dem Gleichheitskriterium für Abbildungen (3.6). Umgekehrt sei eine Partition $\mathcal{P}$ von X gegeben. Für $x, y \in X$ gilt genau dann $y =_{q_{\mathcal{P}}} x$, wenn $q_{\mathcal{P}}(y) = q_{\mathcal{P}}(x)$ ist, und da $(P)_{P\in\mathcal{P}}$ disjunkt ist, ist dies äquivalent zu $y \in q_{\mathcal{P}}(x)$. Folglich ist

$$[x]_{=_{q_{\mathcal{P}}}} = \{y \in X \mid y =_{q_{\mathcal{P}}} x\} = q_{\mathcal{P}}(x)$$

für $x \in X$, also

$$X/{=_{q_{\mathcal{P}}}} = \{[x]_{=_{q_{\mathcal{P}}}} \mid x \in X\} = \{q_{\mathcal{P}}(x) \mid x \in X\} = \mathcal{P}.$$

Nach dem Gleichheitskriterium für Abbildungen (3.6) ist somit auch $X/- \circ =_{q_-} = \mathrm{id}_{\{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } X\}}$.
Insgesamt sind $X/-$ und $=_{q_-}$ zueinander inverse Abbildungen. □

Zusätzliche Konzepte

Im Folgenden geben wir eine zusätzliche Definition, deren Studium dem Leser zur Übung überlassen sei.

(5.21) Definition (erzeugte Äquivalenzrelation)**.** Es seien eine Menge X und eine Relation r auf X gegeben. Für eine Äquivalenzrelation c auf X sagen wir, dass c von r *erzeugt* wird, falls $r \subseteq c$ gilt und falls für jede Äquivalenzrelation d auf X aus $r \subseteq d$ stets $c \subseteq d$ folgt.

(5.22) Proposition. Es seien eine Menge X und eine Relation r auf X gegeben. Es gibt genau eine von r erzeugte Äquivalenzrelation auf X. Die von r erzeugte Äquivalenzrelation ist durch den transitiv-reflexiven Abschluss des symmetrischen Abschlusses von r gegeben.

Beweis. Dies sei dem Leser zur Übung überlassen. □

6 Algebraische Strukturen

Bisher haben wir Mengen und Abbildungen zwischen Mengen betrachtet. Die aus der Schule bekannten Mengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ haben jedoch neben der Zusammenfassung ihrer Elemente noch mehr Struktur – wir können etwa Elemente addieren und multiplizieren. Dieser Aspekt soll in diesem Abschnitt formalisiert werden. Wir beleuchten die algebraische Struktur dieser Zahlbereiche und gelangen dadurch zu Begriffen wie Gruppe und Ring, von denen wir im weiteren Verlauf auch neue Beispiele kennenlernen werden. ([34])

[34] Ein universeller Blick auf algebraische Strukturen wird in Vorlesungen über *universelle Algebra* gegeben. Am Rande taucht ein allgemeiner Zugang, welcher auch die in Abschnitt 8 einzuführenden Ordnungsstrukturen und andere relationale Strukturen umschließt, bei der formalen Behandlung der Prädikatenlogik auf; an der RWTH Aachen üblicherweise im Rahmen der Vorlesung *Mathematische Logik* (etwa 4. Semester im Studiengang B.Sc. Informatik).

Verknüpfungen

Unser intuitives Verständnis der Zahlbereiche lässt an der Gültigkeit des folgenden Satzes keinen Zweifel:

(6.1) Satz.

(a) (i) Für $x, y, z \in \mathbb{N}$ gilt $x + (y + z) = (x + y) + z$.
(ii) Für $x, y \in \mathbb{N}$ gilt $x + y = y + x$.
(iii) Für $x, y, z \in \mathbb{N}$ gilt $x(yz) = (xy)z$.
(iv) Für $x \in \mathbb{N}$ gilt $1x = x1 = x$.
(v) Für $x, y \in \mathbb{N}$ gilt $xy = yx$.

(b) (i) Für $x, y, z \in \mathbb{N}_0$ gilt $x + (y + z) = (x + y) + z$.
(ii) Für $x \in \mathbb{N}_0$ gilt $0 + x = x + 0 = x$.
(iii) Für $x, y \in \mathbb{N}_0$ gilt $x + y = y + x$.
(iv) Für $x, y, z \in \mathbb{N}_0$ gilt $x(yz) = (xy)z$.
(v) Für $x \in \mathbb{N}_0$ gilt $1x = x1 = x$.
(vi) Für $x, y \in \mathbb{N}_0$ gilt $xy = yx$.

(c) (i) Für $x, y, z \in \mathbb{Z}$ gilt $x + (y + z) = (x + y) + z$.
(ii) Für $x \in \mathbb{Z}$ gilt $0 + x = x + 0 = x$.
(iii) Für $x \in \mathbb{Z}$ gilt $(-x) + x = x + (-x) = 0$.
(iv) Für $x, y \in \mathbb{Z}$ gilt $x + y = y + x$.
(v) Für $x, y, z \in \mathbb{Z}$ gilt $x(yz) = (xy)z$.
(vi) Für $x \in \mathbb{Z}$ gilt $1x = x1 = x$.
(vii) Für $x, y \in \mathbb{Z}$ gilt $xy = yx$.
(viii) Für $x, y, z \in \mathbb{Z}$ gilt $x(y + z) = xy + xz$ und $(x + y)z = xz + yz$.

(d) (i) Für $x, y, z \in \mathbb{Q}$ gilt $x + (y + z) = (x + y) + z$.
(ii) Für $x \in \mathbb{Q}$ gilt $0 + x = x + 0 = x$.
(iii) Für $x \in \mathbb{Q}$ gilt $(-x) + x = x + (-x) = 0$.
(iv) Für $x, y \in \mathbb{Q}$ gilt $x + y = y + x$.
(v) Für $x, y, z \in \mathbb{Q}$ gilt $x(yz) = (xy)z$.
(vi) Für $x \in \mathbb{Q}$ gilt $1x = x1 = x$.
(vii) Für $x \in \mathbb{Q} \setminus \{0\}$ gilt $x^{-1}x = xx^{-1} = 1$.
(viii) Für $x, y \in \mathbb{Q}$ gilt $xy = yx$.
(ix) Für $x, y, z \in \mathbb{Q}$ gilt $x(y + z) = xy + xz$ und $(x + y)z = xz + yz$.

Die Rechenregeln aus Satz (6.1) geben die grundsätzlichen Eigenschaften der Addition und der Multiplikation von rationalen Zahlen und gewissen Teilmengen wieder. Im Folgenden wollen wir diese Eigenschaften genauer analysieren, formalisieren und so zu neuen Begrifflichkeiten auf einer abstrakten Ebene gelangen, welche sich dann wiederum bei weiteren Beispielen in ganz anderen Bereichen verwenden lassen.
Zunächst müssen wir uns darüber im Klaren werden, was eine Addition bzw. eine Multiplikation eigentlich ist. Bei der Addition natürlicher Zahlen x und y ordnen wir diesen ihre Summe $x + y$ zu. In Abschnitt 3 haben wir gesehen, dass sich solche Zuordnungen mit Hilfe von Abbildungen formalisieren lassen. Da jeder Ausdruck der Form $x + y$ aus den beiden Summanden x und y entsteht, ordnen wir bei der Addition einem Paar (x, y) in $\mathbb{N}$, also einem Element in $\mathbb{N} \times \mathbb{N}$, das Element $x + y$ in $\mathbb{N}$ zu. Bei der Addition handelt es sich also um eine Abbildung

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N},\ (x, y) \mapsto x + y.$$

Wir werden nun Abbildungen von dieser Form systematisch studieren und ihnen deswegen eine eigene Bezeichnung verleihen.

(6.2) Definition (Verknüpfung)**.** Es sei eine Menge X gegeben. Eine *Verknüpfung* (oder *binäre algebraische Operation*) auf X ist eine Abbildung $m\colon X \times X \to X$. Für $(x, y) \in X \times X$ schreiben wir $x\, m\, y := m(x, y)$.

Da zu einer gegebenen Menge X die Start- und die Zielmenge einer Verknüpfung auf X eindeutig festgelegt sind ($X \times X$ bzw. X), lassen wir diese Angaben im Folgenden meist weg.

(6.3) Beispiel.

(a) Auf $\mathbb{N}$ haben wir die Verknüpfungen $(x, y) \mapsto x + y$ und $(x, y) \mapsto x \cdot y$.

(b) Auf $\mathbb{N}_0$ haben wir die Verknüpfungen $(x, y) \mapsto x + y$ und $(x, y) \mapsto x \cdot y$.

(c) Auf $\mathbb{Z}$ haben wir die Verknüpfungen $(x, y) \mapsto x + y$ und $(x, y) \mapsto x - y$ und $(x, y) \mapsto x \cdot y$.

(d) Auf $\mathbb{Q}$ haben wir die Verknüpfungen $(x, y) \mapsto x + y$ und $(x, y) \mapsto x - y$ und $(x, y) \mapsto x \cdot y$.

Verknüpfungen auf endlichen Mengen lassen sich durch *Verknüpfungstafeln* verbildlichen:

(6.4) Beispiel.

(a) Es seien verschiedene Objekte a, b, c gegeben. Auf $\{a, b, c\}$ haben wir eine Verknüpfung m, welche durch folgende Verknüpfungstafel gegeben ist:

m	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

(b) Es seien verschiedene Objekte a, b, c, d, e gegeben. Auf $\{a, b, c, d, e\}$ haben wir eine Verknüpfung m, welche durch folgende Verknüpfungstafel gegeben ist:

m	a	b	c	d	e
a	b	c	d	e	a
b	d	e	a	c	b
c	e	d	b	a	c
d	c	a	e	b	d
e	a	b	c	d	e

Natürlich gibt es auf $\mathbb{N}$ und den anderen Zahlbereichen noch viel mehr Verknüpfungen, doch diese beiden zeichnen sich durch besondere Eigenschaften aus, wie wir in Satz (6.1) gesehen haben. Wir wollen diese Eigenschaften nun für allgemeine Verknüpfungen studieren.

(6.5) Definition (Assoziativität, Kommutativität)**.** Es seien eine Menge X und eine Verknüpfung m auf X gegeben.

(a) Wir sagen, dass m *assoziativ* ist, wenn für $x, y, z \in X$ stets

$$x\, m\, (y\, m\, z) = (x\, m\, y)\, m\, z$$

gilt.

(b) Wir sagen, dass m *kommutativ* ist, wenn für $x, y \in X$ stets

$$x\, m\, y = y\, m\, x$$

gilt.

Die Aussagen aus Satz (6.1)(a)(i), (ii), (iii), (v) lassen sich nun auch kurz wie folgt formulieren:

(6.6) Beispiel. Die Verknüpfungen $(x, y) \mapsto x + y$ und $(x, y) \mapsto x \cdot y$ auf $\mathbb{N}$ sind assoziativ und kommutativ.

(6.7) Beispiel.

(a) Es seien verschiedene Objekte a, b, c gegeben und auf $\{a, b, c\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Dann ist m assoziativ und kommutativ.

(b) Es seien verschiedene Objekte a, b, c, d, e gegeben und auf $\{a, b, c, d, e\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c	d	e
a	b	c	d	e	a
b	d	e	a	c	b
c	e	d	b	a	c
d	c	a	e	b	d
e	a	b	c	d	e

Dann ist m nicht assoziativ und nicht kommutativ.

Beweis.

(a) Wegen

$$
\begin{aligned}
&a\,m\,(a\,m\,a) = a\,m\,a = a = a\,m\,a = (a\,m\,a)\,m\,a,\\
&a\,m\,(a\,m\,b) = a\,m\,b = b = a\,m\,b = (a\,m\,a)\,m\,b,\\
&a\,m\,(a\,m\,c) = a\,m\,c = c = a\,m\,c = (a\,m\,a)\,m\,c,\\
&a\,m\,(b\,m\,a) = a\,m\,b = b = b\,m\,a = (a\,m\,b)\,m\,a,\\
&a\,m\,(b\,m\,b) = a\,m\,c = c = b\,m\,b = (a\,m\,b)\,m\,b,\\
&a\,m\,(b\,m\,c) = a\,m\,a = a = b\,m\,c = (a\,m\,b)\,m\,c,\\
&a\,m\,(c\,m\,a) = a\,m\,c = c = c\,m\,a = (a\,m\,c)\,m\,a,\\
&a\,m\,(c\,m\,b) = a\,m\,a = a = c\,m\,b = (a\,m\,c)\,m\,b,\\
&a\,m\,(c\,m\,c) = a\,m\,b = b = c\,m\,c = (a\,m\,c)\,m\,c,\\
&b\,m\,(a\,m\,a) = b\,m\,a = b = a\,m\,a = (b\,m\,a)\,m\,a,\\
&b\,m\,(a\,m\,b) = b\,m\,b = c = a\,m\,b = (b\,m\,a)\,m\,b,\\
&b\,m\,(a\,m\,c) = b\,m\,c = a = a\,m\,c = (b\,m\,a)\,m\,c,\\
&b\,m\,(b\,m\,a) = b\,m\,b = c = b\,m\,a = (b\,m\,b)\,m\,a,\\
&b\,m\,(b\,m\,b) = b\,m\,c = a = b\,m\,b = (b\,m\,b)\,m\,b,\\
&b\,m\,(b\,m\,c) = b\,m\,a = b = b\,m\,c = (b\,m\,b)\,m\,c,\\
&b\,m\,(c\,m\,a) = b\,m\,c = a = c\,m\,a = (b\,m\,c)\,m\,a,\\
&b\,m\,(c\,m\,b) = b\,m\,a = b = c\,m\,b = (b\,m\,c)\,m\,b,\\
&b\,m\,(c\,m\,c) = b\,m\,b = c = c\,m\,c = (b\,m\,c)\,m\,c,\\
&c\,m\,(a\,m\,a) = c\,m\,a = c = c\,m\,a = (c\,m\,a)\,m\,a,\\
&c\,m\,(a\,m\,b) = c\,m\,b = a = c\,m\,b = (c\,m\,a)\,m\,b,\\
&c\,m\,(a\,m\,c) = c\,m\,c = b = c\,m\,c = (c\,m\,a)\,m\,c,\\
&c\,m\,(b\,m\,a) = c\,m\,b = a = a\,m\,a = (c\,m\,b)\,m\,a,\\
&c\,m\,(b\,m\,b) = c\,m\,c = b = a\,m\,b = (c\,m\,b)\,m\,b,\\
&c\,m\,(b\,m\,c) = c\,m\,a = c = a\,m\,c = (c\,m\,b)\,m\,c,\\
&c\,m\,(c\,m\,a) = c\,m\,c = b = b\,m\,a = (c\,m\,c)\,m\,a,
\end{aligned}
$$

$$c\,m\,(c\,m\,b) = c\,m\,a = c = b\,m\,b = (c\,m\,c)\,m\,b,$$
$$c\,m\,(c\,m\,c) = c\,m\,b = a = b\,m\,c = (c\,m\,c)\,m\,c$$

ist m assoziativ.

Wegen

$$a\,m\,b = b = b\,m\,a,$$
$$a\,m\,c = c = c\,m\,a,$$
$$b\,m\,c = a = c\,m\,a$$

gilt $x\,m\,y = y\,m\,x$ für alle $x, y \in \{a, b, c\}$ mit $x \neq y$. Da für $x, y \in \{a, b, c\}$ mit $x = y$ ebenfalls $x\,m\,y = x\,m\,x = y\,m\,x$ gilt, ist m somit kommutativ.

(b) Wegen

$$b\,m\,(a\,m\,a) = b\,m\,b = e \neq c = d\,m\,a = (b\,m\,a)\,m\,a$$

ist m nicht assoziativ. Wegen

$$a\,m\,b = c \neq d = b\,m\,a$$

ist m nicht kommutativ. □

In Satz (6.1)(a)(iv) haben wir gesehen, dass dem Element $1 \in \mathbb{N}$ eine besondere Stellung bzgl. der Multiplikation von natürlichen Zahlen zukommt: Multipliziert man ein Element $x \in \mathbb{N}$ mit 1, egal von welcher Seite, so erhält man als Produkt das Element x zurück. Eine ganz ähnliche Rolle hat das Element $0 \in \mathbb{N}_0$ bzgl. der Addition von $\mathbb{N}_0$, siehe Satz (6.1)(b)(ii): Addiert man 0 zu einem Element $x \in \mathbb{N}_0$, so bekommt man als Summe wieder x. Wir abstrahieren wieder:

(6.8) Definition (neutrales Element)**.** Es seien eine Menge X und eine Verknüpfung m auf X gegeben. Ein *neutrales Element* (in X) bzgl. m ist ein Element e in X, welches

$$e\,m\,x = x\,m\,e = x$$

für alle $x \in X$ erfüllt.

(6.9) Beispiel. Es ist 1 ein neutrales Element bzgl. der Verknüpfung $(x, y) \mapsto x \cdot y$ auf $\mathbb{N}$.

(6.10) Beispiel.

(a) Es seien verschiedene Objekte a, b, c gegeben und auf $\{a, b, c\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Dann ist a ein neutrales Element in $\{a, b, c\}$ bzgl. m.

(b) Es seien verschiedene Objekte a, b, c, d, e gegeben und auf $\{a, b, c, d, e\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c	d	e
a	b	c	d	e	a
b	d	e	a	c	b
c	e	d	b	a	c
d	c	a	e	b	d
e	a	b	c	d	e

Dann ist e ein neutrales Element in $\{a, b, c, d, e\}$ bzgl. m.

Beweis.

(a) Wegen $a\,m\,x = x\,m\,a = x$ für alle $x \in \{a, b, c\}$ ist a ein neutrales Element bzgl. m.

(b) Wegen $e\,m\,x = x\,m\,e = x$ für alle $x \in \{a, b, c, d, e\}$ ist e ein neutrales Element bzgl. m. □

Wir werden nun sehen, dass es bzgl. einer Verknüpfung niemals mehrere neutrale Elemente geben kann.

(6.11) Bemerkung. Es seien eine Menge X und eine Verknüpfung m auf X gegeben. Dann gibt es höchstens ein neutrales Element bzgl. m.

Beweis. Es seien neutrale Elemente e und e' in X bzgl. m gegeben. Da e neutral ist, gilt $emx = x$ für alle $x \in X$, also insbesondere $e\,m\,e' = e'$. Da e' neutral ist, gilt $x\,m\,e' = x$ für alle $x \in X$, also insbesondere $e\,m\,e' = e$. Insgesamt haben wir

$$e = e\,m\,e' = e'.$$ □

Die Addition auf $\mathbb{N}$ liefert ein Beispiel für eine Verknüpfung bzgl. derer es kein neutrales Element gibt.
Das wesentliche Merkmal, was die ganzen Zahlen von den natürlichen Zahlen unterscheidet, ist das Hinzukommen von negativen Elementen. Diese haben die Eigenschaft, dass sie zu dem entsprechenden positiven Element addiert die Zahl 0, das neutrale Element bzgl. der Addition, ergeben. Ganz ähnlich liefert die Multiplikation mit einem inversen Element in $\mathbb{Q}$ die Zahl 1, das neutrale Element bzgl. der Multiplikation.
Wir abstrahieren von der konkreten Situation:

(6.12) Definition (inverses Element)**.** Es seien eine Menge X, eine Verknüpfung m auf X, ein neutrales Element e bzgl. m und ein $x \in X$ gegeben.

(a) Ein *linksinverses Element* (in X) zu x bzgl. m ist ein Element y in X, welches $y\,m\,x = e$ erfüllt.

(b) Ein *rechtsinverses Element* (in X) zu x bzgl. m ist ein Element y in X, welches $x\,m\,y = e$ erfüllt.

(c) Ein *inverses Element* (in X) zu x bzgl. m ist ein Element y in X, welches links- und rechtsinvers zu x bzgl. m ist.

(6.13) Beispiel. Es ist $\frac{4}{3}$ ein zu $\frac{3}{4}$ inverses Element bzgl. der Verknüpfung $(m, n) \mapsto m \cdot n$ auf $\mathbb{Q}$.

(6.14) Beispiel.

(a) Es seien verschiedene Objekte a, b, c gegeben und auf $\{a, b, c\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Dann ist b ein zu c inverses Element in $\{a, b, c\}$ bzgl. m.

(b) Es seien verschiedene Objekte a, b, c, d, e gegeben und auf $\{a, b, c, d, e\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c	d	e
a	b	c	d	e	a
b	d	e	a	c	b
c	e	d	b	a	c
d	c	a	e	b	d
e	a	b	c	d	e

Dann ist b ein zu b inverses Element in $\{a, b, c, d, e\}$ bzgl. m. Ferner ist c linksinvers zu a und d rechtsinvers zu a bzgl. m.

Beweis.

(a) Nach Beispiel (6.10)(a) ist a ein neutrales Element bzgl. m. Wegen $b\,m\,c = c\,m\,b = a$ ist daher b ein zu c inverses Element bzgl. m.

(b) Nach Beispiel (6.10)(b) ist e ein neutrales Element bzgl. m. Wegen $b\,m\,b = e$ ist daher b ein zu b inverses Element bzgl. m. Wegen $c\,m\,a = e$ ist ferner c linksinvers zu a bzgl. m und wegen $a\,m\,d = e$ ist d rechtsinvers zu a bzgl. m. □

Wir haben hier zwischen linksinversen, rechtsinversen und inversen Elementen unterschieden, da es Situationen gibt, in welchen ein Element ein linksinverses Element, aber kein rechtsinverses Element hat, und umgekehrt. Ist die betrachtete Verknüpfung assoziativ, so kann es jedoch nicht passieren, dass ein Element verschiedene links- und rechtsinverse Elemente hat:

(6.15) Bemerkung. Es seien eine Menge X, eine assoziative Verknüpfung m auf X und ein neutrales Element e bzgl. m gegeben. Ferner seien $x \in X$, ein linksinverses Element y und ein rechtsinverses Element y' zu x bzgl. m gegeben. Dann gilt

$$y = y'.$$

Beweis. Da e neutral bzgl. m ist, gilt $y\,m\,e = y$ und $e\,m\,y' = y'$. Da y linksinvers zu x bzgl. m ist, gilt $y\,m\,x = e$. Da y' rechtsinvers zu x bzgl. m ist, gilt $x\,m\,y' = e$. Unter Ausnutzung der Assoziativität von m erhalten wir

$$y = y\,m\,e = y\,m\,(x\,m\,y') = (y\,m\,x)\,m\,y' = e\,m\,y' = y'.$$ □

Man vergleiche den Beweis der vorangegangenen Bemerkung (6.15) mit dem Beweis von Bemerkung (3.19).

(6.16) Korollar. Es seien eine Menge X, eine assoziative Verknüpfung m auf X, ein neutrales Element e bzgl. m und ein $x \in X$ gegeben. Dann gibt es höchstens ein inverses Element zu x bzgl. m.

Beweis. Es seien inverse Elemente y und y' zu x gegeben. Dann ist y insbesondere linksinvers und y' insbesondere rechtsinvers zu x bzgl. m, so dass aus Bemerkung (6.15) bereits $y = y'$ folgt. □

Halbgruppen und Monoide

Als nächstes wollen wir uns davon lösen, Verknüpfungen als eigenständige Objekte zu betrachten. Wir wollen den Standpunkt einnehmen, dass Verknüpfungen „fest“ zu einer Menge dazugehören, und wollen die Menge zusammen mit den Verknüpfungen als eine gemeinsame „algebraische Struktur“ ansehen.
Obwohl wir auf $\mathbb{N}$ und $\mathbb{N}_0$ mehrere uns vertraute Verknüpfungen haben, begnügen wir uns zunächst mit „einfacheren“ Strukturen und studieren Mengen, die mit genau einer Verknüpfung versehen sind und einige der gerade eingeführten Eigenschaften erfüllen. Mengen, welche mit zwei miteinander verträglichen Verknüpfungen ausgestattet sind, werden dann später eingeführt.

(6.17) Definition (Halbgruppe, kommutative Halbgruppe, Monoid)**.**

(a) Eine *Halbgruppe* besteht aus einer Menge M zusammen mit einer assoziativen Verknüpfung m auf M. Unter Missbrauch der Notation bezeichnen wir sowohl die besagte Halbgruppe als auch die unterliegende Menge mit M. Die Verknüpfung m wird *Multiplikation* (oder *Halbgruppenverknüpfung*) von M genannt.
Für eine Halbgruppe M mit Multiplikation m schreiben wir $\cdot = \cdot^M := m$ und $xy = x \cdot y$ für $x, y \in M$.

(b) Eine Halbgruppe M heißt *kommutativ*, falls die Multiplikation von M kommutativ ist.

(c) Ein *Monoid* ist eine Halbgruppe M, welche ein neutrales Element bzgl. $\cdot^M$ besitzt. Die Halbgruppenverknüpfung eines Monoids M wird auch *Monoidverknüpfung* von M genannt. Das neutrale Element bzgl. der Multiplikation wird auch *Eins* (oder *Einselement*) von M genannt und als $1 = 1^M$ notiert.

Bei der Festlegung „$\cdot = \cdot^M := m$“ in Definition (6.17)(a) für die Multiplikation einer Halbgruppe handelt es sich um eine Notation, um in einer abstrakt (d.h. nicht in einem konkreten Beispiel) gegebenen Halbgruppe einfach von der Verknüpfung sprechen zu können und diese nicht immer explizit erwähnen zu müssen. In der Regel werden wir also von einer „Halbgruppe M“ anstatt von einer „Halbgruppe M mit Multiplikation m“ sprechen, die Multiplikation als implizit gegeben ansehen und diese dann mit dem Symbol $\cdot$ bezeichnen. Die Bezeichnung $\cdot^M$

werden wir nur dann verwenden, wenn wir explizit darauf hinweisen möchten, dass diese Multiplikation zu M gehört (etwa, wenn wir mehrere Halbgruppen auf einmal betrachten); in der Regel werden wir jedoch darauf verzichten.
Die Notationen „$\cdot$“ und „1“ sowie auch die Bezeichnungen „Multiplikation“ und „Eins“ sind von Beispielen wie dem der natürlichen Zahlen motiviert. Es gibt auch andere Beispiele, wo die Halbgruppenverknüpfung keine Multiplikation im vertrauten Sinne ist. In diesen konkret gegebenen Beispielen verwenden wir weiterhin die jeweils vorliegende Notation, die durch das Beispiel mitgebracht wird; siehe insbesondere Bemerkung (6.22).
Mit Hilfe der Standardnotation in einer Halbgruppe M liest sich die Assoziativität der Multiplikation wie folgt:

- *Assoziativität.* Für $x, y, z \in M$ ist $x(yz) = (xy)z$.

Ist eine Halbgruppe M kommutativ, so gilt neben der Assoziativität zusätzlich noch:

- *Kommutativität.* Für $x, y \in M$ ist $xy = yx$.

Mit Hilfe der Standardnotation in einem Monoid M lesen sich dessen *Axiome*, d.h. dessen definierende Eigenschaften, wie folgt:

- *Assoziativität.* Für $x, y, z \in M$ ist $x(yz) = (xy)z$.
- *Existenz der Eins.* Es existiert ein $e \in M$ derart, dass für $x \in M$ stets $ex = xe = x$ gilt. Dieses e ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für $x \in M$.

Da Monoide insbesondere Halbgruppen sind, erhalten wir auch den Begriff eines *kommutativen Monoids*.
Neben der Multiplikation auf den natürlichen Zahlen ist auch die Addition assoziativ und kommutativ. Für kommutative Halbgruppen, Monoide und Gruppen haben sich daher noch andere Bezeichnungen und Schreibweisen eingebürgert:

(6.18) Definition (abelsche Halbgruppe, abelsches Monoid)**.**

(a) Eine *abelsche Halbgruppe* ist eine kommutative Halbgruppe A mit Halbgruppenverknüpfung $+ = +^A$, genannt *Addition* von A.

(b) Ein *abelsches Monoid* ist eine abelsche Halbgruppe A, welche ein neutrales Element bzgl. $+^A$ besitzt. Das neutrale Element bzgl. der Addition wird auch *Null* (oder *Nullelement*) von A genannt und als $0 = 0^A$ notiert.

Eine abelsche Halbgruppe ist also strukturell gesehen das Gleiche wie eine kommutative Halbgruppe; wir verwenden lediglich in abstrakten abelschen Halbgruppen eine andere Standardnotation: Abstrakte Halbgruppen (die ggf. auch mal kommutativ sein dürfen, aber im Allgemeinen nicht müssen) werden multiplikativ geschrieben, abstrakte abelsche Halbgruppen werden additiv geschrieben.
Insbesondere gilt: Alle Aussagen über beliebige Halbgruppen und über kommutative Halbgruppen (in multiplikativer Notation geschrieben) bleiben auch für abelsche Halbgruppen (in additiver Notation geschrieben) korrekt. Umgekehrt bleiben alle Aussagen über abelsche Halbgruppen (in additiver Notation geschrieben) auch für kommutative Halbgruppen (in multiplikativer Notation geschrieben) korrekt. Bei der Verwendung solcher Aussagen muss gegebenenfalls nur die jeweilige Notation angepasst werden. In der Regel werden wir getroffene Aussagen über Halbgruppen nicht für abelsche Halbgruppen in additiver Notation wiederholen.
Mit Hilfe der Standardnotation in einer abelschen Halbgruppe A lesen sich deren Axiome wie folgt:

- *Assoziativität.* Für $x, y, z \in A$ ist $x + (y + z) = (x + y) + z$.
- *Kommutativität.* Für $x, y \in A$ ist $x + y = y + x$.

Die Axiome eines abelschen Monoids A sind die eines kommutativen Monoids in additiver Notation:

- *Assoziativität.* Für $x, y, z \in A$ ist $x + (y + z) = (x + y) + z$.
- *Existenz der Null.* Es existiert ein $n \in A$ derart, dass für $x \in A$ stets $n + x = x + n = x$ gilt. Dieses n ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 0 bezeichnet. Wir haben also $0 + x = x + 0 = x$ für $x \in A$.
- *Kommutativität.* Für $x, y \in A$ ist $x + y = y + x$.

Vom Rechnen in den natürlichen Zahlen sind wir es gewohnt, bei Produkten aus mehreren Faktoren bzw. Summen aus mehreren Summanden keine Klammern zu setzen. Dies ist durch die Assoziativität gerechtfertigt, da verschiedene Klammerungen zum selben Wert führen würden. Wir übertragen diese Konvention auf den allgemeinen Fall:

(6.19) Konvention. Wegen der Assoziativität der Multiplikation einer Halbgruppe bzw. der Addition einer abelschen Halbgruppe kommt es bei iterierter Bildung nicht auf die Klammerung an. Im Regelfall lassen wir daher die Klammern im Folgenden weg.

Nachdem wir alle in Satz (6.1)(a), (b) auftauchenden Phänomene analysiert und von den konkreten Beispielen $\mathbb{N}$ und $\mathbb{N}_0$ abstrahiert haben, lassen sich diese nun kurz wie folgt reformulieren.

(6.20) Beispiel.

(a) (i) Die Menge $\mathbb{N}$ zusammen mit der üblichen Addition ist eine abelsche Halbgruppe, aber kein abelsches Monoid.

(ii) Die Menge $\mathbb{N}$ zusammen mit der üblichen Multiplikation ist ein kommutatives Monoid. Die Eins von $\mathbb{N}$ ist die übliche Eins.

(b) (i) Die Menge $\mathbb{N}_0$ zusammen mit der üblichen Addition ist ein abelsches Monoid. Die Null von $\mathbb{N}_0$ ist die übliche Null.

(ii) Die Menge $\mathbb{N}_0$ zusammen mit der üblichen Multiplikation ist ein kommutatives Monoid. Die Eins von $\mathbb{N}_0$ ist die übliche Eins.

(6.21) Beispiel. Es gibt ein nicht-kommutatives Monoid mit genau drei Elementen, dessen Multiplikation durch folgende Verknüpfungstafel gegeben ist.

$\cdot$	1	c_1	c_2
1	1	c_1	c_2
c_1	c_1	c_1	c_1
c_2	c_2	c_2	c_2

Das Abbildungsmonoid

Nach der bis hierher erfolgten abstrakten Begriffsbildung können wir nun das folgende Beispiel untersuchen, in welchem sich die soeben eingeführte Struktur eines Monoids erkennen lässt.
Falls nicht anders erwähnt, fassen wir ohne weiteren Kommentar die Menge der Abbildungen auf einer gegebenen Menge als Monoid im folgenden Sinne auf.

(6.22) Bemerkung. Es sei eine Menge X gegeben. Die Menge $\mathrm{Map}(X,X)$ wird ein Monoid mit Monoidverknüpfung $(g,f)\mapsto g\circ f$. Das Einselement von $\mathrm{Map}(X,X)$ ist id_X. Ein Element $f\in\mathrm{Map}(X,X)$ ist genau dann invertierbar in $\mathrm{Map}(X,X)$, wenn f invertierbar im Sinne von Definition (3.17)(b) ist.

Beweis. Für $f,g,h\in\mathrm{Map}(X,X)$ gilt $h\circ(g\circ f)=(h\circ g)\circ f$ nach Bemerkung (3.12). Für $f\in\mathrm{Map}(X,X)$ gilt $\mathrm{id}_X\circ f=f\circ\mathrm{id}_X=f$ nach Bemerkung (3.16). Insgesamt wird $\mathrm{Map}(X,X)$ ein Monoid mit Monoidverknüpfung $(g,f)\mapsto g\circ f$ und Einselement id_X. □

(6.23) Konvention. Es sei eine Menge X gegeben. Wenn wir in Zukunft vom Monoid $\mathrm{Map}(X,X)$ sprechen, so meinen wir damit stets $\mathrm{Map}(X,X)$ mit Monoidverknüpfung $(g,f)\mapsto g\circ f$.

Wir benutzen für die Monoidverknüpfung von $\mathrm{Map}(X,X)$ für eine Menge X oft eine multiplikative Schreibweise:

(6.24) Notation. Es sei eine Menge X gegeben. Für $f,g\in\mathrm{Map}(X,X)$ schreiben wir oft

$$gf:=g\circ f.$$

Invertierbare Elemente

Wir legen eine Sprechweise für die Existenz eines inversen Elements bzgl. der Monoidverknüpfung in einem gegebenen Monoid fest:

(6.25) Definition (Invertierbarkeit)**.**

(a) Es sei ein Monoid M gegeben. Ein Element x in M heißt *invertierbar* in M (oder eine *Einheit* von M), falls es ein inverses Element zu x bzgl. $\cdot$ gibt. Das zu einem invertierbaren Element x in M bzgl. $\cdot$ inverse Element y wird auch das *Inverse* (oder das *inverse Element*) zu x in M genannt und als $x^{-1} = (x^{-1})^M := y$ notiert.

Die *Menge der invertierbaren Elemente* in M bezeichnen wir mit

$$M^\times = \{x \in M \mid x \text{ ist invertierbar}\}.$$

(b) Es sei ein abelsches Monoid A gegeben. Ein Element x in A heißt *negierbar* in A, falls es ein inverses Element zu x bzgl. $+^A$ gibt. Das zu einem negierbaren Element x in A bzgl. $+^A$ inverse Element y wird auch das *Negative* (oder das *negative Element*) zu x in A genannt und als $-x = (-x)^A := y$ notiert.

Die etwas ungewöhnlich aussehende Notation $(x^{-1})^M$ in Definition (6.25)(a) soll lediglich deutlich machen, in welchem Monoid wir das Inverse zu x bilden – nämlich gerade im Monoid M. Wir werden diese Notation nur dann verwenden, wenn wir explizit darauf hinweisen wollen, in welchem Monoid das Inverse gebildet wird.
Bei additiv geschriebenen abelschen Monoiden wird die Notation $M^\times$ in aller Regel nicht verwendet.

(6.26) Beispiel.

(a) Es ist $\mathbb{N}_0{}^\times = \{1\}$, d.h. das einzige invertierbare Element in $\mathbb{N}_0$ (bzgl. der üblichen Multiplikation) ist 1.

(b) Das einzige negierbare Element in $\mathbb{N}_0$ (bzgl. der üblichen Addition) ist 0.

Wir wollen einige einfache Eigenschaften von invertierbaren Elementen herleiten.

(6.27) Proposition. Es sei ein Monoid M gegeben.

(a) Für $x, y \in M^\times$ ist auch $xy \in M^\times$ mit

$$(xy)^{-1} = y^{-1}x^{-1}.$$

(b) Es ist $1 \in M^\times$ mit

$$1^{-1} = 1.$$

(c) Für $x \in M^\times$ ist auch $x^{-1} \in M^\times$ mit

$$(x^{-1})^{-1} = x.$$

Beweis. Dies lässt sich analog zu Proposition (3.21) beweisen. Die Details seien dem Leser zur Übung überlassen. □

(6.28) Bemerkung. Es seien ein Monoid M und $a \in M^\times$, $b, x \in M$ gegeben.

(a) Genau dann gilt $ax = b$, wenn $x = a^{-1}b$ ist.

(b) Genau dann gilt $xa = b$, wenn $x = ba^{-1}$ ist.

Beweis.

(a) Wenn $ax = b$ gilt, dann auch

$$x = 1x = a^{-1}ax = a^{-1}b.$$

Umgekehrt, wenn $x = a^{-1}b$ ist, dann haben wir nach Proposition (6.27)(c) auch

$$b = (a^{-1})^{-1}x = ax.$$

(b) Dies lässt sich analog zu (a) beweisen. □

(6.29) Korollar. Es seien ein Monoid M und $a \in M^\times$, $x, y \in M$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist $ax = ay$.

(b) Es ist $xa = ya$.

(c) Es ist $x = y$.

Beweis. Wir zeigen die Äquivalenz von Bedingung (a) und Bedingung (c); die Äquivalenz von Bedingung (b) und Bedingung (c) lässt sich analog beweisen.
Wenn Bedingung (a) gilt, d.h. wenn $ax = ay$ ist, dann ist nach Bemerkung (6.28)(a) auch

$$x = a^{-1}ay = 1y = y,$$

d.h. es gilt Bedingung (c).
Umgekehrt, wenn Bedingung (c) gilt, d.h. wenn $x = y$ ist, dann ist insbesondere auch $ax = ay$, d.h. es gilt Bedingung (a).
Folglich sind Bedingung (a) und Bedingung (c) äquivalent.
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

(6.30) Korollar. Es sei ein Monoid M und $a \in M^\times$, $x \in M$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist $ax = a$.

(b) Es ist $xa = a$.

(c) Es ist $x = 1$.

Beweis. Wegen $a = a \cdot 1$ gilt genau dann Bedingung (a), wenn $ax = a \cdot 1$ ist. Wegen $a = 1 \cdot a$ gilt genau dann Bedingung (b), wenn $xa = 1 \cdot a$ ist. Die Äquivalenz von Bedingung (a), Bedingung (b) und Bedingung (c) folgt somit aus Korollar (6.29). □

Gruppen

Im abelschen Monoid der ganzen Zahlen $\mathbb{Z}$ zusammen mit der üblichen Addition ist jedes Element negierbar, vgl. Satz (6.1)(c)(iii). Für eine solche Situation benutzen wir einen neuen Begriff, den wir jetzt einführen wollen.

(6.31) Definition ((abelsche) Gruppe)**.**

(a) Eine *Gruppe* ist ein Monoid G, in welchem jedes Element von G invertierbar ist. Die Monoidverknüpfung einer Gruppe G wird auch *Gruppenverknüpfung* von G genannt.

(b) Eine *abelsche Gruppe* ist ein abelsches Monoid A, in welchem jedes Element von A negierbar ist.

Die Axiome einer Gruppe G in Standardnotation lesen sich insgesamt wie folgt:

- *Assoziativität.* Für $x, y, z \in G$ ist $x(yz) = (xy)z$.
- *Existenz der Eins.* Es existiert ein $e \in G$ derart, dass für $x \in G$ stets $ex = xe = x$ gilt. Dieses e ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für $x \in G$.
- *Existenz der Inversen.* Für jedes $x \in G$ existiert ein $y \in G$ mit $yx = xy = 1$. Dieses y ist nach Korollar (6.16) eindeutig bestimmt und wird mit x^{-1} bezeichnet. Wir haben also $x^{-1}x = xx^{-1} = 1$.

Ist G kommutativ, so gilt zusätzlich noch:

- *Kommutativität.* Für $x, y \in G$ ist $xy = yx$.

Die Axiome einer abelschen Gruppe A sind die einer kommutativen Gruppe in additiver Notation. Wir betonen noch einmal: Jede kommutative Gruppe lässt sich als abelsche Gruppe auffassen und umgekehrt – strukturell gesehen sind es die gleichen Objekte, wir bringen durch die unterschiedlichen Terminologien lediglich zum Ausdruck, welche Notation wir verwenden. Insbesondere bleiben alle Aussagen über Gruppen auch für abelsche Gruppen gültig, sie müssen nur in der Notation angepasst werden.
Wir fassen einige Eigenschaften aus Satz (6.1)(c), (d) mit Hilfe der neuen Terminologien noch einmal zusammen:

(6.32) Beispiel.

(a) (i) Die Menge $\mathbb{Z}$ zusammen mit der üblichen Addition ist eine abelsche Gruppe. Die Null von $\mathbb{Z}$ ist die übliche Null. Für $x \in \mathbb{Z}$ ist das Negative zu x in $\mathbb{Z}$ das übliche Negative.

(ii) Die Menge $\mathbb{Z}$ zusammen mit der üblichen Multiplikation ist ein kommutatives Monoid, aber keine Gruppe. Die Eins von $\mathbb{Z}$ ist die übliche Eins.

(b) (i) Die Menge $\mathbb{Q}$ zusammen mit der üblichen Addition ist eine abelsche Gruppe. Die Null von $\mathbb{Q}$ ist die übliche Null. Für $x \in \mathbb{Q}$ ist das Negative zu x in $\mathbb{Q}$ das übliche Negative.

(ii) Die Menge $\mathbb{Q}$ zusammen mit der üblichen Multiplikation ist ein kommutatives Monoid, aber keine Gruppe. Die Eins von $\mathbb{Q}$ ist die übliche Eins.

(iii) Die Menge $\mathbb{Q} \setminus \{0\}$ zusammen mit der üblichen Multiplikation ist eine kommutative Gruppe. Die Eins von $\mathbb{Q} \setminus \{0\}$ ist die übliche Eins. Für $x \in \mathbb{Q} \setminus \{0\}$ ist das Inverse zu x in $\mathbb{Q} \setminus \{0\}$ das übliche Inverse.

(6.33) Konvention. Wenn wir in Zukunft von der abelschen Gruppe $\mathbb{Z}$ sprechen, so meinen wir damit stets $\mathbb{Z}$ mit der üblichen Addition. Wenn wir vom kommutativen Monoid $\mathbb{Z}$ sprechen, so meinen wir damit stets $\mathbb{Z}$ mit der üblichen Multiplikation. Ähnlich für $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Q}$, $\mathbb{R}$.

(6.34) Beispiel. Es gibt eine nicht-kommutative Gruppe mit genau sechs Elementen, dessen Multiplikation durch folgende Verknüpfungstafel gegeben ist.

$\cdot$	1	τ_1	τ_2	τ_3	σ_1	σ_2
1	1	τ_1	τ_2	τ_3	σ_1	σ_2
τ_1	τ_1	1	σ_2	σ_1	τ_3	τ_2
τ_2	τ_2	σ_1	1	σ_2	τ_1	τ_3
τ_3	τ_3	σ_2	σ_1	1	τ_2	τ_1
σ_1	σ_1	τ_2	τ_3	τ_1	σ_2	1
σ_2	σ_2	τ_3	τ_1	τ_2	1	σ_1

Wie von den ganzen Zahlen bekannt, liefert die Existenz von negativen Elementen in einer abelschen Gruppe eine neue Verknüpfung:

(6.35) Definition (Subtraktion)**.** Es sei eine abelsche Gruppe A gegeben. Die Verknüpfung $(x, y) \mapsto x + (-y)$ auf A wird *Subtraktion* von A genannt und als $-$ notiert.

Wir betonen, dass die Addition einer abelschen Gruppe A ein Teil der Daten von A ist (d.h. A besteht aus der unterliegenden Menge, die unter Missbrauch der Notation ebenfalls mit A bezeichnet wird, und der Addition). Hingegen wird die Subtraktion mit Hilfe der Addition und den negativen Elementen definiert und ist insbesondere somit durch die Daten (unterliegende Menge und Addition) eindeutig festgelegt.
Da Gruppen (multiplikativ geschrieben) nicht kommutativ sein müssen, können wir die analoge Verknüpfung $(x, y) \mapsto x : y$, wie etwa aus dem Beispiel $\mathbb{Q} \setminus \{0\}$ bekannt, nicht bilden: für Gruppenelemente x und y muss im Allgemeinen nicht $xy^{-1} = y^{-1}x$ gelten. Genauer gesagt erhalten wir zwei Verknüpfungen, welche im Allgemeinen nicht übereinstimmen und für welche sich keine neue Notation eingebürgert hat.

Die Gruppe der invertierbaren Elemente

Während in einer Gruppe jedes Element invertierbar ist, haben wir in einem beliebigen Monoid auch nicht-invertierbare Elemente. In Beispiel (6.32)(b)(iii) haben wir gesehen, dass wir eine Gruppe erhalten, wenn wir die Multiplikation des Monoids $\mathbb{Q}$ auf die Menge der invertierbaren Elemente $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ einschränken. Dieses Resultat lässt sich auf beliebige Monoide verallgemeinern:

(6.36) Bemerkung. Für jedes Monoid M wird $M^\times$ eine Gruppe, wobei die Multiplikation auf $M^\times$ durch

$$x \cdot^{M^\times} y = x \cdot^M y$$

für $x, y \in M$ gegeben ist.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(6.37) Definition (Gruppe der invertierbaren Elemente)**.** Es sei ein Monoid M gegeben. Die Gruppe $M^\times$ mit der Multiplikation aus Bemerkung (6.36) heißt *Gruppe der invertierbaren Elemente* (oder *Einheitengruppe*) von M.

Ein Monoid G ist also genau dann eine Gruppe, wenn $G^\times = G$ ist.

(6.38) Beispiel.

(a) Es ist

$$\mathbb{Z}^\times = \{1, -1\}.$$

(b) Es ist

$$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}.$$

Ringe und Körper

Bei den uns vertrauten Strukturen spielen jeweils Addition und Multiplikation eine wichtige Rolle. Aus diesem Grund wollen wir als nächstes algebraische Strukturen betrachten, deren unterliegende Mengen mit zwei Verknüpfungen versehen sind.

(6.39) Definition (Ring, kommutativer Ring, Körper)**.**

(a) Ein *Ring* (genauer *unitärer Ring* oder *Ring mit Eins* oder *Ring mit Einselement*) besteht aus einer abelschen Gruppe R zusammen mit einer Verknüpfung m auf R so, dass die unterliegende Menge von R ein Monoid mit Multiplikation m wird und so, dass folgendes Axiom gilt.

- *Distributivität.* Für alle $x, y, z \in R$ ist

$$x\, m\, (y + z) = (x\, m\, y) + (x\, m\, z),$$
$$(x + y)\, m\, z = (x\, m\, z) + (y\, m\, z).$$

Unter Missbrauch der Notation bezeichnen wir sowohl den besagten Ring als auch die unterliegende abelsche Gruppe mit R. Die Verknüpfung m wird *Multiplikation* von R genannt.

Für einen Ring R mit Multiplikation m schreiben wir wie üblich $\cdot = \cdot^R := m$ und $xy = x \cdot y$ für $x, y \in R$.

(b) Ein Ring R heißt *kommutativ*, falls die Multiplikation von R kommutativ ist.

(c) Ein *Körper* ist ein kommutativer Ring K, in welchem $1 \neq 0$ gilt und in welchem jedes Element von $K \setminus \{0\}$ invertierbar (bzgl. der Multiplikation $\cdot^K$) ist.

(6.40) Konvention. In Ringen lassen wir die Klammern um Produkte meistens weg, d.h. es gelte *Punkt- vor Strichrechnung.*

Wir verwenden die in Definition (6.18)(a) bzw. Definition (6.17)(a) eingeführten Notationen für die Addition einer abelschen Halbgruppe (und also insbesondere einer abelschen Gruppe) bzw. für die Multiplikation einer Halbgruppe (und also insbesondere eines Monoids) auch weiterhin für Ringe. Ebenso verwenden wir die Notationen und Begriffe für die neutralen und inversen Elemente bzgl. dieser Verknüpfungen, vgl. Definition (6.25)(a) und Definition (6.35).
Die Axiome eines Rings R in Standardnotation lesen sich also wie folgt:

- *Assoziativität der Addition.* Für $x, y, z \in R$ ist $x + (y + z) = (x + y) + z$.

- *Existenz der Null.* Es existiert ein $n \in R$ derart, dass für $x \in R$ stets $n + x = x + n = x$ gilt. Dieses n ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 0 bezeichnet. Wir haben also $0 + x = x + 0 = x$ für alle $x \in R$.
- *Existenz der Negativen.* Für jedes $x \in R$ existiert ein $y \in R$ mit $y + x = x + y = 0$. Dieses y ist nach Korollar (6.16) eindeutig bestimmt und wird mit $-x$ bezeichnet. Wir haben also $(-x) + x = x + (-x) = 0$.
- *Kommutativität der Addition.* Für $x, y \in R$ ist $x + y = y + x$.
- *Assoziativität der Multiplikation.* Für $x, y, z \in R$ ist $x(yz) = (xy)z$.
- *Existenz der Eins.* Es existiert ein $e \in R$ derart, dass für $x \in R$ stets $ex = xe = x$ gilt. Dieses e ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für alle $x \in R$.
- *Distributivität.* Für $x, y, z \in R$ ist $x(y + z) = xy + xz$ und $(x + y)z = xz + yz$.

Ist R kommutativ, so gilt zusätzlich noch:

- *Kommutativität der Multiplikation.* Für $x, y \in R$ ist $xy = yx$.

Ist R ein Körper, so ist R kommutativ und es gilt ferner noch:

- *Existenz der Inversen.* Es ist $1 \neq 0$. Für jedes $x \in R \setminus \{0\}$ existiert ein $y \in R$ mit $yx = xy = 1$. Dieses y ist nach Korollar (6.16) eindeutig bestimmt und wird mit x^{-1} bezeichnet. Wir haben also $x^{-1}x = xx^{-1} = 1$.

Selbstverständlich bleiben alle Aussagen über (abelsche) Gruppen für die einem Ring unterliegende abelsche Gruppe, bestehend aus der unterliegenden Menge zusammen mit der Addition des Rings, sowie alle Aussagen über Monoide für das einem Ring unterliegende Monoid, bestehend aus der unterliegenden Menge zusammen mit der Multiplikation des Rings, gültig.
Mit Hilfe der Begriffe aus Definition (6.39) lassen sich die Aussagen aus Satz (6.1)(c), (d) noch knapper zusammenfassen:

(6.41) Beispiel.

(a) Die Menge $\mathbb{Z}$ zusammen mit der üblichen Addition und der üblichen Multiplikation ist ein kommutativer Ring, aber kein Körper. Die Null von $\mathbb{Z}$ ist die übliche Null und die Eins von $\mathbb{Z}$ ist die übliche Eins. Für $x \in \mathbb{Z}$ ist das Negative zu x in $\mathbb{Z}$ das übliche Negative.

(b) Die Menge $\mathbb{Q}$ zusammen mit der üblichen Addition und der üblichen Multiplikation ist ein Körper. Die Null von $\mathbb{Q}$ ist die übliche Null und die Eins von $\mathbb{Q}$ ist die übliche Eins. Für $x \in \mathbb{Q}$ ist das Negative zu x in $\mathbb{Q}$ das übliche Negative und für $x \in \mathbb{Q} \setminus \{0\}$ ist das Inverse zu x in $\mathbb{Q}$ das übliche Inverse.

(6.42) Konvention. Wenn wir in Zukunft vom (kommutativen) Ring $\mathbb{Z}$ sprechen, so meinen wir damit stets $\mathbb{Z}$ mit der üblichen Addition und der üblichen Multiplikation. Ähnlich für $\mathbb{Q}$ und $\mathbb{R}$.

(6.43) Beispiel. Es gibt einen Körper mit genau zwei Elementen, der Null 0 und der Eins 1, dessen Addition und Multiplikation durch folgende Verknüpfungstafeln gegeben sind. ([35])

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

(6.44) Beispiel. Es gibt einen nicht-kommutativen Ring mit genau acht Elementen, dessen Addition und Multiplikation durch folgende Verknüpfungstafeln gegeben sind.

$+$	0	1	e_1	e_2	n	u	s_1	s_2
0	0	1	e_1	e_2	n	u	s_1	s_2
1	1	0	e_2	e_1	u	n	s_2	s_1
e_1	e_1	e_2	0	1	s_1	s_2	n	u
e_2	e_2	e_1	1	0	s_2	s_1	u	n
n	n	u	s_1	s_2	0	1	e_1	e_2
u	u	n	s_2	s_1	1	0	e_2	e_1
s_1	s_1	s_2	n	u	e_1	e_2	0	1
s_2	s_2	s_1	u	n	e_2	e_1	1	0

$\cdot$	0	1	e_1	e_2	n	u	s_1	s_2
0	0	0	0	0	0	0	0	0
1	0	1	e_1	e_2	n	u	s_1	s_2
e_1	0	e_1	e_1	0	n	s_1	s_1	n
e_2	0	e_2	0	e_2	0	e_2	0	e_2
n	0	n	0	n	0	n	0	n
u	0	u	e_1	s_2	n	1	s_1	e_2
s_1	0	s_1	e_1	n	n	e_1	s_1	0
s_2	0	s_2	0	s_2	0	s_2	0	s_2

[35] Dieser Körper wird in Definition (13.27) eingeführt, siehe auch Beispiel (13.28)(a).

Eine Axiomatisierung der Eigenschaften von $\mathbb{N}_0$, welche Addition und Multiplikation involviert, wird manchmal *Halbring* genannt. Da eine solche Struktur für uns im Folgenden nur von untergeordnetem Interesse sein würde, werden wir solche Strukturen nicht einführen und genauer betrachten.
Im Folgenden halten wir einige elementare Eigenschaften von Ringen und Körpern fest.

(6.45) Proposition. Es sei ein Ring R gegeben.

(a) Für $a \in R$ gilt $a \cdot 0 = 0 \cdot a = 0$.

(b) Für $a, b \in R$ gilt $a(-b) = (-a)b = -ab$.

(c) Für $a, b \in R$ gilt $(-a)(-b) = ab$.

Beweis.

(a) Für $a \in R$ gilt

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

und damit $a \cdot 0 = 0$ nach Korollar (6.30).

(b) Für $a, b \in R$ gilt

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

nach (a) und damit $-ab = a(-b)$ wegen der Kommutativität der Addition. Die andere Gleichung lässt sich analog zeigen.

(c) Für $a, b \in R$ gilt

$$(-a)(-b) = -a(-b) = -(-ab) = ab$$

nach (b) und Proposition (6.27)(c). □

Die Ringe $\mathbb{Z}$ und $\mathbb{Q}$ sind nullteilerfrei, eine Eigenschaft, welche nicht in jedem Ring gilt. Nullteilerfreie kommutative Ringe sind unter folgendem Namen bekannt:

(6.46) Definition (Integritätsbereich)**.** Ein *Integritätsbereich* ist ein kommutativer Ring R mit $1 \neq 0$ und so, dass folgende Eigenschaft gilt:

- *Nullteilerfreiheit.* Für $a, b \in R$ folgt aus $ab = 0$ stets $a = 0$ oder $b = 0$.

(6.47) Beispiel. Es gibt einen kommutativen Ring mit genau vier Elementen, dessen Addition und Multiplikation durch folgende Verknüpfungstafeln gegeben sind, welcher kein Integritätsbereich ist. ([36])

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Der Ring aus Beispiel (6.44) liefert ein Beispiel für einen nicht-kommutativen Ring, welcher nicht nullteilerfrei ist, d.h. in welchem es zwei (nicht notwendigerweise verschiedene) von Null verschiedene Elemente gibt, deren Produkt Null ist.

(6.48) Proposition. Jeder Körper ist ein Integritätsbereich.

Beweis. Es sei ein Körper K gegeben. Für $a, b \in K$ mit $ab = 0$ und $a \neq 0$ gilt $a \in K^\times$, nach Bemerkung (6.28)(a) und Proposition (6.45)(a) folgt also $b = a^{-1}0 = 0$. Somit folgt für $a, b \in R$ aus $ab = 0$ stets $a = 0$ oder $b = 0$, d.h. K ist ein Integritätsbereich. □

(6.49) Beispiel. Der Ring $\mathbb{Z}$ ist ein Integritätsbereich.

[36] Dieser kommutative Ring wird in Definition (13.8) eingeführt, siehe auch Beispiel (13.20).

Beweis. Nach Proposition (6.48) ist $\mathbb{Q}$ als Körper ein Integritätsbereich, d.h. für $a, b \in \mathbb{Q}$ folgt aus $ab = 0$ stets $a = 0$ oder $b = 0$. Wegen $\mathbb{Z} \subseteq \mathbb{Q}$ folgt dann aber insbesondere für $a, b \in \mathbb{Z}$ aus $ab = 0$ stets $a = 0$ oder $b = 0$. Folglich ist auch $\mathbb{Z}$ ein Integritätsbereich. □

(6.50) Bemerkung. Es sei ein kommutativer Ring R mit $1 \neq 0$ gegeben. Die folgenden Bedingungen sind äquivalent:

(a) Es ist R ein Integritätsbereich.

(b) Für $a, x, y \in R$ folgt aus $ax = ay$ stets $a = 0$ oder $x = y$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

Zusätzliche Konzepte

Im Folgenden geben wir einige zusätzliche Definitionen, deren Studium dem Leser zur Übung überlassen sei.

(6.51) Definition ((abelsche) Unterhalbgruppe, (abelsches) Untermonoid, (abelsche) Untergruppe)**.**

(a) (i) Es sei eine Halbgruppe M gegeben. Eine Teilmenge U von M heißt *Unterhalbgruppe* von M, falls gilt:
- Für $u, u' \in U$ ist $uu' \in U$.

(ii) Es sei eine abelsche Halbgruppe A gegeben. Eine *abelsche Unterhalbgruppe* von A ist eine Unterhalbgruppe von A.

(b) (i) Es sei ein Monoid M gegeben. Eine Unterhalbgruppe U von M heißt *Untermonoid* von M, falls gilt:
- Es ist $1 \in U$.

(ii) Es sei ein abelsches Monoid A gegeben. Ein *abelsches Untermonoid* von A ist ein Untermonoid von A.

(c) (i) Es sei eine Gruppe G gegeben. Ein Untermonoid U von G heißt *Untergruppe* von G, falls (zusätzlich) gilt:
- Für $u \in U$ ist $u^{-1} \in U$.

(ii) Es sei eine abelsche Gruppe A gegeben. Eine *abelsche Untergruppe* von A ist eine Untergruppe von A.

Da wir abelsche Halbgruppen, abelsche Monoide und abelsche Gruppen additiv schreiben, ändern sich die Schreibweisen der definierenden Eigenschaften einer abelschen Halbgruppe, eines abelschen Untermonoids und einer abelschen Untergruppe.

(6.52) Definition (Homomorphismus)**.**

(a) (i) Es seien Halbgruppen M und N gegeben. Ein *Halbgruppenhomomorphismus* (oder *Homomorphismus* von *Halbgruppen* oder *Homomorphismus*) von M nach N ist eine Abbildung $\varphi\colon M \to N$ derart, dass folgendes Axiom gilt:
- Für $x, x' \in M$ ist $\varphi(xx') = \varphi(x)\,\varphi(x')$.

(ii) Es seien abelsche Halbgruppen A und B gegeben. Ein *Homomorphismus abelscher Halbgruppen* (oder *Homomorphismus*) von A nach B ist ein Halbgruppenhomomorphismus von A nach B.

(b) (i) Es seien Monoide M und N gegeben. Ein *Monoidhomomorphismus* (oder *Homomorphismus* von *Monoiden* oder *Homomorphismus*) von M nach N ist ein Halbgruppenhomomorphismus $\varphi\colon M \to N$ derart, dass folgendes Axiom gilt:
- Es ist $\varphi(1) = 1$.

(ii) Es seien abelsche Monoide A und B gegeben. Ein *Homomorphismus abelscher Monoide* (oder *Homomorphismus*) von A nach B ist ein Monoidhomomorphismus von A nach B.

(c) (i) Es seien Gruppen G und H gegeben. Ein *Gruppenhomomorphismus* (oder *Homomorphismus* von *Gruppen* oder *Homomorphismus*) von G nach H ist ein Monoidhomomorphismus $\varphi\colon G \to H$ derart, dass folgendes Axiom gilt:
- Für $x \in G$ ist $\varphi(x^{-1}) = \varphi(x)^{-1}$.

(ii) Es seien abelsche Gruppen A und B gegeben. Ein *Homomorphismus abelscher Gruppen* (oder *Homomorphismus*) von A nach B ist ein Gruppenhomomorphismus von A nach B.

Da wir abelsche Halbgruppen, abelsche Monoide und abelsche Gruppen additiv schreiben, ändern sich die Schreibweisen der definierenden Eigenschaften eines Homomorphismus abelscher Halbgruppen, eines Homomorphismus abelscher Monoide und eines Homomorphismus abelscher Gruppen.
Die per Definition geforderten Eigenschaften eines Gruppenhomomorphismus sind redundant:

(6.53) Bemerkung (Kriterium für Gruppenhomomorphismen)**.** Es seien Gruppen G und H und eine Abbildung $\varphi\colon G \to H$ gegeben. Genau dann ist φ ein Gruppenhomomorphismus, wenn φ ein Halbgruppenhomomorphismus ist.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(6.54) Bemerkung.

(a) Es sei ein Halbgruppenhomomorphismus $\varphi\colon M \to N$ gegeben. Dann ist $\operatorname{Im}\varphi$ eine Unterhalbgruppe von N.

(b) Es sei ein Monoidhomomorphismus $\varphi\colon M \to N$ gegeben. Dann ist $\operatorname{Im}\varphi$ eine Untermonoid von N.

(c) Es sei ein Gruppenhomomorphismus $\varphi\colon G \to H$ gegeben. Dann ist $\operatorname{Im}\varphi$ eine Untergruppe von H.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(6.55) Lemma. Es sei ein Gruppenhomomorphismus $\varphi\colon G \to H$ gegeben. Genau dann ist φ injektiv, wenn für $x \in G$ aus $\varphi(x) = 1$ bereits $x = 1$ folgt.

Beweis. Dies sei dem Leser zur Übung überlassen. □

7 Operationen

Neben (inneren) Verknüpfungen im Sinne von Definition (6.2) spielen auch sogenannte Operationen einer Struktur auf einer anderen eine wichtige Rolle.

Begriffsbildung

Wir beginnen mit der Definition einer Operation eines Monoids auf einer Menge.

(7.1) Definition (Operation)**.** Es seien ein Monoid M und eine Menge X gegeben. Eine *Operation* (oder *Aktion* oder *Wirkung* oder *Linksoperation* oder *Linksaktion* oder *Linkswirkung*) von M auf X ist eine Abbildung $o\colon M \times X \to X$ derart, dass folgende Axiome gelten.

- *Assoziativität der Operation.* Für $a, b \in M$, $x \in X$ ist $o(a, o(b, x)) = o(ab, x)$.
- *Neutralität der Eins bzgl. der Operation.* Für $x \in X$ ist $o(1, x) = x$.

Für $a \in M$, $x \in X$ schreiben wir $a \mathbin{o} x := o(a, x)$.

Mit der Infixnotation lesen sich die Axiome einer Operation wie folgt:

- *Assoziativität der Operation.* Für $a, b \in M$, $x \in X$ ist $a \mathbin{o} (b \mathbin{o} x) = ab \mathbin{o} x$.
- *Neutralität der Eins bzgl. der Operation.* Für $x \in X$ ist $1 \mathbin{o} x = x$.

Neben Operationen von Monoiden auf Mengen gibt es weitere Sorten von Operationen, bei denen ggf. noch weitere Verträglichkeiten gefordert werden. Bspw. ist die Skalarmultiplikation eines Vektorraums V über einem Körper K eine Operation eines Körpers auf einer abelschen Gruppe. ([37])

[37] Vektorräume werden in Vorlesungen über *lineare Algebra* studiert; an der RWTH Aachen bspw. im Kurs *Lineare Algebra für Informatiker* (etwa 2. Semester im Studiengang B.Sc. Informatik).

(7.2) Beispiel.

(a) Es ist

$$\mathbb{Q} \times (\mathbb{Q} \times \mathbb{Q}) \to \mathbb{Q} \times \mathbb{Q},\ (a, x) \mapsto (ax_1, ax_2)$$

eine Operation von $\mathbb{Q}$ auf $\mathbb{Q} \times \mathbb{Q}$.

(b) Es ist

$$\mathbb{N}_0 \times \mathbb{N} \to \mathbb{N},\ (k, x) \mapsto x^k$$

eine Operation von $\mathbb{N}_0$ auf $\mathbb{N}$.

Beweis.

(a) Es sei $s\colon \mathbb{Q} \times (\mathbb{Q} \times \mathbb{Q}) \to \mathbb{Q} \times \mathbb{Q},\ (a, x) \mapsto (ax_1, ax_2)$. Wir verifizieren die Axiome einer Operation.

- *Assoziativität der Operation.* Für $a, b \in \mathbb{Q}$, $x \in \mathbb{Q} \times \mathbb{Q}$ ist

$$s(a, s(b, x)) = s(a, (bx_1, bx_2)) = (a(bx_1), a(bx_2)) = ((ab)x_1, (ab)x_2) = s(ab, x).$$

- *Neutralität der Eins bzgl. der Operation.* Für $x \in \mathbb{Q} \times \mathbb{Q}$ ist

$$s(1, x) = (1 \cdot x_1, 1 \cdot x_2) = (x_1, x_2) = x.$$

Folglich ist s eine Operation von $\mathbb{Q}$ auf $\mathbb{Q} \times \mathbb{Q}$.

(b) Es sei $p\colon \mathbb{N}_0 \times \mathbb{N} \to \mathbb{N},\ (k, x) \mapsto x^k$. Wir verifizieren die Axiome einer Operation.

- *Assoziativität der Operation.* Für $k, l \in \mathbb{N}_0$, $x \in \mathbb{N}$ ist

$$p(k, p(l, x)) = p(k, x^l) = (x^l)^k = x^{lk} = x^{kl} = p(kl, x).$$

- *Neutralität der Eins bzgl. der Operation.* Für $x \in \mathbb{N}$ ist

$$p(1, x) = x^1 = x.$$

Folglich ist p eine Operation von $\mathbb{N}_0$ auf $\mathbb{N}$. □

Statt Linksoperationen werden manchmal auch Rechtsoperationen betrachtet. Die Axiome einer Rechtsoperation $o\colon X \times M \to X$ eines Monoids M auf einer Menge X lesen sich in Infixnotation wie folgt:

- *Assoziativität der Rechtsoperation.* Für $a, b \in M$, $x \in X$ ist $(x\, o\, a)\, o\, b = x\, o\, ab$.
- *Neutralität der Eins bzgl. der Rechtsoperation.* Für $x \in X$ ist $x\, o\, 1 = x$.

Mengen über einem Monoid

Als nächstes wollen wir wieder die strukturelle Sichtweise einnehmen: In aller Regel studieren wir Operationen von Monoiden auf Mengen nicht losgelöst, sondern fassen die Menge zusammen mit der Operation als Struktur auf:

(7.3) Definition (Menge über einem Monoid)**.** Es sei ein Monoid M gegeben. Eine *Menge* über M (oder *M-Menge* oder *Akt* über M oder *M-Akt* oder *Linksmenge* über M oder *M-Linksmenge* oder *Linksakt* über M oder *M-Linksakt*) besteht aus einer Menge X zusammen mit einer Operation o von M auf X. Unter Missbrauch der Notation bezeichnen wir sowohl die besagte M-Menge als auch die unterliegende Menge mit X. Die Operation o wird *Operation* von X genannt.
Für eine M-Menge X mit Operation o schreiben wir $\cdot = \cdot^X := o$ und $ax = a \cdot x$ für $a \in M$, $x \in X$.

Die Axiome einer Menge X über einem Monoid M in Standardnotation lesen sich wie folgt:

- *Assoziativität der Operation.* Für $a, b \in M$, $x \in X$ ist $a(bx) = (ab)x$.

- *Neutralität der Eins bzgl. der Operation.* Für $x \in X$ ist $1 \cdot x = x$.

(7.4) Beispiel. Es wird $\mathbb{Z} \times \mathbb{Z}$ eine $\mathbb{Z}$-Menge mit Operation gegeben durch

$$ax = (ax_1, ax_2)$$

für $a \in \mathbb{Z}$, $x \in \mathbb{Z} \times \mathbb{Z}$.

Beweis. Dies folgt aus Beispiel (7.2). □

Wir betrachten einige elementare Eigenschaften von Mengen über Monoiden, welche Verallgemeinerungen der entsprechenden Eigenschaften für Monoide sind.

(7.5) Bemerkung. Es seien ein Monoid M, eine M-Menge X und $a \in M^\times$, $x, y \in X$ gegeben. Genau dann gilt $ax = y$, wenn $x = a^{-1}y$ ist.

Beweis. Dies lässt sich analog zu Bemerkung (6.28) beweisen; die Details seien dem Leser zur Übung überlassen. □

(7.6) Korollar. Es seien ein Monoid M, eine M-Menge X und $a \in M^\times$, $x, y \in X$ gegeben. Genau dann gilt $ax = ay$, wenn $x = y$ ist.

Beweis. Dies lässt sich analog zu Korollar (6.29) beweisen; die Details seien dem Leser zur Übung überlassen. □

Standardoperation

Jede Menge lässt sich als Menge über dem Abbildungsmonoid auffassen, vgl. Konvention (6.23).

(7.7) Bemerkung. Es sei eine Menge X gegeben. Dann wird X zu einer Menge über $\mathrm{Map}(X, X)$ mit Operation gegeben durch

$$fx = f(x)$$

für $f \in \mathrm{Map}(X, X)$, $x \in X$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(7.8) Konvention. Es sei eine Menge X gegeben. Wenn wir in Zukunft von der Menge X über $\mathrm{Map}(X, X)$ sprechen, so meinen wir damit stets X mit der Operation gegeben durch

$$fx = f(x)$$

für $f \in \mathrm{Map}(X, X)$, $x \in X$.

Reguläre Operation

Jedes Monoid lässt sich als Menge über sich selbst auffassen:

(7.9) Bemerkung. Es sei ein Monoid M gegeben. Die unterliegende Menge von M wird zu einer M-Menge mit Operation gegeben durch die Multiplikation des Monoids M.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(7.10) Konvention. Es sei ein Monoid M gegeben. Wenn wir in Zukunft von der M-Menge M sprechen, so meinen wir damit stets M mit der Operation gegeben durch die Multiplikation des Monoids M.

8 Ordnungsstrukturen

Nachdem wir in Abschnitt 6 einige algebraische Strukturen eingeführt haben, widmen wir uns nun sogenannten Ordnungsstrukturen. ([38]) Durch Ordnungen lassen sich Elemente einer Menge vergleichen.

[38] Wie algebraische Strukturen spielen auch Ordnungsstrukturen und andere relationale Strukturen bei einer formalen Behandlung der Prädikatenlogik eine Rolle. An der RWTH Aachen wird eine solche üblicherweise im Rahmen des Kurses *Mathematische Logik* (etwa 4. Semester im Studiengang B.Sc. Informatik) gelehrt.

Ordnungen

Wir beginnen mit der Definition einer Ordnung und etwas allgemeiner einer Präordnung.

(8.1) Definition (Präordnung, Ordnung, Totalordnung)**.** Es sei eine Menge X gegeben.

(a) Eine *Präordnung* (oder *Präordnungsrelation*) auf X ist eine Relation auf X, welche transitiv und reflexiv ist.

(b) Eine *Ordnung* (genauer *partielle Ordnung*, oder *Ordnungsrelation* oder *partielle Ordnungsrelation*) auf X ist eine antisymmetrische Präordnung auf X.

(c) Eine *Totalordnung* (oder *Totalordnungsrelation*) auf X ist eine vollständige Ordnung auf X.

Wir erinnern an die übliche Ordnung auf der Menge der natürlichen Zahlen $\mathbb{N}$: Für $m, n \in \mathbb{N}$ gilt genau dann $m \leq n$, wenn es ein $p \in \mathbb{N}_0$ mit $n = p + m$ gibt.

(8.2) Beispiel.

(a) Die Relation $\leq$ auf $\mathbb{N}$ ist eine Totalordnung.

(b) Es sei eine Menge X gegeben. Die Relation $\subseteq$ auf $\mathrm{Pot}(X)$ ist eine Ordnung.

(c) Die Relation $<$ auf $\mathbb{N}$ ist keine Präordnung.

Beweis.

(a) Es seien $m, n, p \in \mathbb{N}$ mit $m \leq n$ und $n \leq p$ gegeben. Dann gibt es $q, r \in \mathbb{N}_0$ mit $n = q + m$ und $p = r + n$. Es folgt $p = r + n = r + q + m$, also $m \leq p$. Folglich ist $\leq$ transitiv.

Für alle $m \in \mathbb{N}$ gilt $m = 0 + m$ und damit $m \leq m$. Folglich ist $\leq$ reflexiv.

Es seien $m, n \in \mathbb{N}$ mit $m \leq n$ und $n \leq m$ gegeben, so dass es ein $p, q \in \mathbb{N}_0$ mit $n = p + m$ und $m = q + n$ gibt. Dann folgt $m = q + n = q + p + m$, also $q + p = 0$. Dies impliziert aber $p = 0$ und damit $m = n$. Folglich ist $\leq$ antisymmetrisch.

Für $m, n \in \mathbb{N}$ gibt es ferner $p \in \mathbb{N}_0$ mit $n = p + m$ oder $m = p + n$, d.h. es gilt $m \leq n$ oder $n \leq m$. Folglich ist $\leq$ vollständig.

Insgesamt ist $\leq$ eine Totalordnung auf $\mathbb{N}$.

(b) Für $U, V, W \in \mathrm{Pot}(X)$ mit $U \subseteq V$ und $V \subseteq W$ gilt auch $U \subseteq W$. Folglich ist $\subseteq$ transitiv.

Für $U \in \mathrm{Pot}(X)$ gilt $U \subseteq U$. Folglich ist $\subseteq$ reflexiv.

Für $U, V \in \mathrm{Pot}(X)$ mit $U \subseteq V$ und $V \subseteq U$ gilt nach dem Gleichheitskriterium für Mengen (2.13) stets $U = V$. Folglich ist $\subseteq$ antisymmetrisch.

Insgesamt ist $\subseteq$ eine Ordnung auf $\mathrm{Pot}(X)$.

(c) Nach Beispiel (4.5) ist $<$ nicht reflexiv, also insbesondere keine Präordnung. □

(8.3) Beispiel. Es seien verschiedene Objekte a, b und c gegeben.

(a) Es sei o die Relation auf $\{a, b, c\}$ gegeben durch

$$o = \{(a, a), (b, b), (c, c), (a, b), (a, c)\}.$$

Dann ist o eine Ordnung auf $\{a, b, c\}$, aber keine Totalordnung auf $\{a, b, c\}$.

(b) Es sei o die Relation auf $\{a, b, c\}$ gegeben durch

$$o = \{(a, a), (b, b), (c, c), (a, c), (b, c)\}.$$

Dann ist o eine Ordnung auf $\{a, b, c\}$, aber keine Totalordnung auf $\{a, b, c\}$.

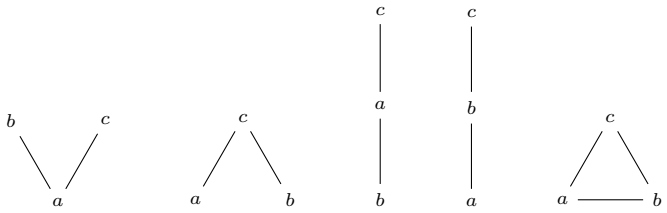


Abbildung 5: (Prä-)Ordnungen auf endlichen Mengen

(c) Es sei o die Relation auf $\{a, b, c\}$ gegeben durch

$$o = \{(a, a), (b, b), (c, c), (b, a), (a, c), (b, c)\}.$$

Dann ist o eine Totalordnung auf $\{a, b, c\}$.

(d) Es sei o die Relation auf $\{a, b, c\}$ gegeben durch

$$o = \{(a, a), (b, b), (c, c), (a, b), (a, c), (b, c)\}.$$

Dann ist o eine Totalordnung auf $\{a, b, c\}$.

(e) Es sei o die Relation auf $\{a, b, c\}$ gegeben durch

$$o = \{(a, a), (b, b), (c, c), (a, b), (b, a), (a, c), (b, c)\}.$$

Dann ist o eine Präordnung auf $\{a, b, c\}$, aber keine Ordnung auf $\{a, b, c\}$.

Die für uns wichtigste Präordnung wird die Teilbarkeitsrelation, siehe Definition (12.5), sein, welche wir in Abschnitt 12 studieren werden.
In der Informatik tauchen Ordnungen bspw. bei der Beschreibung von Sprachen, welche durch sogenannte (formale) Grammatiken erzeugt werden, auf.

(8.4) Bemerkung. Es seien eine Menge X, eine nicht leere Menge I und eine Familie $(o_i)_{i \in I}$ von Präordnungen auf X gegeben. Für $x, y \in X$ gelte genau dann $x \; o \; y$, wenn für $i \in I$ stets $x \; o_i \; y$ gilt.

(a) Es ist o auch eine Präordnung auf X.

(b) Wenn es ein $i \in I$ derart gibt, dass o_i eine Ordnung auf X ist, dann ist o auch eine Ordnung auf X.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(8.5) Beispiel. Es seien o' und o'' die Relationen auf $\{1, 2\}$ gegeben durch

$$o' = \{(1, 1), (2, 2), (1, 2)\},$$
$$o'' = \{(1, 1), (2, 2), (2, 1)\}.$$

Für $x, y \in \{1, 2\}$ gelte genau dann $x \; o \; y$, wenn $x \; o' \; y$ und $x \; o'' \; y$ gilt. Dann sind o' und o'' Totalordnungen auf $\{1, 2\}$, aber o ist keine Totalordnung auf $\{1, 2\}$.

Beweis. Dies folgt aus Beispiel (4.8). Die Details seien dem Leser zur Übung überlassen. □

Geordnete Mengen

So wie die in Abschnitt 6 eingeführten algebraischen Strukturen aus Mengen zusammen mit Verknüpfungen bestehen, lassen sich in analoger Weise auch Ordnungsstrukturen bestehend aus Mengen mit Ordnungen oder allgemeiner mit Präordnungen einführen:

(8.6) Definition (prägeordnete Menge, geordnete Menge, total geordnete Menge)**.**

(a) Eine *prägeordnete Menge* besteht aus einer Menge X zusammen mit einer Präordnung o auf X. Unter Missbrauch der Notation bezeichnen wir sowohl die besagte prägeordnete Menge als auch die unterliegende Menge mit X. Die Präordnung o wird *Präordnung* von X genannt.

Für eine prägeordnete Menge X mit Präordnung o schreiben wir $\leq = \leq^X := o$.

(b) Eine *geordnete Menge* (genauer *partiell geordnete Menge*) ist eine prägeordnete Menge X derart, dass die Präordnung von X eine Ordnung auf der unterliegenden Menge von X ist. Die Präordnung einer geordneten Menge wird auch *Ordnung* von X genannt.

(c) Eine *totalgeordnete Menge* (oder *angeordnete Menge*) ist eine geordnete Menge X derart, dass die Ordnung von X eine Totalordnung auf der unterliegenden Menge von X ist. Die Ordnung einer totalgeordneten Menge wird auch *Totalordnung* von X genannt.

Mit Hilfe der Standardnotation in einer prägeordneten Menge X lesen sich deren Axiome wie folgt:

- *Transitivität.* Für $x, y, z \in X$ folgt aus $x \leq y$ und $y \leq z$ stets $x \leq z$.
- *Reflexivität.* Für $x \in X$ ist $x \leq x$.

Ist X eine geordnete Menge, so gilt zusätzlich noch:

- *Antisymmetrie.* Für $x, y \in X$ folgt aus $x \leq y$ und $y \leq x$ bereits $x = y$.

Ist X eine totalgeordnete Menge, so ist X insbesondere eine geordnete Menge und es gilt ferner noch:

- *Vollständigkeit.* Für $x, y \in X$ gilt $x \leq y$ oder $y \leq x$.

(8.7) Beispiel.

(a) Die Menge $\mathbb{N}$ zusammen mit der üblichen Ordnung ist eine totalgeordnete Menge.

(b) Es sei eine Menge X gegeben. Die Potenzmenge $\mathrm{Pot}(X)$ zusammen mit der Inklusionsrelation $\subseteq$ ist eine geordnete Menge.

(8.8) Konvention.

(a) Wenn wir in Zukunft von der geordneten Menge $\mathbb{N}$ sprechen, so meinen wir damit stets $\mathbb{N}$ mit der üblichen Ordnung. Ähnlich für $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

(b) Es sei eine Menge X gegeben. Wenn wir in Zukunft von der geordneten Menge $\mathrm{Pot}(X)$ sprechen, so meinen wir damit stets $\mathrm{Pot}(X)$ mit der Inklusionsrelation. Ähnlich für $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

Ähnlich wie die Subtraktion in einer abelschen Gruppe aus der Addition und den Negativen definiert wird, leiten wir von der Ordnung in einer geordneten Menge eine weitere Relation ab:

(8.9) Definition (Striktordnung)**.** Es sei eine geordnete Menge X gegeben. Die *Striktordnung* von X ist die wie folgt gegebene Relation $< = <^X$ auf X: Für $x, y \in X$ gelte genau dann $x < y$, wenn $x \leq y$ und $x \neq y$ ist.

Viele weitere Beispiele von geordneten Mengen erhalten wir durch Einschränkung der Ordnung der geordneten Menge auf eine Teilmenge:

(8.10) Bemerkung. Es seien eine prägeordnete Menge X und eine Teilmenge U von X gegeben. Die Menge U wird zu einer prägeordneten Menge mit Präordnung $\leq^U$ gegeben wie folgt. Für $u, v \in U$ gilt genau dann $u \leq^U v$ in U, wenn $u \leq^X v$ in X gilt. Wenn X eine geordnete Menge ist, dann wird U ebenfalls eine geordnete Menge. Wenn X eine total geordnete Menge ist, dann wird U ebenfalls eine total geordnete Menge.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(8.11) Beispiel.

(a) Für jedes $n \in \mathbb{N}_0$ wird $[1, n]$ eine totalgeordnete Menge.

(b) Es sei eine Menge X gegeben. Die Menge $\mathrm{Pot}(X) \setminus \{\emptyset\}$ wird eine geordnete Menge.

In der Literatur finden sich weitere Instanzen von Ordnungsstrukturen wie etwa *angeordnete Körper*, d.h. Körper zusammen mit einer Totalordnung, welche in geeigneter Art und Weise verträglich mit Addition und Multiplikation ist.

Extremale Elemente

Nun studieren wir Elemente von geordneten Mengen, welche extremal bzgl. der gegebenen Ordnung sind.

(8.12) Definition (minimales Element, maximales Element)**.** Es seien eine prägeordnete Menge X und ein $x \in X$ gegeben.

(a) Wir sagen, dass x ein *minimales* Element in X ist, falls für alle $y \in X$ mit $y \leq x$ auch $x \leq y$ gilt.

(b) Wir sagen, dass x ein *maximales* Element in X ist, falls für alle $y \in X$ mit $x \leq y$ auch $y \leq x$ gilt.

(8.13) Beispiel.

(a) Es ist 1 das eindeutige minimale Element in $\mathbb{N}$. Maximale Elemente gibt es in $\mathbb{N}$ nicht.

(b) Es sei eine Menge X gegeben. Dann ist $\emptyset$ das eindeutige minimale Element und X das eindeutige maximale Element in $\mathrm{Pot}(X)$.

(c) Die minimalen Elemente in $\mathrm{Pot}(\{1,2,3\}) \setminus \{\emptyset\}$ sind die einelementigen Mengen $\{1\}$, $\{2\}$ und $\{3\}$. Es ist $\{1,2,3\}$ das eindeutige maximale Element in $\mathrm{Pot}(\{1,2,3\}) \setminus \{\emptyset\}$.

(d) Es ist $\emptyset$ das eindeutige minimale Element in $\mathrm{Pot}(\{1,2,3\}) \setminus \{\{1,2,3\}\}$. Die maximalen Elemente in $\mathrm{Pot}(\{1,2,3\}) \setminus \{\{1,2,3\}\}$ sind die zweielementigen Mengen $\{1,2\}$, $\{1,3\}$ und $\{2,3\}$.

(8.14) Bemerkung. Es sei eine geordnete Menge X und ein $x \in X$ gegeben.

(a) Die folgenden Bedingungen sind äquivalent.

(i) Das Element x ist minimal in X.

(ii) Für $y \in X$ gilt genau dann $y \leq x$, wenn $y = x$ gilt.

(b) Die folgenden Bedingungen sind äquivalent.

(i) Das Element x ist maximal in X.

(ii) Für $y \in X$ gilt genau dann $x \leq y$, wenn $y = x$ gilt.

Beweis.

(a) Zunächst gelte Bedingung (i), d.h. x sei minimal in X. Für $y \in X$ mit $y \leq x$ gilt dann auch $x \leq y$ und damit $y = x$ auf Grund der Antisymmetrie der Ordnung $\leq$. Für $y \in X$ mit $y = x$ gilt hingegen auch $y \leq x$ auf Grund der Reflexivität von $\leq$. Somit gilt für $y \in X$ genau dann $y \leq x$, wenn $y = x$ gilt, d.h. es gilt Bedingung (ii).

Umgekehrt gelte Bedingung (ii), d.h. für $y \in X$ gelte genau dann $y \leq x$, wenn $y = x$ gilt. Dann gilt insbesondere für $y \in X$ mit $y \leq x$ auch $y = x$, auf Grund der Reflexivität von $\leq$ also auch $x \leq y$. Folglich ist x minimal in X, d.h. es gilt Bedingung (i).

Insgesamt sind Bedingung (i) und Bedingung (ii) äquivalent.

(b) Dies lässt sich dual zu (a) beweisen. □

(8.15) Definition (kleinstes Element, größtes Element)**.** Es seien eine prägeordnete Menge X und ein $x \in X$ gegeben.

(a) Wir sagen, dass x ein *kleinstes* Element in X (oder ein *Minimum* von X) ist, falls $x \leq y$ für alle $y \in X$ gilt.

(b) Wir sagen, dass x ein *größtes* Element in X (oder ein *Maximum* von X) ist, falls $y \leq x$ für alle $y \in X$ gilt.

(8.16) Beispiel.

(a) Es ist 1 ein kleinstes Element in $\mathbb{N}$. Größte Elemente gibt es in $\mathbb{N}$ nicht.

(b) Es sei eine Menge X gegeben. Dann ist $\emptyset$ ein kleinstes Element und X ein größtes Element in $\mathrm{Pot}(X)$.

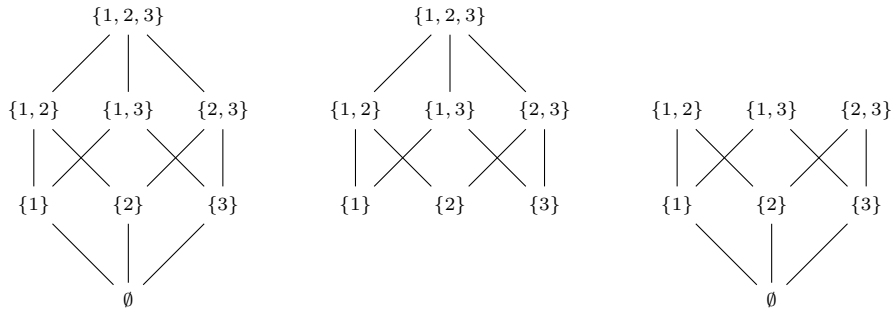


Abbildung 6: Extremale Elemente in Potenzmengen und in Teilmengen von Potenzmengen

(c) Es ist $\{1,2,3\}$ ein größtes Element in $\mathrm{Pot}(\{1,2,3\}) \setminus \{\emptyset\}$. Kleinste Elemente gibt es in $\mathrm{Pot}(\{1,2,3\}) \setminus \{\emptyset\}$ nicht.

(d) Es ist $\emptyset$ ein kleinstes Element in $\mathrm{Pot}(\{1,2,3\}) \setminus \{\{1,2,3\}\}$. Größte Elemente gibt es in $\mathrm{Pot}(\{1,2,3\}) \setminus \{\{1,2,3\}\}$ nicht.

(8.17) Bemerkung. Es sei eine prägeordnete Menge X gegeben.

(a) Jedes kleinste Element in X ist auch minimal.

(b) Jedes größte Element in X ist auch maximal.

Beweis.

(a) Es sei ein kleinstes Element x in X gegeben, so dass $x \leq y$ für alle $y \in X$ gilt. Dann gilt aber insbesondere für alle $y \in X$ mit $y \leq x$ auch $x \leq y$. Folglich ist x minimal in X.

(b) Dies lässt sich dual zu (a) beweisen. □

In Beispiel (8.13)(c) haben wir gesehen, dass es mehrere minimale Elemente bzgl. einer Ordnung geben kann. Nun werden wir zeigen, dass kleinste Elemente in geordneten Mengen hingegen stets eindeutig sind.

(8.18) Proposition. Es seien eine prägeordnete Menge X und ein Element y in X gegeben.

(a) Es sei ein kleinstes Element x in X gegeben. Die folgenden Bedingungen sind äquivalent.

  (i) Das Element y ist ein kleinstes Element in X.
  (ii) Das Element y ist ein minimales Element in X.
  (iii) Es gilt $x \leq y$ und $y \leq x$.
  (iv) Es gilt $y \leq x$.

(b) Es sei ein größtes Element x in X gegeben. Die folgenden Bedingungen sind äquivalent.

  (i) Das Element y ist ein größtes Element in X.
  (ii) Das Element y ist ein maximales Element in X.
  (iii) Es gilt $x \leq y$ und $y \leq x$.
  (iv) Es gilt $x \leq y$.

Beweis.

(a) Falls Bedingung (i) gilt, d.h. falls y ein kleinstes Element in X ist, dann ist y nach Bemerkung (8.17)(a) auch ein minimales Element in X, d.h. es gilt Bedingung (ii).

Als nächstes gelte Bedingung (ii), d.h. es sei y ein minimales Element in X. Da x ein kleinstes Element in X ist, gilt $x \leq z$ für $z \in X$, also insbesondere $x \leq y$. Aber dann impliziert die Minimalität von y, dass außerdem auch $y \leq x$ ist. Folglich gilt Bedingung (iii).

Wenn Bedingung (iii) gilt, d.h. wenn $x \leq y$ und $y \leq x$ ist, dann ist insbesondere $y \leq x$, d.h. Bedingung (iv) gilt.

Schließlich gelte Bedingung (iv), d.h. es sei $y \leq x$. Da x ein kleinstes Element in X ist, gilt $x \leq z$ für $z \in X$, also auch $y \leq z$ für $z \in X$ auf Grund der Transitivität der Ordnung von X. Folglich ist y ein kleinstes Element in X, d.h. Bedingung (i) gilt.

Insgesamt sind Bedingung (i), Bedingung (ii), Bedingung (iii) und Bedingung (iv) äquivalent.

(b) Dies lässt sich dual zu (a) beweisen. □

(8.19) Korollar. Es sei eine geordnete Menge X gegeben.

(a) Es gibt höchstens ein kleinstes Element in X.

(b) Es gibt höchstens ein größtes Element in X.

Beweis.

(a) Es seien kleinste Elemente x und y in X gegeben. Nach Proposition (8.18)(a) gilt dann $x \leq y$ und $y \leq x$, also $x = y$ auf Grund der Antisymmetrie der Ordnung von X.

(b) Dies lässt sich dual zu (a) beweisen. □

(8.20) Notation. Es sei eine geordnete Menge X gegeben.

(a) Es gebe ein kleinstes Element x in X. Wir schreiben

$$\min X := x.$$

(b) Es gebe ein größtes Element x in X. Wir schreiben

$$\max X := x.$$

(8.21) Proposition. Es seien eine total geordnete Menge X und ein $x \in X$ gegeben.

(a) Ein Element in X ist genau dann ein kleinstes Element in X, wenn es ein minimales Element in X ist.

(b) Ein Element in X ist genau dann ein größtes Element in X, wenn es ein maximales Element in X ist.

Beweis.

(a) Es sei ein Element x in X gegeben. Wenn x ein kleinstes Element ist, dann ist x nach Bemerkung (8.17)(a) auch minimal. Wir nehmen also umgekehrt an, dass x minimal ist. Nach Bemerkung (8.14)(a) gilt dann für alle $y \in X$ mit $y \leq x$ bereits $y = x$. Im Umkehrschluss bedeutet dies, dass für alle $y \in X \setminus \{x\}$ nicht $y \leq x$ ist. Die Vollständigkeit der Ordnung von X impliziert dann aber bereits, dass $x \leq y$ für alle $y \in X \setminus \{x\}$ gilt. Andererseits gilt aber auch $x \leq x$ wegen der Reflexivität der Ordnung von X. Insgesamt ist also $x \leq y$ für alle $y \in X$, d.h. x ist ein kleinstes Element in X.

(b) Dies lässt sich dual zu (a) beweisen. □

Zusätzliche Konzepte

Im Folgenden geben wir eine zusätzliche Definition, deren Studium dem Leser zur Übung überlassen sei.

(8.22) Definition (erzeugte Ordnung)**.** Es seien eine Menge X und eine Relation r auf X gegeben. Für eine Ordnung o auf X sagen wir, dass o von r *erzeugt* wird, falls $r \subseteq o$ gilt und falls für jede Ordnung p auf X aus $r \subseteq p$ stets $o \subseteq p$ folgt.

(8.23) Proposition. Es seien eine Menge X und eine Relation r auf X gegeben.

(a) Es gibt höchstens eine von r erzeugte Ordnung auf X.

(b) Es sei eine von r erzeugte Ordnung o auf X gegeben. Dann ist o der transitiv-reflexive Abschluss von r.

(c) Genau dann gibt es eine von r erzeugte Ordnung auf X, wenn der transitiv-reflexive Abschluss von r antisymmetrisch ist.

Beweis. Dies sei dem Leser zur Übung überlassen. □

9 Induktion und Rekursion

Im Folgenden beschäftigen wir uns etwas näher mit den natürlichen Zahlen. Ausgehend von der Eigenschaft, dass sich natürliche Zahlen „zählen“ lassen, entwickeln wir das Beweisprinzip der Induktion. Dies führt uns auf den Rekursionssatz (9.5), welcher besagt, dass sich Folgen, also Familien über den natürlichen Zahlen, rekursiv definieren lassen. Mit der Produkt- und der Summennotation führen wir schließlich Schreibweisen für einige solcher rekursiv definierter Folgen ein, mit deren Hilfe wir am Ende des Abschnitts schließlich beispielhaft einige weitere rekursiv definierte Folgen beschreiben können, d.h., sogenannte Rekursionsgleichungen lösen können.

Induktion

Da uns die natürlichen Zahlen vertraut sind, haben wir ein intuitives Verständnis für die Gültigkeit des folgenden Satzes:

(9.1) Satz (Peano-Arithmetik)**.** Es sei $s\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto n+1$. Dann gilt:

(a) Es ist s injektiv.

(b) Es ist $1 \notin \operatorname{Im} s$.

(c) *Induktionsprinzip.* Für jede Teilmenge U von $\mathbb{N}$ mit $1 \in U$ und $s(U) \subseteq U$ (d.h. für alle $n \in U$ ist auch $s(n) = n+1 \in U$) gilt $U = \mathbb{N}$.

Die in Satz (9.1) aufgeführten Eigenschaften charakterisieren die natürlichen Zahlen bis auf Bijektion. Mit Hilfe dieser Eigenschaften lassen sich die Addition, die Multiplikation und die Ordnung auf $\mathbb{N}$ konstruieren.
Für uns von besonderem Interesse ist das Induktionsprinzip (9.1)(c) (auch *Prinzip der vollständigen Induktion* genannt), welches sich wie folgt äquivalent umformulieren lässt: Zum Beweis einer Aussage der Form

$$(\forall n \in \mathbb{N} : A(n)) := (\forall n : n \in \mathbb{N} \Rightarrow A(n))$$

können wir zeigen, dass die Aussage der Form

$$A(1) \wedge (\forall n \in \mathbb{N} : A(n) \Rightarrow A(n+1))$$

gültig ist, d.h. dass zum einen die Aussage der Form

$$A(1)$$

und zum anderen für jedes $n \in \mathbb{N}$ die Aussage der Form

$$A(n) \Rightarrow A(n+1)$$

gilt.
Um zu zeigen, dass dieses Beweisprinzip gültig ist, nehmen wir an, dass beide Bedingungen erfüllt sind, also dass die Aussage der Form $A(1)$ gilt und dass für jedes $n \in \mathbb{N}$ die Aussage der Form $A(n) \Rightarrow A(n+1)$ gilt. Ferner setzen wir $U := \{n \in \mathbb{N} \mid \text{die Aussage der Form } A(n) \text{ gilt}\}$. Dann ist die Gültigkeit der Aussage der Form $A(1)$ äquivalent zu $1 \in U$. Für alle $n \in U$ gilt ferner die Aussage der Form $A(n)$. Da für jedes $n \in U$ wegen $U \subseteq \mathbb{N}$ die Aussage der Form $A(n) \Rightarrow A(n+1)$ gilt, haben wir auch die Gültigkeit der Aussage der Form $A(n+1)$, d.h. für jedes $n \in U$ ist auch $n+1 \in U$. Nach dem Induktionsprinzip (9.1)(c) impliziert dies bereits $U = \mathbb{N}$, d.h. die Aussage der Form $A(n)$ gilt für alle $n \in \mathbb{N}$. Mit anderen Worten: die Aussage der Form $\forall n \in \mathbb{N} : A(n)$ ist gezeigt.
Wir illustrieren das Induktionsprinzip an einem Beispiel.

(9.2) Anwendungsbeispiel. Für jede ungerade natürliche Zahl m ist $2^m + 1$ ein Vielfaches von 3.

Beweis. Für jedes ungerade $m \in \mathbb{N}$ gibt es (genau) ein $n \in \mathbb{N}$ mit $m = 2n-1$. Wir wollen zeigen, dass $2^{2n-1}+1$ für alle $n \in \mathbb{N}$ ein Vielfaches von 3 ist. Hierzu führen wir Induktion nach n.
Induktionsanfang. Für $n = 1$ ist

$$2^{2n-1} + 1 = 2^{2\cdot 1-1} + 1 = 3 = 1 \cdot 3$$

ein Vielfaches von 3.
Induktionsvoraussetzung. Nun sei $n \in \mathbb{N}$ so gegeben, dass $2^{2n-1}+1$ ein Vielfaches von 3 ist.
Induktionsschritt. Dann gibt es ein $q \in \mathbb{N}$ mit $2^{2n-1}+1 = q \cdot 3$. Es folgt $2^{2n-1} = q \cdot 3 - 1$ und somit

$$\begin{aligned} 2^{2(n+1)-1}+1 &= 2^{2n+2-1}+1 = 4 \cdot 2^{2n-1}+1 = 4 \cdot (q \cdot 3 - 1) + 1 = 4q \cdot 3 - 4 + 1 = 4q \cdot 3 - 3 \\ &= (4q-1) \cdot 3. \end{aligned}$$

Insbesondere ist auch $2^{2(n+1)-1}+1$ ein Vielfaches von 3.
Nach dem Induktionsprinzip ist $2^{2n-1}+1$ für alle $n \in \mathbb{N}$ ein Vielfaches von 3. □

Im obigen Beispiel haben wir in der Induktionsvoraussetzung angenommen, dass ein (beliebiges) $n \in \mathbb{N}$ gegeben ist und dass die Aussage für dieses n gilt. Anschließend haben wir im Induktionsschritt gezeigt, dass die Aussage unter dieser Annahme auch für $n+1$ gilt. Äquivalent hätten wir in der Induktionsvoraussetzung natürlich auch annehmen können, dass ein (beliebiges) $n \in \mathbb{N}$ mit $n \geq 2$ gegeben ist und dass die Aussage für $n-1$ gilt, um im Induktionsschritt dann die Aussage für n zu zeigen.

Alternativer Beweis. Wir zeigen erneut durch Induktion nach n, dass $2^{2n-1}+1$ für alle $n \in \mathbb{N}$ ein Vielfaches von 3 ist.
Induktionsanfang. Für $n = 1$ verfahren wir wie oben.
Induktionsvoraussetzung. Nun sei $n \in \mathbb{N}$ mit $n \geq 2$ so gegeben, dass $2^{2(n-1)-1}+1$ ein Vielfaches von 3 ist.
Induktionsschritt. Dann gibt es ein $q \in \mathbb{N}$ mit $2^{2(n-1)-1}+1 = q \cdot 3$. Es folgt $2^{2(n-1)-1} = q \cdot 3 - 1$ und somit

$$\begin{aligned} 2^{2n-1}+1 &= 2^{2(n-1)+2-1}+1 = 4 \cdot 2^{2(n-1)-1}+1 = 4 \cdot (q \cdot 3 - 1) + 1 = 4q \cdot 3 - 4 + 1 = 4q \cdot 3 - 3 \\ &= (4q-1) \cdot 3. \end{aligned}$$

Insbesondere ist auch $2^{2n-1}+1$ ein Vielfaches von 3.
Nach dem Induktionsprinzip ist $2^{2n-1}+1$ für alle $n \in \mathbb{N}$ ein Vielfaches von 3. □

Eine Variante des Induktionsprinzips lässt sich wie folgt formulieren. Um eine Aussage der Form $\forall n \in \mathbb{N} : A(n)$ zu beweisen, können wir die Aussage der Form

$$A(1) \wedge (\forall n \in \mathbb{N} : A(1) \wedge \ldots \wedge A(n) \Rightarrow A(n+1))$$

zeigen, d.h. zum einen die Aussage der Form

$$A(1)$$

und zum anderen für jedes $n \in \mathbb{N}$ die Aussage der Form

$$A(1) \wedge \ldots \wedge A(n) \Rightarrow A(n+1).$$

Um zu zeigen, dass auch diese Variante gültig ist, nehmen wir an, dass beide Bedingungen erfüllt sind, also dass die Aussage der Form $A(1)$ gilt und dass für jedes $n \in \mathbb{N}$ die Aussage der Form $A(1) \wedge \ldots \wedge A(n) \Rightarrow A(n+1)$ gilt. Dann gilt nach Beispiel (1.29) für jedes $n \in \mathbb{N}$ aber auch die Aussage der Form

$$A(1) \wedge \ldots \wedge A(n) \Rightarrow A(1) \wedge \ldots \wedge A(n) \wedge A(n+1),$$

so dass nach dem Induktionsprinzip die Aussage der Form $\forall n \in \mathbb{N} : A(1) \wedge \ldots \wedge A(n)$ gilt. Nach Beispiel (1.28)(a) gilt dann aber insbesondere die Aussage der Form $\forall n \in \mathbb{N} : A(n)$.
Wir wollen auch die Nützlichkeit dieses Induktionsprinzip anhand eines Beispiels verdeutlichen.

(9.3) Anwendungsbeispiel. Jede natürliche Zahl ist ein Produkt ([39]) von Primzahlen.

Beweis. Wir wollen zeigen, dass jedes $n \in \mathbb{N}$ ein Produkt aus Primzahlen ist. Hierzu führen wir Induktion nach n.
Induktionsanfang. Es ist $n = 1$ ein Produkt aus 0 Faktoren, vgl. Notation (9.7) unten, also insbesondere ein Produkt aus Primzahlen (bestehend aus null Faktoren).

[39] Genauer meinen wir hier ein Produkt aus einer endlichen Anzahl an Faktoren, wobei ein Produkt aus null Faktoren per Definition immer gleich 1 ist, vgl. Notation (9.7).

Induktionsvoraussetzung. Nun sei $n \in \mathbb{N}$ gegeben und es sei angenommen, dass jedes $m \in \mathbb{N}$ mit $m < n$ ein Produkt aus Primzahlen ist.
Induktionsschritt. Wenn n eine Primzahl ist, so ist n insbesondere ein Produkt aus Primzahlen (bestehend aus einem Faktor). Andernfalls ist n zusammengesetzt, d.h. es gibt $l, m \in \mathbb{N}$ mit $l < n$, $m < n$ und $n = lm$. Nach Induktionsvoraussetzung sind l und m Produkte aus Primzahlen. Wegen $n = lm$ ist dann aber auch n ein Produkt aus Primzahlen.
Nach dem Induktionsprinzip ist jedes $n \in \mathbb{N}$ ein Produkt aus Primzahlen. □

Mit Hilfe eines abgewandelten Induktionsprinzips lassen sich auch Aussagen für ganze Zahlen ab einer bestimmten Grenze zeigen – das Beweisprinzip bleibt dasselbe, lediglich der Induktionsanfang bei 1 wird zu einem Induktionsanfang bei irgendeinem gegebenen $n_0 \in \mathbb{Z}$. Präzise formuliert: Um für ein $n_0 \in \mathbb{Z}$ eine Aussage der Form $\forall n \in \mathbb{Z} : n \geq n_0 \Rightarrow A(n)$ zu beweisen, können wir die Aussage der Form

$$A(n_0) \wedge (\forall n \in \mathbb{Z} : n \geq n_0 \Rightarrow (A(n) \Rightarrow A(n+1)))$$

zeigen, d.h. zum einen die Aussage der Form

$$A(n_0)$$

und zum anderen für jedes $n \in \mathbb{Z}$ mit $n \geq n_0$ die Aussage der Form

$$A(n) \Rightarrow A(n+1).$$

Um zu zeigen, dass auch diese Variante gültig ist, nehmen wir an, dass beide Bedingungen erfüllt sind, also dass die Aussage der Form $A(n_0)$ gilt und dass für jedes $n \in \mathbb{Z}$ mit $n \geq n_0$ die Aussage der Form $A(n) \Rightarrow A(n+1)$ gilt. Da $\mathbb{N} \to \{n \in \mathbb{Z} \mid n \geq n_0\}$, $m \mapsto n_0 - 1 + m$ eine wohldefinierte Bijektion ist, gilt dann die Aussage der Form

$$A(n_0 - 1 + 1)$$

sowie für jedes $m \in \mathbb{N}$ die Aussage der Form

$$A(n_0 - 1 + m) \Rightarrow A(n_0 - 1 + m + 1).$$

Nach dem Induktionsprinzip ist dann aber die Gültigkeit der Aussage der Form $\forall m \in \mathbb{N} : A(n_0 - 1 + m)$ nachgewiesen, so dass aus der Bijektion die Gültigkeit der Aussage der Form $\forall n \in \mathbb{Z} : n \geq n_0 \Rightarrow A(n)$ folgt.
Diese Variante des Induktionsprinzips lässt sich zum Beispiel zum Beweis der folgenden Aussage verwenden.

(9.4) Anwendungsbeispiel. Für jedes $n \in \mathbb{N}$ mit $n \geq 4$ gilt $n^2 > 2n + 7$.

Beweis. Wir führen Induktion nach n.
Induktionsanfang. Für $n = 4$ gilt

$$n^2 = 4^2 = 16 > 15 = 2 \cdot 4 + 7 = 2n + 7.$$

Induktionsvoraussetzung. Nun sei $n \in \mathbb{N}$ mit $n \geq 4$ so gegeben, dass $n^2 > 2n + 7$ gilt.
Induktionsschritt. Dann folgt auch

$$(n+1)^2 = n^2 + 2n + 1 > 2n + 7 + 2n + 1 > 2n + 7 + 2 = 2n + 2 + 7 = 2(n+1) + 7.$$

Nach dem Induktionsprinzip gilt $n^2 > 2n + 7$ für alle $n \in \mathbb{N}$ mit $n \geq 4$. □

Rekursion

Auf Grund des Induktionsprinzips lassen sich Folgen, also Familien über $\mathbb{N}$, rekursiv definieren:

(9.5) Proposition (Rekursionssatz)**.** Für jede Menge X, jede Abbildung $t\colon X \to X$ und jedes $a \in X$ gibt es genau eine Folge $x = (x_k)_{k \in \mathbb{N}}$ in X mit $x_1 = a$ und $x_{k+1} = t(x_k)$ für $k \in \mathbb{N}$.

(9.6) Beispiel. Für jedes $a \in \mathbb{R}$ gibt es genau eine Folge $x = (x_k)_{k \in \mathbb{N}}$ in $\mathbb{R}$ mit $x_1 = a$ und $x_{k+1} = ax_k$ für $k \in \mathbb{N}$.

Beweis. Es sei $a \in \mathbb{R}$ gegeben und es sei $t\colon \mathbb{R} \to \mathbb{R}$, $y \mapsto ay$. Nach dem Rekursionssatz (9.5) gibt es genau eine Folge $x = (x_k)_{k \in \mathbb{N}}$ in $\mathbb{R}$ mit $x_1 = a$ und $x_{k+1} = t(x_k) = ax_k$. □

Produkt- und Summennotation

Mit Hilfe von Rekursion führen wir die Produkt- bzw. Summenschreibweise ein:

(9.7) Notation.

(a) Es sei ein Monoid M gegeben. Für jedes $n \in \mathbb{N}_0$ und alle $x \in M^n$ mit $x_i x_j = x_j x_i$ für $i, j \in [1, n]$ notieren wir rekursiv

$$\prod_{i\in[1,n]} x_i = \begin{cases} 1, & \text{falls } n = 0, \\ (\prod_{i\in[1,n-1]} x_i)\, x_n, & \text{falls } n > 0. \end{cases}$$

(b) Es sei ein abelsches Monoid A gegeben. Für jedes $n \in \mathbb{N}_0$ und alle $x \in A^n$ notieren wir rekursiv

$$\sum_{i\in[1,n]} x_i := \begin{cases} 0, & \text{falls } n = 0, \\ \sum_{i\in[1,n-1]} x_i + x_n, & \text{falls } n > 0. \end{cases}$$

Wie skizzieren einen Beweis für die Wohldefiniertheit des in Notation (9.7)(a) definierten Objekts: Es sei

$$t\colon \dot{\bigcup_{n\in\mathbb{N}_0}} \operatorname{Map}(M^n, M) \to \dot{\bigcup_{n\in\mathbb{N}_0}} \operatorname{Map}(M^n, M)$$

gegeben durch

$$t(f)\colon M^{n+1} \to M,\ x \mapsto f((x_i)_{i\in[1,n]}) \cdot x_{n+1}$$

für $f \in \operatorname{Map}(M^n, M)$, $n \in \mathbb{N}_0$. Nach dem Rekursionssatz (9.5) ([40]) gibt es genau eine durch $\mathbb{N}_0$ indizierte Folge $(p_n)_{n\in\mathbb{N}_0}$ in $\dot{\bigcup}_{n\in\mathbb{N}_0} \operatorname{Map}(M^n, M)$ mit $p_0\colon M^0 \to M$, $x \mapsto 1$ und mit $p_n = t(p_{n-1})$ für $n \in \mathbb{N}_0$. Nach dem Induktionsprinzip ist dann p_n für jedes $n \in \mathbb{N}_0$ eine Abbildung von M^n nach M. Für $n \in \mathbb{N}_0$, $x \in M^n$ mit $x_i x_j = x_j x_i$ für $i, j \in [1, n]$ schreiben wir

$$\prod_{i\in[1,n]} x_i = p_n(x),$$

dann gilt

$$\prod_{i\in[1,n]} x_i = p_n(x) = \left\{ \begin{cases} 1, & \text{falls } n = 0, \\ (t(p_{n-1}))(x), & \text{falls } n > 0 \end{cases} \right\} = \left\{ \begin{cases} 1, & \text{falls } n = 0, \\ p_{n-1}((x_i)_{i\in[1,n-1]}) \cdot x_n, & \text{falls } n > 0 \end{cases} \right\}$$
$$= \begin{cases} 1, & \text{falls } n = 0, \\ (\prod_{i\in[1,n-1]} x_i) \cdot x_n, & \text{falls } n > 0. \end{cases}$$

(9.8) Beispiel (kleiner Gauß)**.** Für $n \in \mathbb{N}_0$ gilt

$$\sum_{i\in[1,n]} i = \frac{n(n+1)}{2}.$$

Beweis. Wir führen Induktion nach n. Für $n = 0$ gilt

$$\sum_{i\in[1,n]} i = \sum_{i\in[1,0]} i = 0 = \frac{0(0+1)}{2} = \frac{n(n+1)}{2}.$$

Für $n \in \mathbb{N}$ mit $\sum_{i\in[1,n-1]} i = \frac{(n-1)(n-1+1)}{2} = \frac{(n-1)n}{2}$ gilt

$$\sum_{i\in[1,n]} i = \sum_{i\in[1,n-1]} i + n = \frac{(n-1)n}{2} + n = \frac{(n-1)n + 2n}{2} = \frac{(n-1+2)n}{2} = \frac{(n+1)n}{2} = \frac{n(n+1)}{2}.$$

Nach dem Induktionsprinzip gilt $\sum_{i\in[1,n]} i = \frac{n(n+1)}{2}$ für alle $n \in \mathbb{N}_0$. □

[40] Genau genommen benutzen wir eine Variante für $\mathbb{N}_0$ statt $\mathbb{N}$.

(9.9) Bemerkung. Es seien ein Monoid M, eine endliche Menge I und ein $x \in M^I$ so gegeben, dass $x_i x_j = x_j x_i$ für $i, j \in I$ gilt. Für Abzählungen e und e' von I gilt

$$\prod_{k\in[1,|I|]} x_{e(k)} = \prod_{k\in[1,|I|]} x_{e'(k)}.$$

Beweisidee. Dies folgt aus der Assoziativität von M. □

Die vorangegangene Bemerkung erlaubt uns, die Produkt- und Summenschreibweise auf beliebige endliche Indexmengen zu verallgemeinern:

(9.10) Notation. Es sei eine endliche Menge I gegeben. Wir wählen eine Abzählung $e\colon [1, |I|] \to I$.

(a) Es seien ein Monoid M und ein $x \in M^I$ so gegeben, dass $x_i x_j = x_j x_i$ für $i, j \in I$ gilt. Wir setzen

$$\prod_{i\in I} x_i := \prod_{k\in[1,|I|]} x_{e(k)}.$$

(b) Es seien ein abelsches Monoid A und ein $x \in A^I$ gegeben. Wir setzen

$$\sum_{i\in I} x_i := \sum_{k\in[1,|I|]} x_{e(k)}.$$

(9.11) Notation. Es seien ein Monoid M und eine Menge I gegeben. Wir setzen

$$M^{(I)} := \{x \in M^I \mid \{i \in I \mid x_i \neq 1\} \text{ ist endlich}\}.$$

(9.12) Notation. Es sei eine Menge I gegeben.

(a) Es seien ein Monoid M und ein $x \in M^{(I)}$ so gegeben, dass $x_i x_j = x_j x_i$ für $i, j \in I$ gilt. Wir setzen

$$\prod_{i\in I} x_i := \prod_{\substack{i\in I\\ x_i\neq 1}} x_i := \prod_{i\in\{j\in I\mid x_j\neq 1\}} x_i.$$

(b) Es seien ein abelsches Monoid A und ein $x \in A^{(I)}$ gegeben. Wir setzen

$$\sum_{i\in I} x_i := \sum_{\substack{i\in I\\ x_i\neq 0}} x_i := \sum_{i\in\{j\in I\mid x_j\neq 0\}} x_i.$$

Wir kommen zum Spezialfall, bei welchem alle indizierten Elemente gleich sind:

(9.13) Notation.

(a) Es seien ein Monoid M und $x \in M$ gegeben. Für $k \in \mathbb{N}_0$ setzen wir

$$x^k := \prod_{i\in[1,k]} x.$$

Wenn x invertierbar in M ist, so setzen wir

$$x^{-k} := (x^{-1})^k$$

für $k \in \mathbb{N}$.

(b) Es seien ein abelsches Monoid A und $x \in A$ gegeben. Für $k \in \mathbb{N}_0$ setzen wir

$$kx = k \cdot x := \sum_{i\in[1,k]} x.$$

Wenn x negierbar in A ist, so setzen wir

$$(-k)x := k(-x)$$

für $k \in \mathbb{N}$.

(9.14) Proposition (Potenzgesetze)**.** Es sei ein Monoid M gegeben.

(a) Für $x \in M$, $k, l \in \mathbb{N}_0$ gilt

$$x^k x^l = x^{k+l}.$$

Für $x \in M^\times$, $k, l \in \mathbb{Z}$ gilt

$$x^k x^l = x^{k+l}.$$

(b) Für $x \in M$, $k, l \in \mathbb{N}_0$ gilt

$$(x^k)^l = x^{kl}.$$

Für $x \in M^\times$, $k, l \in \mathbb{Z}$ gilt

$$(x^k)^l = x^{kl}.$$

(c) Es sei M kommutativ. Für $x, y \in M$, $k \in \mathbb{N}_0$ gilt

$$x^k y^k = (xy)^k.$$

Für $x, y \in M^\times$, $k \in \mathbb{Z}$ gilt

$$x^k y^k = (xy)^k.$$

Beweis.

(a) Es seien $x \in M$ und $k \in \mathbb{N}_0$ gegeben. Um $x^k x^l = x^{k+l}$ für alle $l \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach l. Für $l = 0$ gilt

$$x^k x^l = x^k x^0 = x^k \cdot 1 = x^k = x^{k+0}.$$

Für $l \in \mathbb{N}$ mit $x^k x^{l-1} = x^{k+l-1}$ gilt $k + l \geq l > 0$ und somit

$$x^k x^l = x^k (x^{l-1} x) = (x^k x^{l-1}) x = x^{k+l-1} x = x^{k+l}.$$

Nach dem Induktionsprinzip ist $x^k x^l = x^{k+l}$ für alle $l \in \mathbb{N}_0$.

Um $x^k x^l = x^{k+l}$ für alle $x \in M^\times$, $k, l \in \mathbb{Z}$ zu zeigen, unterscheiden wir drei Fälle. Zuerst verifizieren wir die Gleichung für den Spezialfall $x \in M^\times$, $k \in \mathbb{Z}$, $l = 1$, danach für $x \in M^\times$, $k \in \mathbb{Z}$, $l \in \mathbb{Z}$ mit $l \geq 0$ mittels Induktion nach l, und schließlich für $x \in M^\times$, $k \in \mathbb{Z}$, $l \in \mathbb{Z}$ mit $l < 0$.

Zum ersten Fall. Es seien $x \in M^\times$ und $l = 1$ gegeben. Für $k \in \mathbb{Z}$ mit $k \geq 0$ haben wir $x^{k+l} = x^k x^l$ bereits gezeigt. Für $k \in \mathbb{Z}$ mit $k < 0$ gilt $-k > 0$ und damit ebenfalls

$$\begin{aligned} x^k x^l = x^k x^1 = (x^{-1})^{-k} x = ((x^{-1})^{-k-1} x^{-1}) x = (x^{-1})^{-k-1} (x^{-1} x) = (x^{-1})^{-(k+1)} \cdot 1 = (x^{-1})^{-(k+1)} \\ = \begin{cases} (x^{-1})^0, & \text{falls } k = -1, \\ x^{-(-(k+1))}, & \text{falls } k < -1 \end{cases} \Bigg\} = \begin{cases} 1, & \text{falls } k = -1, \\ x^{k+1}, & \text{falls } k < -1 \end{cases} \Bigg\} = x^{k+1} = x^{k+l}. \end{aligned}$$

Zum zweiten Fall. Es seien $x \in M^\times$, $k \in \mathbb{Z}$ gegeben. Um $x^k x^l = x^{k+l}$ für $l \in \mathbb{Z}$ mit $l \geq 0$ zu zeigen, führen wir Induktion nach l ([41]): Für $l = 0$ gilt

$$x^k x^l = x^k x^0 = x^k \cdot 1 = x^k = x^{k+0}.$$

Für $l \in \mathbb{Z}$ mit $l > 0$ und $x^k x^{l-1} = x^{k+l-1}$ gilt unter Benutzung des ersten Falls auch

$$x^k x^l = x^k (x^{l-1} x) = (x^k x^{l-1}) x = x^{k+l-1} x = x^{k+l}.$$

Nach dem Induktionsprinzip ist $x^k x^l = x^{k+l}$ für alle $l \in \mathbb{Z}$ mit $l \geq 0$.

[41] Dieser Schritt ist analog zum Beweis für $x \in M$, $k, l \in \mathbb{N}_0$.

Zum dritten Fall. Schließlich seien $x \in M^\times$, $k, l \in \mathbb{Z}$ mit $l < 0$ gegeben. Dann ist $-l > 0$, es gilt also

$$x^{k+l}x^{-l} = x^{k+l+(-l)} = x^k$$

nach dem zweiten Fall und damit $x^{k+l} = x^k(x^{-l})^{-1}$. Nun haben wir aber

$$x^{-l}x^l = ((x^{-1})^{-1})^{-l}(x^{-1})^{-l} = (x^{-1})^{-(-l)}(x^{-1})^{-l} = (x^{-1})^l(x^{-1})^{-l} = (x^{-1})^{l+(-l)} = (x^{-1})^0 = 1$$

unter Benutzung des zweiten Falls, also $(x^{-l})^{-1} = x^l$ nach Bemerkung (6.15) und damit auch in diesem Fall

$$x^k x^l = x^k(x^{-l})^{-1} = x^{k+l}.$$

(b) Es seien $x \in M$ und $k \in \mathbb{N}_0$ gegeben. Um $(x^k)^l = x^{kl}$ für alle $l \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach l. Für $l = 0$ gilt

$$(x^k)^l = (x^k)^0 = 1 = x^0 = x^{k\cdot 0} = x^{kl}.$$

Für $l \in \mathbb{N}$ mit $(x^k)^{l-1} = x^{k(l-1)}$ gilt nach (a) auch

$$(x^k)^l = (x^k)^{l-1}x^k = x^{k(l-1)}x^k = x^{k(l-1)+k} = x^{kl}.$$

Nach dem Induktionsprinzip ist $(x^k)^l = x^{kl}$ für alle $l \in \mathbb{N}_0$.

Um $(x^k)^l = x^{kl}$ für alle $x \in M^\times$, $k, l \in \mathbb{Z}$ zu zeigen, unterscheiden wir drei Fälle. Zuerst verifizieren wir die Gleichung für $k, l \in \mathbb{Z}$ mit $k \geq 0$, $l \geq 0$, danach für $k, l \in \mathbb{Z}$ mit $k < 0$, $l \geq 0$, und schließlich für $k, l \in \mathbb{Z}$ mit $l < 0$.

Zum ersten Fall. Wir haben bereits bewiesen, dass $(x^k)^l = x^{kl}$ für alle $x \in M$, $k, l \in \mathbb{N}_0$ gilt, also insbesondere für $x \in M^\times$, $k, l \in \mathbb{Z}$, $k \geq 0$, $l \geq 0$.

Zum zweiten Fall. Es seien $x \in M^\times$, $k, l \in \mathbb{Z}$ mit $k < 0$ und $l \geq 0$ gegeben. Dann ist $-k > 0$ und $-kl > 0$, also

$$(x^k)^l = ((x^{-1})^{-k})^l = (x^{-1})^{(-k)l} = (x^{-1})^{-kl} = x^{kl}$$

nach dem ersten Fall.

Zum dritten Fall. Es seien $x \in M^\times$, $k, l \in \mathbb{Z}$ mit $l < 0$ gegeben. Dann ist $-l > 0$, also

$$(x^k)^{-l} = x^{k(-l)}$$

nach dem ersten oder zweiten Fall. Nun ist aber $(x^k)^l\,(x^k)^{-l} = (x^k)^0 = 1$ und $x^{k(-l)}x^{kl} = x^0 = 1$ nach (a), also $((x^k)^{-l})^{-1} = (x^k)^l$ und $(x^{k(-l)})^{-1} = x^{kl}$ nach Bemerkung (6.15). Wir erhalten also auch in diesem Fall

$$(x^k)^l = ((x^k)^{-l})^{-1} = (x^{k(-l)})^{-1} = x^{kl}.$$

(c) Es seien $x, y \in M$ gegeben. Um $x^k y^k = (xy)^k$ für alle $k \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach k. Für $k = 0$ gilt

$$x^k y^k = x^0 y^0 = 1 \cdot 1 = 1 = (xy)^0.$$

Für $k \in \mathbb{N}$ mit $x^{k-1}y^{k-1} = (xy)^{k-1}$ gilt auch

$$x^k y^k = (x^{k-1}x)(y^{k-1}y) = (x^{k-1}y^{k-1})(xy) = (xy)^{k-1}\,(xy) = (xy)^k.$$

Nach dem Induktionsprinzip ist $x^k y^k = (xy)^k$ für alle $k \in \mathbb{N}_0$.

Für $x, y \in M^\times$, $k \in \mathbb{Z}$ mit $k < 0$ ist $-k > 0$, es gilt also auch

$$x^k y^k = (x^{-1})^{-k}(y^{-1})^{-k} = (x^{-1}y^{-1})^{-k} = (y^{-1}x^{-1})^{-k} = ((xy)^{-1})^{-k} = (xy)^k$$

nach Proposition (6.27)(a). □

Jeder Ring R hat eine unterliegende abelsche Gruppe. Folglich haben wir für alle $k \in \mathbb{Z}$ und alle $x \in R$ den Ausdruck $kx = k \cdot x \in R$ definiert, vgl. Notation (9.13)(b).

(9.15) Notation. Es sei ein Ring R gegeben. Für $k \in \mathbb{Z}$ schreiben wir auch

$$k = k^R := k \cdot 1^R.$$

Wir betonen, dass die vorangegangene Vereinbarung konform mit unserer Notation für das Nullelement und das Einselement in einem Ring R ist. Sie besagt unter anderem, dass wir $2^R = 2 \cdot 1^R = 1^R + 1^R$, $3^R = 3 \cdot 1^R = 2 \cdot 1^R + 1^R = 2^R + 1^R$, etc., setzen.
Hin und wieder werden wir außerdem folgende Schreibweise antreffen:

(9.16) Definition (Kronecker-Delta)**.** Es seien ein Ring R und eine Menge I gegeben. Die Familie $\delta = (\delta_{i,j})_{(i,j)\in I\times I}$ gegeben durch

$$\delta_{i,j} := \begin{cases} 1^R & \text{für } i,j \in I \text{ mit } i = j, \\ 0^R & \text{für } i,j \in I \text{ mit } i \neq j. \end{cases}$$

wird *Kronecker-Delta* genannt.

Rekursionsgleichungen

Als nächstes wollen wir beispielhaft sogenannte Rekursionsgleichungen studieren. Wir beginnen mit dem vermutlich berühmtesten Beispiel, der sogenannten Fibonacci-Folge $f = (f_k)_{k\in\mathbb{N}_0} \in {\mathbb{N}_0}^{\mathbb{N}_0}$, welche rekursiv durch

$$f_k = \begin{cases} 0, & \text{für } k = 0, \\ 1, & \text{für } k = 1, \\ f_{k-2} + f_{k-1}, & \text{für } k \in \mathbb{N}_0 \text{ mit } k \geq 2 \end{cases}$$

gegeben ist. Es ist also $f_0 = 0$, $f_1 = 1$, $f_2 = f_0 + f_1 = 1$, $f_3 = f_1 + f_2 = 2$, $f_4 = f_2 + f_3 = 3$, usw. Möchte man nun nur einen Wert der Fibonacci-Folge an einer großen Stelle wissen, etwa f_{10000}, so muss man mit dieser rekursiven Definition erst die Werte f_i für $i \in \mathbb{N}_0$ mit $i \leq 9999$ berechnen. Es stellt sich daher die Frage, ob es nicht eine „geschlossene Formel“ für diese Folge gibt, welche einem die direkte Berechnung von f_{10000} ermöglicht.
Eine *Rekursionsgleichung* in den Unbekannten x_k für $k \in \mathbb{N}_0$ ist durch

$$x_k = t_k(x_0, \ldots, x_{k-1})$$

für eine durch $\mathbb{N}_0$ indizierte Folge $(t_k)_{k\in\mathbb{N}_0}$ von Abbildungen $t_k \colon X^{[0,k-1]} \to X$ für $k \in \mathbb{N}_0$ gegeben. Genau genommen handelt es sich bei einer solchen Rekursionsgleichung also nicht um eine Gleichung, sondern um unendlich viele Gleichungen:

$$\begin{aligned} x_0 &= t_0(\,), \\ x_1 &= t_1(x_0), \\ x_2 &= t_2(x_0, x_1), \\ x_3 &= t_3(x_0, x_1, x_2), \\ &\vdots \end{aligned}$$

Wenn wir eine solche Rekursionsgleichung lösen wollen, so suchen wir die Menge aller $x = (x_k)_{k\in\mathbb{N}_0} \in X^{\mathbb{N}_0}$, welche alle diese Gleichungen erfüllen. Im Fall der Fibonacci-Folge ist für $k \in \mathbb{N}_0$ etwa $t_k \colon {\mathbb{N}_0}^{[0,k-1]} \to \mathbb{N}_0$ gegeben durch

$$t_k(a_0, \ldots, a_{k-1}) = \begin{cases} 0, & \text{falls } k = 0, \\ 1, & \text{falls } k = 1, \\ a_{k-2} + a_{k-1}, & \text{falls } k \geq 2 \end{cases}$$

für $(a_0, \ldots, a_{k-1}) \in {\mathbb{N}_0}^{[0,k-1]}$.
Wir geben nun eine geschlossene Formel für die Fibonacci-Folge an:

(9.17) Beispiel (Binets Formel für die Fibonacci-Folge)**.** Es sei $f \in \mathbb{N}_0^{\mathbb{N}_0}$ gegeben durch

$$f_k = \begin{cases} 0, & \text{für } k = 0, \\ 1, & \text{für } k = 1, \\ f_{k-2} + f_{k-1}, & \text{für } k \in \mathbb{N}_0 \text{ mit } k \geq 2. \end{cases}$$

Dann gilt

$$f_k = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^k - (\frac{1-\sqrt{5}}{2})^k)$$

für $k \in \mathbb{N}_0$.

Beweis. Wir führen Induktion nach k. Für $k = 0$ gilt

$$f_k = f_0 = 0 = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^0 - (\frac{1-\sqrt{5}}{2})^0) = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^k - (\frac{1-\sqrt{5}}{2})^k).$$

Für $k = 1$ gilt

$$f_k = f_1 = 1 = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^1 - (\frac{1-\sqrt{5}}{2})^1) = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^k - (\frac{1-\sqrt{5}}{2})^k).$$

Für $k \in \mathbb{N}_0$ mit $k \geq 2$ und $f_{k-2} = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-2} - (\frac{1-\sqrt{5}}{2})^{k-2})$ und $f_{k-1} = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-1})$ gilt auch

$$\begin{aligned}
f_k = f_{k-2} + f_{k-1} &= \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-2} - (\frac{1-\sqrt{5}}{2})^{k-2}) + \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-1}) \\
&= \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-2} - (\frac{1-\sqrt{5}}{2})^{k-2} + (\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-1}) \\
&= \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-2} + (\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-2} - (\frac{1-\sqrt{5}}{2})^{k-1}) \\
&= \frac{1}{\sqrt{5}}(\frac{2^2(1+\sqrt{5})^{k-2} + 2(1+\sqrt{5})^{k-1}}{2^k} - \frac{2^2(1-\sqrt{5})^{k-2} + 2(1-\sqrt{5})^{k-1}}{2^k}) \\
&= \frac{1}{\sqrt{5}}(\frac{(4+2(1+\sqrt{5}))(1+\sqrt{5})^{k-2}}{2^k} - \frac{(4+2(1-\sqrt{5}))(1-\sqrt{5})^{k-2}}{2^k}) \\
&= \frac{1}{\sqrt{5}}(\frac{(4+2+2\sqrt{5})(1+\sqrt{5})^{k-2}}{2^k} - \frac{(4+2-2\sqrt{5})(1-\sqrt{5})^{k-2}}{2^k}) \\
&= \frac{1}{\sqrt{5}}(\frac{(1+2\sqrt{5}+(\sqrt{5})^2)(1+\sqrt{5})^{k-2}}{2^k} - \frac{(1-2\sqrt{5}+(\sqrt{5})^2)(1-\sqrt{5})^{k-2}}{2^k}) \\
&= \frac{1}{\sqrt{5}}(\frac{(1+\sqrt{5})^2\,(1+\sqrt{5})^{k-2}}{2^k} - \frac{(1-\sqrt{5})^2\,(1-\sqrt{5})^{k-2}}{2^k}) = \frac{1}{\sqrt{5}}(\frac{(1+\sqrt{5})^k}{2^k} - \frac{(1-\sqrt{5})^k}{2^k}) \\
&= \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^k - (\frac{1-\sqrt{5}}{2})^k).
\end{aligned}$$

Nach dem Induktionsprinzip gilt $f_k = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^k - (\frac{1-\sqrt{5}}{2})^k)$ für alle $k \in \mathbb{N}_0$. □

Das Erstaunliche an Binets Formel (9.17) ist die Verwendung der irrationalen Zahlen $\frac{1+\sqrt{5}}{2}$ und $\frac{1-\sqrt{5}}{2}$; der Formel ist auf den ersten Blick nicht anzusehen, dass die Fibonacci-Folge lediglich (nicht-negative) ganzzahlige Einträge besitzt. Eine Methode zur Bestimmung dieser Formel liefert die Eigenwerttheorie aus der Linearen Algebra [18, Abschn. 6].
Im Rahmen dieser Vorlesung beschäftigen wir uns zunächst mit Rekursionsgleichungen, deren Lösungen wir erraten können, wie etwa folgendes Beispiel: Es sei $x \in \mathbb{Z}^{\mathbb{N}_0}$ mit

$$x_k = \begin{cases} 7 & \text{für } k = 0, \\ -2x_{k-1} & \text{für } k \in \mathbb{N} \end{cases}$$

gegeben. Dann ist etwa

$$\begin{aligned}
x_0 &= 7,\\
x_1 &= -2x_0 = -2 \cdot 7 = -14,\\
x_2 &= -2x_1 = -2 \cdot (-14) = 28,\\
x_3 &= -2x_2 = -2 \cdot 28 = -56.
\end{aligned}$$

Für diese ersten vier Werte gilt

$$\begin{aligned}
x_0 &= 7 = (-2)^0 \cdot 7,\\
x_1 &= -14 = (-2)^1 \cdot 7,\\
x_2 &= 28 = (-2)^2 \cdot 7,\\
x_3 &= -56 = (-2)^3 \cdot 7.
\end{aligned}$$

Wir vermuten daher, dass

$$x_k = (-2)^k \cdot 7$$

für $k \in \mathbb{N}_0$ gilt, und werden dies auch gleich in Beispiel (9.18) verifizieren.
Lässt sich eine geschlossene Formel nicht so leicht erraten, so hilft manchmal eine symbolische Behandlung der betrachteten Rekursionsgleichung. In obigem Beispiel haben wir etwas Übersicht durch das Ausrechnen mit den involvierten Werten 7 und -2 verloren. Dies können wir umgehen, indem wir etwa $a := -2$ setzen; für die Folge x gilt dann

$$x_k = ax_{k-1}$$

für $k \in \mathbb{N}$. Ersetzen wir nun bei der Berechnung der Anfangswerte x_0 zunächst nicht durch 7 bzw. a zunächst nicht durch -2, so erhalten wir

$$\begin{aligned}
x_1 &= ax_0,\\
x_2 &= ax_1 = aax_0 = a^2x_0,\\
x_3 &= ax_2 = aa^2x_0 = a^3x_0.
\end{aligned}$$

Hieraus lässt sich nun sehr leicht die Vermutung, dass

$$x_k = a^kx_0 = (-2)^k \cdot 7$$

für $k \in \mathbb{N}_0$ gilt, ablesen.
Und nicht nur das, durch die symbolische Behandlung haben wir implizit eine allgemeinere Situation betrachtet: Für jedes $x \in \mathbb{Z}^{\mathbb{N}_0}$ und jedes $a \in \mathbb{Z}$ mit

$$x_k = ax_{k-1}$$

für $k \in \mathbb{N}$ vermuten wir, dass

$$x_k = a^kx_0$$

für $k \in \mathbb{N}_0$ gilt.
Ferner haben wir beim symbolischen Rechnen nur benutzt, dass wir das Objekt a geeignet von links an ein Objekt x_k „ranmultiplizieren“ können und sich durch diese Operation ein Objekt x_{k+1} ergibt, was vom selben „Typ“ ist wie x_k. Die Tatsache, dass unsere Elemente aus $\mathbb{Z}$ sind, hat nirgendwo eine echte Rolle gespielt. Wir vermuten daher sogar für jedes Monoid M, jede M-Menge X, jedes $x \in X^{\mathbb{N}_0}$ und jedes $a \in M$ mit

$$x_k = ax_{k-1}$$

für $k \in \mathbb{N}$, dass

$$x_k = a^kx_0$$

für $k \in \mathbb{N}_0$ gilt. Diese Vermutung wollen wir nun verifizieren:

(9.18) Beispiel. Es seien ein Monoid M, eine M-Menge X, $x \in X^{\mathbb{N}_0}$ und $a \in M$ mit

$$x_{k+1} = ax_k$$

für $k \in \mathbb{N}_0$ gegeben. Dann ist

$$x_k = a^k x_0$$

für $k \in \mathbb{N}_0$.

Beweis. Wir führen Induktion nach k. Für $k = 0$ gilt

$$x_k = x_0 = 1x_0 = a^0 x_0 = a^k x_0.$$

Für $k \in \mathbb{N}_0$ mit $x_k = a^k x_0$ gilt auch

$$x_{k+1} = ax_k = aa^k x_0 = a^{k+1} x_0.$$

Nach dem Induktionsprinzip gilt also in der Tat $x_k = a^k x_0$ für alle $k \in \mathbb{N}_0$. □

Die Aussage aus Beispiel (9.18) lässt sich auch so ausdrücken: Für jedes $c \in X$ ist das Urbild von c unter der Bijektion

$$\{x \in X^{\mathbb{N}_0} \mid x_{k+1} = ax_k \text{ für } k \in \mathbb{N}_0\} \to X,\ x \mapsto x_0$$

gegeben durch $(a^k c)_{k \in \mathbb{N}_0}$. ([42])
Dadurch, dass wir Beispiel (9.18) nicht nur für $\mathbb{Z}$, sondern direkt für beliebige Mengen über Monoiden bewiesen haben, bleibt die Aussage auch gültig für Folgen mit Einträgen in $\mathbb{R}$: Die Menge der reellen Zahlen $\mathbb{R}$ bildet zusammen mit der üblichen Addition und der üblichen Multiplikation einen Körper, also insbesondere zusammen mit der üblichen Multiplikation ein Monoid und nach Bemerkung (7.9) somit auch eine Menge über diesem Monoid. Nach Beispiel (9.18) gilt für jede Folge $x = (x_k)_{k \in \mathbb{N}_0}$ mit Einträgen in $\mathbb{R}$ und mit $x_{k+1} = ax_k$ für $k \in \mathbb{N}_0$ also

$$x_k = a^k x_0$$

für $k \in \mathbb{N}_0$. Aber nicht nur das: Die Menge $\mathbb{R}$ bildet zusammen mit der üblichen Addition auch eine abelsche Gruppe und damit insbesondere ein abelsches Monoid. Dadurch können wir Beispiel (9.18) auch auf die analoge Situation für die Addition in $\mathbb{R}$ anwenden, sofern wir überall die Notation anpassen: Für jede Folge $x = (x_k)_{k \in \mathbb{N}_0}$ mit Einträgen in $\mathbb{R}$ und mit $x_{k+1} = a + x_k$ für $k \in \mathbb{N}_0$ gilt

$$x_k = ka + x_0$$

für $k \in \mathbb{N}_0$.
De facto ist es sehr naheliegend, dass die Folge x aus Beispiel (9.18) durch

$$x_k = a^k x_0$$

für $k \in \mathbb{N}_0$ gegeben ist. Ist nämlich zusätzlich $x_0 = 1$, so gilt

$$x_k = \begin{cases} 1, & \text{für } k = 0, \\ ax_{k-1}, & \text{für } k \in \mathbb{N}. \end{cases}$$

Nach Notation (9.7)(a) und Notation (9.13)(a) ist dann aber

$$x_k = \prod_{i \in [1,k]} a = a^k$$

für $k \in \mathbb{N}_0$, da wir die Produktnotation gerade auf diese Weise rekursiv definiert haben. Im Fall $x_0 = 1$ gilt daher $x_k = a^k = a^k x_0$ *per Definition*.
Wenig überraschend erhalten wir folgende Verallgemeinerung von Beispiel (9.18):

[42] Die Bijektivität dieser Abbildung ist gerade die Aussage des Rekursionssatzes (9.5) (in einer Variante für $\mathbb{N}_0$ statt $\mathbb{N}$).

(9.19) Beispiel. Es seien ein Monoid M, eine M-Menge X, $x \in X^{\mathbb{N}_0}$ und $a \in M^{\mathbb{N}}$ mit

$$x_{k+1} = a_{k+1}x_k$$

für $k \in \mathbb{N}_0$ gegeben. Dann ist

$$x_k = (\prod_{i\in[1,k]} a_i)x_0$$

für $k \in \mathbb{N}_0$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(9.20) Beispiel. Es sei $x \in \mathbb{R}^{\mathbb{N}_0}$ mit

$$x_{k+1} = x_k + k + 1$$

für $k \in \mathbb{N}_0$ gegeben. Dann ist

$$x_k = \frac{k(k+1)}{2} + x_0$$

für $k \in \mathbb{N}_0$.

Beweis. Nach Beispiel (9.19) und dem kleinen Gauß (9.8) ist

$$x_k = \sum_{i\in[1,k]} i + x_0 = \frac{k(k+1)}{2} + x_0$$

für $k \in \mathbb{N}_0$. □

Natürlich lässt sich Beispiel (9.20) analog zu Beispiel (9.8) auch direkt beweisen:

Alternativer Beweis von Beispiel (9.20). Wir führen Induktion nach k. Für $k = 0$ gilt

$$x_k = x_0 = \frac{0(0+1)}{2} + x_0 = \frac{k(k+1)}{2} + x_0.$$

Für $k \in \mathbb{N}_0$ mit $x_k = \frac{k(k+1)}{2} + x_0$ gilt

$$\begin{aligned} x_{k+1} &= x_k + k + 1 = \frac{k(k+1)}{2} + x_0 + k + 1 = \frac{k(k+1) + 2(k+1)}{2} + x_0 = \frac{(k+2)(k+1)}{2} + x_0 \\ &= \frac{(k+1)(k+2)}{2} + x_0 = \frac{(k+1)(k+1+1)}{2} + x_0. \end{aligned}$$

Nach dem Induktionsprinzip gilt $x_k = \frac{k(k+1)}{2} + x_0$ für alle $k \in \mathbb{N}_0$. □

Schließlich betrachten wir noch ein ähnliches Beispiel, welches sowohl Addition als auch Multiplikation reeller Zahlen involviert:

(9.21) Beispiel. Es sei $x \in \mathbb{R}^{\mathbb{N}_0}$ mit

$$x_{k+1} = 2(x_k + 2^k)$$

für $k \in \mathbb{N}_0$ gegeben. Dann ist

$$x_k = 2^k(k + x_0)$$

für $k \in \mathbb{N}_0$.

Beweis. Für $k = 0$ gilt

$$x_k = x_0 = 2^0 \cdot (0 + x_0) = 2^k(k + x_0).$$

Für $k \in \mathbb{N}_0$ mit $x_k = 2^k(k + x_0)$ gilt auch

$$x_{k+1} = 2(x_k + 2^k) = 2(2^k(k + x_0) + 2^k) = 2 \cdot 2^k(k + x_0 + 1) = 2^{k+1}(k + 1 + x_0).$$

Nach dem Induktionsprinzip gilt $x_k = 2^k(k + x_0)$ für alle $k \in \mathbb{N}_0$. □

In der Informatik treten Rekursionsgleichungen beispielsweise bei der Laufzeitanalyse sogenannter Divide-and-Conquer-Algorithmen ([43]) auf. Diese sind von der Form

$$x_k = a x_{\lfloor \frac{k}{n} \rfloor} + c_k$$

oder Varianten hiervon, wobei $x \in \mathbb{R}_{\geq 0}^{\mathbb{N}_0}$, $a \in \mathbb{R}_{>0}$, $n \in \mathbb{N}$ mit $n \geq 2$ und $c \in \mathbb{R}_{\geq 0}^{\mathbb{N}_0}$. Mit der Notation $\lfloor \frac{k}{n} \rfloor$ wird hierbei die „Abrundung“ von $\frac{k}{n}$ auf die nächstkleinere ganze Zahl, also die größte ganze Zahl, welche kleiner oder gleich $\frac{k}{n}$ ist, bezeichnet.

(9.22) Beispiel. Es sei $x \in \mathbb{R}^{\mathbb{N}_0}$ mit

$$x_k = 2x_{\lfloor \frac{k}{2} \rfloor} + k$$

für $k \in \mathbb{N}$ gegeben. Dann ist

$$x_k = \sum_{i \in [0, \lfloor \log_2(k) \rfloor]} \lfloor \frac{k}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(k) \rfloor + 1} x_0$$

für $k \in \mathbb{N}$.

Beweis. Für $k = 1$ gilt

$$\begin{aligned} \sum_{i \in [0, \lfloor \log_2(k) \rfloor]} \lfloor \frac{k}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(k) \rfloor + 1} x_0 &= \sum_{i \in [0, \lfloor \log_2(1) \rfloor]} \lfloor \frac{1}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(1) \rfloor + 1} x_0 = \sum_{i \in [0,0]} \lfloor \frac{1}{2^i} \rfloor \, 2^i + 2^{0+1} x_0 \\ &= 1 + 2x_0, \end{aligned}$$

also

$$x_k = x_1 = 2x_{\lfloor \frac{1}{2} \rfloor} + 1 = 2x_0 + 1 = 1 + 2x_0 = \sum_{i \in [0, \lfloor \log_2(k) \rfloor]} \lfloor \frac{k}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(k) \rfloor + 1} x_0.$$

Für $k \in \mathbb{N}$ mit $k > 1$ und $x_{\lfloor \frac{k}{2} \rfloor} = \sum_{i \in [0, \lfloor \log_2(\lfloor \frac{k}{2} \rfloor) \rfloor]} \lfloor \frac{\lfloor \frac{k}{2} \rfloor}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(\lfloor \frac{k}{2} \rfloor) \rfloor + 1} x_0$ gilt auch

$$\begin{aligned} x_k &= 2x_{\lfloor \frac{k}{2} \rfloor} + k = 2\Big(\sum_{i \in [0, \lfloor \log_2(\lfloor \frac{k}{2} \rfloor) \rfloor]} \lfloor \frac{\lfloor \frac{k}{2} \rfloor}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(\lfloor \frac{k}{2} \rfloor) \rfloor + 1} x_0 \Big) + k \\ &= 2\Big(\sum_{i \in [0, \lfloor \log_2(\frac{k}{2}) \rfloor]} \lfloor \frac{k}{2^{i+1}} \rfloor \, 2^i + 2^{\lfloor \log_2(\frac{k}{2}) \rfloor + 1} x_0 \Big) + k = \sum_{i \in [0, \lfloor \log_2(k) - 1 \rfloor]} \lfloor \frac{k}{2^{i+1}} \rfloor \, 2^{i+1} + 2^{\lfloor \log_2(k) - 1 \rfloor + 1 + 1} x_0 + k \\ &= k + \sum_{i \in [0, \lfloor \log_2(k) \rfloor - 1]} \lfloor \frac{k}{2^{i+1}} \rfloor \, 2^{i+1} + 2^{\lfloor \log_2(k) \rfloor + 1} x_0 = \lfloor \frac{k}{2^0} \rfloor \, 2^0 + \sum_{i \in [1, \lfloor \log_2(k) \rfloor]} \lfloor \frac{k}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(k) \rfloor + 1} x_0 \\ &= \sum_{i \in [0, \lfloor \log_2(k) \rfloor]} \lfloor \frac{k}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(k) \rfloor + 1} x_0. \end{aligned}$$

Nach dem Induktionsprinzip gilt $x_k = \sum_{i \in [0, \lfloor \log_2(k) \rfloor]} \lfloor \frac{k}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(k) \rfloor + 1} x_0$ für alle $k \in \mathbb{N}$. □

[43] Divide-and-Conquer-Algorithmen und deren Laufzeiten werden an der RWTH Aachen im Rahmen des Kurses *Datenstrukturen und Algorithmen* (etwa 2. Semester im Studiengang B.Sc. Informatik) studiert.

Wie wir gesehen haben, lässt sich mit etwas Mühe auch zur rekursiv gegebenen Folge aus Beispiel (9.22) eine geschlossene Formel angeben und verifizieren. Der Nachteil dieser geschlossenen Formel liegt aber nicht nur in der höheren Komplexität im Vergleich zu den vorher betrachteten Beispielen; für die Anwendung in der Informatik ist sie auch insofern unzweckmäßig, dass sie nur sehr schlecht einen Überblick über das Wachstum der gegebenen Folge gibt. Einen besseren Eindruck erhalten wir, wenn wir nur Zweierpotenzen betrachten:

(9.23) Beispiel. Es sei $x \in \mathbb{R}^{\mathbb{N}_0}$ mit

$$x_k = 2x_{\lfloor \frac{k}{2} \rfloor} + k$$

für $k \in \mathbb{N}$ gegeben. Dann ist

$$x_{2^l} = 2^l(l + 2x_0 + 1)$$

für $l \in \mathbb{N}_0$. Mit anderen Worten: Für $k \in 2^{\mathbb{N}_0} = \{2^l \mid l \in \mathbb{N}_0\}$ gilt

$$x_k = k(\log_2(k) + 2x_0 + 1).$$

Beweis. Für $k \in \mathbb{N}$ gilt $x_k = 2x_{\lfloor \frac{k}{2} \rfloor} + k$, also insbesondere

$$x_{2k} = 2x_{\lfloor \frac{2k}{2} \rfloor} + 2k = 2x_k + 2k.$$

Für $l \in \mathbb{N}_0$ folgt

$$x_{2^{l+1}} = x_{2\cdot 2^l} = 2x_{2^l} + 2 \cdot 2^l = 2x_{2^l} + 2^{l+1} = 2(x_{2^l} + 2^l),$$

und damit

$$x_{2^l} = 2^l(l + x_{2^0}) = 2^l(l + x_1) = 2^l(l + 2x_0 + 1)$$

nach Beispiel (9.21). □

Es seien $x, y \in \mathbb{R}^{\mathbb{N}_0}$ gegeben durch

$$x_k = \begin{cases} 0, & \text{für } k = 0, \\ 2x_{\lfloor \frac{k}{2} \rfloor} + k, & \text{für } k \in \mathbb{N}, \end{cases}$$

$$y_k = \begin{cases} 0, & \text{für } k = 0, \\ k(\log_2(k) + 1), & \text{für } k \in \mathbb{N}. \end{cases}$$

Auch wenn nicht $x_k = y_k$ für alle $k \in \mathbb{N}_0$ gilt, so erkennen wir doch, dass uns die Folge y einen ganz guten Überblick über das Wachstum der Folge x liefert:

k	x_k	y_k
10^0	$1.00 \cdot 10^0$	$1.00 \cdot 10^0$
10^1	$3.60 \cdot 10^1$	$4.32 \cdot 10^1$
10^2	$6.52 \cdot 10^2$	$7.64 \cdot 10^2$
10^3	$9.12 \cdot 10^3$	$10.97 \cdot 10^3$
10^4	$1.33 \cdot 10^5$	$1.43 \cdot 10^5$
10^5	$1.66 \cdot 10^6$	$1.76 \cdot 10^6$
10^6	$1.92 \cdot 10^7$	$2.09 \cdot 10^7$
10^7	$2.34 \cdot 10^8$	$2.43 \cdot 10^8$
10^8	$2.60 \cdot 10^9$	$2.76 \cdot 10^9$
10^9	$2.92 \cdot 10^{10}$	$3.09 \cdot 10^{10}$
10^{10}	$3.35 \cdot 10^{11}$	$3.42 \cdot 10^{11}$

De facto liefert uns sogar $z \in \mathbb{R}^{\mathbb{N}_0}$ gegeben durch

$$z_k = \begin{cases} 0, & \text{für } k = 0, \\ k \log_2(k), & \text{für } k \in \mathbb{N}, \end{cases}$$

bereits eine realitätsnahe Vorstellung über das Wachstum von x, da für große Stellen k der Einfluss des Summanden k in $y_k = k(\log_2(k)+1) = k\log_2(k)+k$ unerheblich wird:

k	x_k	y_k	z_k
10^0	$1.00 \cdot 10^0$	$1.00 \cdot 10^0$	$0.00 \cdot 10^0$
10^{10}	$3.35 \cdot 10^{11}$	$3.42 \cdot 10^{11}$	$3.32 \cdot 10^{11}$
10^{20}	$6.63 \cdot 10^{21}$	$6.74 \cdot 10^{21}$	$6.64 \cdot 10^{21}$
10^{30}	$9.94 \cdot 10^{31}$	$10.07 \cdot 10^{31}$	$9.97 \cdot 10^{31}$
10^{40}	$1.32 \cdot 10^{42}$	$1.34 \cdot 10^{42}$	$1.33 \cdot 10^{42}$
10^{50}	$1.67 \cdot 10^{52}$	$1.67 \cdot 10^{52}$	$1.66 \cdot 10^{52}$
10^{60}	$1.99 \cdot 10^{62}$	$2.00 \cdot 10^{62}$	$1.99 \cdot 10^{62}$
10^{70}	$2.32 \cdot 10^{72}$	$2.34 \cdot 10^{72}$	$2.33 \cdot 10^{72}$
10^{80}	$2.65 \cdot 10^{82}$	$2.67 \cdot 10^{82}$	$2.66 \cdot 10^{82}$
10^{90}	$2.98 \cdot 10^{92}$	$3.00 \cdot 10^{92}$	$2.99 \cdot 10^{92}$
10^{100}	$3.33 \cdot 10^{102}$	$3.33 \cdot 10^{102}$	$3.32 \cdot 10^{102}$

(9.24) Definition (ungefähr gleich schnelles Wachstum)**.** Es seien $x, y \in \mathbb{R}_{\geq 0}^{\mathbb{N}_0}$ gegeben. Wir sagen, dass x *ungefähr* so *schnell* wie y *wächst*, wenn es $c, d \in \mathbb{R}_{>0}$ und ein $k_0 \in \mathbb{N}_0$ derart gibt, dass für $k \in \mathbb{N}_0$ mit $k \geq k_0$ stets

$$cy_k \leq x_k \leq dy_k$$

gilt.

(9.25) Beispiel. Es seien $x, y \in \mathbb{R}_{\geq 0}^{\mathbb{N}_0}$ mit

$$\begin{aligned} x_k &= 2x_{\lfloor \frac{k}{2} \rfloor} + k, \\ y_k &= k\log_2(k) \end{aligned}$$

für $k \in \mathbb{N}$ gegeben. Dann wächst x ungefähr so schnell wie y.

Beweis. Zunächst zeigen wir durch Induktion nach k, dass für $k \in \mathbb{N}_0$ mit $k \geq 2$ stets $x_k \leq 2(x_0+1)y_k$ gilt. Für $k = 2$ gilt

$$\begin{aligned} x_k = x_2 &= 2x_1 + 2 = 2(2x_0+1)+2 = 4x_0+4 = 2(x_0+1)\cdot 2 = 2(x_0+1)\cdot 2\log_2(2) = 2(x_0+1)y_2 \\ &= 2(x_0+1)y_k. \end{aligned}$$

Für $k = 3$ gilt

$$\begin{aligned} x_k = x_3 &= 2x_1 + 3 = 2(2x_0+1)+3 = 4x_0+5 \leq 6x_0+6 = 2(x_0+1)\cdot 3 \leq 2(x_0+1)\cdot 3\log_2(3) \\ &= 2(x_0+1)y_3 = 2(x_0+1)y_k. \end{aligned}$$

Für $k \in \mathbb{N}_0$ mit $k \geq 4$ und $x_{\lfloor \frac{k}{2} \rfloor} \leq 2(x_0+1)y_{\lfloor \frac{k}{2} \rfloor}$ gilt

$$\begin{aligned} x_k &= 2x_{\lfloor \frac{k}{2} \rfloor} + k \leq 2\cdot 2(x_0+1)y_{\lfloor \frac{k}{2} \rfloor} + k = 4(x_0+1)\lfloor \frac{k}{2} \rfloor \log_2(\lfloor \frac{k}{2} \rfloor) + k \leq 4(x_0+1)\frac{k}{2}\log_2(\frac{k}{2}) + k \\ &= 2(x_0+1)k(\log_2(k)-1) + k = 2(x_0+1)k\log_2(k) - 2(x_0+1)k + k = 2(x_0+1)y_k - (2x_0+1)k \\ &\leq 2(x_0+1)y_k. \end{aligned}$$

Nach dem Induktionsprinzip gilt $x_k \leq 2(x_0+1)y_k$ für alle $k \in \mathbb{N}_0$ mit $k \geq 2$.
Als nächstes zeigen wir durch Induktion nach k, dass für $k \in \mathbb{N}_0$ mit $k \geq 1$ stets $x_k \geq \frac{1}{3}y_k$ gilt. Für $k = 1$ gilt

$$x_k = x_1 = 2x_0 + 1 \geq 0 = 1\log_2(1) = y_1 = y_k.$$

Für $k \in \mathbb{N}_0$ mit $k \geq 2$ und $x_{\lfloor \frac{k}{2} \rfloor} \geq \frac{1}{3}y_{\lfloor \frac{k}{2} \rfloor}$ gilt $\log_2(\frac{k-1}{k}) \geq \log_2(\frac{1}{2}) = -1$ und $\log_2(k) \leq k$, also

$$\begin{aligned} x_k &= 2x_{\lfloor \frac{k}{2} \rfloor} + k \geq 2\cdot\frac{1}{3}y_{\lfloor \frac{k}{2} \rfloor} + k = \frac{2}{3}\lfloor \frac{k}{2} \rfloor \log_2(\lfloor \frac{k}{2} \rfloor) + k \\ &\geq \frac{2}{3}\cdot\frac{k-1}{2}\log_2(\frac{k-1}{2}) + k = \frac{1}{3}(k-1)(\log_2(k-1)-1) + k \end{aligned}$$

$$= \frac{1}{3}(k-1)(\log_2(k) + \log_2(\frac{k-1}{k}) - 1) + k \geq \frac{1}{3}(k-1)(\log_2(k) - 1 - 1) + k$$
$$= \frac{1}{3}(k-1)(\log_2(k) - 2) + k = \frac{1}{3}k\log_2(k) - \frac{2}{3}k - \frac{1}{3}\log_2(k) + \frac{2}{3} + k$$
$$= \frac{1}{3}k\log_2(k) + \frac{1}{3}k - \frac{1}{3}\log_2(k) + \frac{2}{3} \geq \frac{1}{3}k\log_2(k) + \frac{2}{3} \geq \frac{1}{3}k\log_2(k) = \frac{1}{3}y_k.$$

Nach dem Induktionsprinzip gilt $x_k \geq \frac{1}{3}y_k$ für alle $k \in \mathbb{N}_0$ mit $k \geq 1$.
Für $k \in \mathbb{N}_0$ mit $k \geq 2$ gilt somit

$$\frac{1}{3}y_k \leq x_k \leq 2(x_0+1)y_k.$$

Folglich wächst x ungefähr so schnell wie y. □

10 Das Stringmonoid

Nach der bis hierher erfolgten abstrakten Begriffsbildung wollen wir in diesem Abschnitt eine Anwendung aus der Informatik kurz anreißen. Hierzu führen wir das Stringmonoid ein, welches die Grundlage für die insbesondere in der theoretischen Informatik untersuchten formalen Sprachen über einem gegebenen Alphabet bildet. Im Anschluss zeigen wir einen Zusammenhang zwischen formalen Sprachen und sogenannten Automaten, welche im Wesentlichen Mengen über dem Stringmonoid sind.

Begriffsbildung

Wir beginnen mit dem Begriff des Stringmonoids.

(10.1) Bemerkung. Es sei eine Menge X gegeben. Die Menge $\dot{\bigcup}_{k\in\mathbb{N}_0} X^k$ wird zu einem Monoid mit Monoidverknüpfung

$$((x_1,\dots,x_k),(y_1,\dots,y_l)) \mapsto (x_1,\dots,x_k,y_1,\dots,y_l)$$

und Einselement $(\,)$.

(10.2) Definition (Stringmonoid)**.** Es sei eine Menge X gegeben. Das Monoid mit unterliegender Menge $\dot{\bigcup}_{k\in\mathbb{N}_0} X^k$ und der Verknüpfung $((x_1,\dots,x_k),(y_1,\dots,y_l)) \mapsto (x_1,\dots,x_k,y_1,\dots,y_l)$ aus Bemerkung (10.1) wird *Stringmonoid* (oder *freies Monoid* oder *Wortmonoid*) über X genannt und als X^* notiert. Die Monoidverknüpfung von X^* wird *Konkatenation* (oder *Aneinanderhängung*) genannt. Ein Element von X^* wird *String* (oder *Zeichenkette*) in X genannt. Das Einselement von X^* wird *leerer String* in X genannt und als $\varepsilon := (\,)$ notiert.
Für einen String $(x_1,\dots,x_k)$ in X schreiben wir $x_1\dots x_k := (x_1,\dots,x_k)$.

(10.3) Beispiel.

(a) Es sei ein Objekt a gegeben. Dann ist das Stringmonoid über $\{a\}$ gegeben durch

$$\{a\}^* = \{\varepsilon, a, aa, aaa, \dots\}.$$

(b) Es seien verschiedene Objekte a und b gegeben. Dann ist das Stringmonoid über $\{a,b\}$ gegeben durch

$$\{a,b\}^* = \{\varepsilon, a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, bab, bba, bbb, \dots\}.$$

(10.4) Bemerkung. Für jede Menge X ist $(X^*)^\times = \{\varepsilon\}$.

Sprachen

Die Wichtigkeit des Stringmonoids, insbesondere in der (theoretischen) Informatik, ergibt sich durch die Betrachtung von Teilmengen: ([44])

[44] Formale Sprachen werden an der RWTH Aachen bspw. im Kurs *Formale Sprachen, Automaten, Prozesse* (etwa 2. Semester im Studiengang B.Sc. Informatik) studiert.

(10.5) Definition (Sprache)**.** Es sei eine Menge X gegeben. Eine (*formale*) *Sprache* über X ist eine Teilmenge von X^*.
Es sei eine Sprache L über X gegeben. Die Menge X wird *Alphabet* von L genannt. Ein Element von X wird *Zeichen* (oder *Buchstabe*) von L genannt. Ein Element von L wird *Wort* in L genannt. ([45])

Da für eine Menge X auch das Stringmonoid X^* eine Sprache über X ist, werden die Strings in X, d.h. die Elemente von X^*, auch Wörter in X^* genannt.

(10.6) Beispiel. Es seien verschiedene Objekte a und b gegeben.

(a) Es ist

$$\{a^n b^n \mid n \in \mathbb{N}\} = \{ab, aabb, aaabbb, \dots\}$$

eine Sprache über $\{a, b\}$.

(b) Es ist

$$\{(ab)^n \mid n \in \mathbb{N}_0\} = \{\varepsilon, ab, abab, ababab, \dots\}$$

eine Sprache über $\{a, b\}$.

Als Anwendungsbeispiel geben wir eine mögliche Formalisierung für die Sprache der Aussagenlogik, vgl. Definition (1.1), an:

(10.7) Anwendungsbeispiel. Das Alphabet der Aussagenlogik sei modelliert als Menge X gegeben durch

$$X = \{A_1, A_2, A_3, \dots\} \dot\cup \{0, 1, \neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\} \dot\cup \{(,)\}.$$

Die Sprache der Aussagenlogik lässt sich dann als (formale) Sprache über X auffassen.

Auch eine beliebige Programmiersprache, wie z.B. C, lässt sich als formale Sprache modellieren:

(10.8) Anwendungsbeispiel. Die Befehle und erlaubten Zeichen einer Programmiersprache seien als Elemente einer Menge X modelliert. Quelltexte für diese Programmiersprache lassen sich dann als Wörter einer Sprache über X auffassen.

Als kurzen Ausblick skizzieren wir das *Wortproblem*: Es sei eine Menge X gegeben. Für einen String x in X bezeichnen wir einen String x' in X als einen *Unterstring* (oder *Teilstring*) von x, falls es Strings p und s in X mit $x = px's$ gibt.
Ferner sei eine Relation r auf X^* gegeben. Die bzgl. r in Relation stehenden Strings in X fassen wir als „Ersetzungsregeln“ im folgenden Sinn auf: Es seien Strings x und y in X gegeben. Wir sagen, dass x und y durch eine elementare Ersetzung auseinander hervorgehen, wenn es Strings p, s, x', y' in X mit $x = px's$, $y = py's$ und $x'\ r\ y'$ gibt, d.h. falls y durch Ersetzung des Unterstrings x' von x durch den Unterstring y' entsteht und umgekehrt.
Das Wortproblem ist nun folgendes: Es seien Strings x und y in X gegeben. Lässt sich überprüfen, ob y durch eine endliche Folge von elementaren Ersetzungen aus x hervorgeht? In vielen Fällen ist dieses Problem nachweislich unentscheidbar.
Es gibt eine bzgl. Inklusion kleinste Sprache L_x, welche zum einen x enthält und welche zum anderen mit jedem Wort z in L_x auch alle diejenigen Strings in X enthält, die durch eine elementare Ersetzung aus z hervorgehen. ([46]) Mit Hilfe von L_x lässt sich das Wortproblem wie folgt umformulieren: Lässt sich überprüfen, ob y ein Wort von L_x ist?

[45] Gelegentlich wird auch eine andere Terminologie verwendet: Die Menge X wird auch *Vokabular* von L genannt. Ein Element von X wird dann *Wort* in L genannt. Ein Element von L wird dann *Satz* in L genannt.

[46] D.h. einerseits ist L_x eine Sprache derart, dass x in L_x enthalten ist, und so, dass mit jedem Wort z in L_x auch alle diejenigen Strings in X enthalten sind, welche durch eine elementare Ersetzung aus z hervorgehen, und andererseits gilt für jede Sprache L derart, dass x in L enthalten ist, und so, dass mit jedem Wort z in L auch alle diejenigen Strings in X enthalten sind, bereits, dass jedes Wort in L_x auch ein Wort von L ist. Vgl. Definition (8.15)(a).

Automaten

In der Informatik spielen Operationen des Stringmonoids, siehe Definition (10.2), eine wichtige Rolle.

(10.9) Definition (Automat)**.** Es sei eine Menge X gegeben. Ein *Automat* (oder *deterministischer Automat* oder *Zustandsmaschine* oder *deterministische Zustandsmaschine*) über X besteht aus einer Menge M über X^* und Teilmengen S und F von M.
Unter Missbrauch der Notation bezeichnen wir sowohl den besagten Automaten als auch die unterliegende Menge über X^* mit M. Die unterliegende Menge von M wird *Menge der Zustände* (oder *Zustandsmenge*) von M genannt. Ein Element von M wird *Zustand* von M genannt. Die Rechtsoperation von M wird (*erweiterte*) *Übergangsfunktion* (oder (*erweiterte*) *Transitionsfunktion*) von M genannt. Die Menge X wird *Eingabealphabet* (oder *Alphabet*) von M genannt. Ein Element von X wird *Zeichen* (oder *Buchstabe*) von M genannt. Die Menge S wird *Menge der Anfangszustände* (oder *Menge der Startzustände* oder *Menge der Initialzustände*) von M genannt. Ein Element von S wird *Anfangszustand* (oder *Startzustand* oder *Initialzustand*) von M genannt. Die Menge F wird *Menge der Endzustände* (oder *Menge der Finalzustände* oder *Menge der Terminalzustände* oder *Menge der akzeptierenden Zustände*) von M genannt. Ein Element von F wird *Endzustand* (oder *Finalzustand* oder *Terminalzustand* oder *akzeptierender Zustand*) von M genannt.

Die (erweiterte) Übergangsfunktion eines Automaten M über einer Menge X ist eindeutig durch ihre Einschränkung auf $M \times X$ festgelegt:

(10.10) Proposition. Es seien Mengen X und M gegeben. Dann ist

$$\{\delta \in \operatorname{Map}(M \times X^*, M) \mid \delta \text{ ist eine Rechtsoperation von } X^* \text{ auf } M\} \to \operatorname{Map}(M \times X, M),$$
$$\delta \mapsto ((q, a) \mapsto q\,\delta\,a)$$

eine wohldefinierte Bijektion.

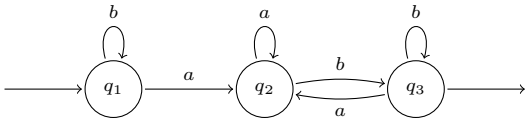
Beweis. Dies sei dem Leser zur Übung überlassen. □

Wegen Proposition (10.10) lassen sich endliche Automaten über endlichen Alphabeten durch Skizzen veranschaulichen, bei denen die Übertragungsfunktion sowie Anfangs- und Endzustände durch Pfeile angegeben werden:

(10.11) Beispiel. Es seien verschiedene Objekte a und b sowie verschiedene Objekte q_1, q_2, q_3 gegeben. Wir haben einen Automaten M über $\{a, b\}$ mit Zustandsmenge $\{q_1, q_2, q_3\}$, Übergangsfunktion bestimmt durch

$$q_1 a = q_2, \quad q_1 b = q_1,$$
$$q_2 a = q_2, \quad q_2 b = q_3,$$
$$q_3 a = q_2, \quad q_3 b = q_3,$$

Menge der Anfangszustände gegeben durch $\{q_1\}$ und Menge der Endzustände gegeben durch $\{q_3\}$.



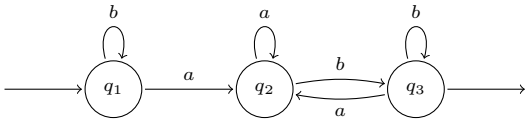
Die Bedeutung von Automaten liegt in der Erkennung formaler Sprachen:

(10.12) Definition (Sprache eines Automaten)**.** Es seien eine Menge X und ein Automat M über X gegeben. Die *Sprache* von M ist definiert als

$$\mathrm{L}(M) := \{x \in X^* \mid \text{es gibt einen Startzustand } p \text{ und einen Endzustand } q \text{ von } M \text{ mit } px = q\}.$$

Es sei ein String x in X gegeben. Wir sagen, dass x von M *akzeptiert* (oder *erkannt*) wird, wenn x ein Wort in $\mathrm{L}(M)$ ist, und ansonsten, dass x von M *zurückgewiesen* (oder *verworfen*) wird.

(10.13) Beispiel. Es seien verschiedene Objekte a und b gegeben. Ferner sei M der folgende Automat über $\{a, b\}$.



Dann ist

$$\mathrm{L}(M) = \{xab^n \mid x \in \{a,b\}^*,\, n \in \mathbb{N}\}.$$

Beweis. Zunächst sei ein von M akzeptiertes Wort y gegeben. Da q_1 der einzige Anfangszustand von M und q_3 der einzige Endzustand von M ist, gilt $q_1 y = q_3$. Wegen $q_1\varepsilon = q_1 \neq q_3$ ist $y \neq \varepsilon$, und wegen $q_i a = q_2 \neq q_3$ für $i \in \{1,2,3\}$ endet y ferner nicht auf a, d.h. es gibt kein $z \in \{a,b\}^*$ mit $y = za$. Folglich endet y auf b. Es seien $n \in \mathbb{N}$ und $z \in \{a,b\}^*$ derart gegeben, dass $y = zb^n$ ist und z nicht auf b endet, d.h. so, dass es kein $x \in \{a,b\}^*$ mit $z = xb$ gibt. Dann ist $q_1 zb^n = q_1 y = q_3$. Wegen $q_1 b^n = q_1 \neq q_3$ ist $z \neq \varepsilon$. Folglich endet z auf a, d.h. es gibt ein $x \in \{a,b\}^*$ mit $z = xa$. Wir haben somit $y = zb^n = xab^n$.
Umgekehrt seien $x \in \{a,b\}^*$ und $n \in \mathbb{N}$ gegeben. Wegen $q_i a = q_2$ für $i \in \{1,2,3\}$ ist dann $q_1 xa = q_2$, also

$$q_1 xab^n = q_2 b^n = q_3 b^{n-1} = q_3.$$

Da q_1 ein Anfangszustand und q_3 ein Endzustand von M ist, wird folglich xab^n von M akzeptiert.
Insgesamt ist $\mathrm{L}(M) = \{xab^n \mid x \in \{a,b\}^*,\, n \in \mathbb{N}\}$. □

11 Der Polynomring

In diesem Abschnitt führen wir Polynome mit Koeffizienten in einem Körper ein. Da sich Polynome addieren und multiplizieren lassen, erhalten wir so für jeden Körper einen kommutativen Ring.
Im Folgenden, bis zum Ende des Abschnitts und mit Ausnahme einiger Beispiele, sei stets ein Körper K gegeben.

Begriffsbildung

Wir beginnen mit der Einführung von Polynomen, wobei wir auf eine Rückführung auf bekannte Konzepte verzichten. Ein Polynom in X soll ein Ausdruck der Form $\sum_{i\in[0,n]} a_i X^i = a_0 + a_1 X + \ldots + a_n X^n$ für ein beliebiges $n \in \mathbb{N}_0$ sein. Führen wir triviale Summanden mit, so können alle Polynome gleich behandelt werden, unabhängig von der Anzahl ihrer jeweiligen nicht-trivialen Summanden. Hierzu betrachten wir im Folgenden die Menge

$$\begin{aligned} K^{(\mathbb{N}_0)} &= \{a \in K^{\mathbb{N}_0} \mid \{i \in \mathbb{N}_0 \mid a_i \neq 0\} \text{ ist endlich}\} \\ &= \{a \in K^{\mathbb{N}_0} \mid \text{es gibt ein } n \in \mathbb{N}_0 \text{ mit } a_i = 0 \text{ für alle } i > n\}. \end{aligned}$$

(11.1) Arbeitsbasis (Polynomring)**.**

(a) Ein *Polynom* in X über K ist ein „Ausdruck“ der Form

$$f = \sum_{i\in\mathbb{N}_0} a_i X^i$$

für ein $a \in K^{(\mathbb{N}_0)}$. Die Familie a wird *Koeffizientenfolge* von f genannt. Für $i \in I$ wird a_i der *Koeffizient* von f an der Stelle i (oder der i-te *Koeffizient* von f) genannt.

(b) Es seien Polynome f und g in X über K und $a, b \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ und $g = \sum_{i\in\mathbb{N}_0} b_i X^i$ gegeben. Die Polynome f und g sind *gleich*, geschrieben $f = g$, falls $a = b$ gilt.

(c) Das Polynom $X = \sum_{i\in\mathbb{N}_0} \delta_{1,i} X^i$ wird *Unbestimmte* genannt.

(d) Der kommutative Ring gegeben durch die Menge der Polynome

$$K[X] := \{\sum_{i\in\mathbb{N}_0} a_i X^i \mid a \in K^{(\mathbb{N}_0)}\}$$

in X über K mit Addition und Multiplikation gegeben durch

$$\sum_{i\in\mathbb{N}_0} a_i X^i + \sum_{i\in\mathbb{N}_0} b_i X^i = \sum_{i\in\mathbb{N}_0} (a_i + b_i) X^i,$$
$$(\sum_{i\in\mathbb{N}_0} a_i X^i)(\sum_{j\in\mathbb{N}_0} b_j X^j) = \sum_{k\in\mathbb{N}_0} (\sum_{\substack{i,j\in\mathbb{N}_0 \\ i+j=k}} a_i b_j) X^k$$

für $a, b \in K^{(\mathbb{N}_0)}$ wird *Polynomring* in X über K genannt.

(e) Wir identifizieren K mit der Teilmenge $\{aX^0 \mid a \in K\}$ von $K[X]$. Das heißt, unter Missbrauch der Notation notieren wir aX^0 für $a \in K$ auch durch a.

Für $a, b \in K^{(\mathbb{N}_0)}$ sind die Polynome $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ und $g = \sum_{i\in\mathbb{N}_0} b_i X^i$ in X über K genau dann gleich, wenn $a = b$ gilt, d.h. wenn $a_i = b_i$ für alle $i \in \mathbb{N}_0$ gilt.

(11.2) Beispiel. Es seien $f, g \in \mathbb{Q}[X]$ gegeben durch $f = X^2 - 1$ und $g = -X^3 + 2X^2 + X + 1$. Dann ist

$$\begin{aligned} f + g &= -X^3 + 3X^2 + X, \\ fg &= -X^5 + 2X^4 + 2X^3 - X^2 - X - 1, \\ -2f &= -2X^2 + 2. \end{aligned}$$

Polynomfunktionen

Die wesentliche Eigenschaft eines Polynoms $f \in K[X]$ ist die Möglichkeit, Elemente von K in f „einzusetzen“. Hierdurch können wir Polynome als Funktionen auffassen.

(11.3) Definition (Polynomfunktion)**.** Es seien $f \in K[X]$ und $a \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ gegeben. Die Abbildung

$$K \to K,\ x \mapsto \sum_{i\in\mathbb{N}_0} a_i x^i$$

heißt *Polynomfunktion* zu f und wird unter Missbrauch der Notation wieder als f notiert.

(11.4) Beispiel. Es sei $f \in \mathbb{Q}[X]$ gegeben durch $f = X^2 - 1$. Dann ist $f(5) = 24$.

Beweis. Es gilt $f(5) = 5^2 - 1 = 24$. □

Wir betonen, dass Polynome keine Funktionen *sind*, sondern nur zugehörige Polynomfunktionen *liefern*. So gibt es etwa über dem zweielementigen Körper aus Beispiel (6.43) unendlich viele Polynome, aber lediglich vier Polynomfunktionen (alle vier Abbildungen von $\{0, 1\}$ nach $\{0, 1\}$ sind Polynomfunktionen).
Einsetzen von Elementen ist verträglich mit den Ringstrukturen von $K[X]$ und K:

(11.5) Proposition.

- *Verträglichkeit mit den Additionen.* Für $f, g \in K[X]$, $x \in K$ ist $(f + g)(x) = f(x) + g(x)$.
- *Verträglichkeit der Nullen.* Für $x \in K$ ist $0(x) = 0$.
- *Verträglichkeit der Negative.* Für $f \in K[X]$, $x \in K$ ist $(-f)(x) = -f(x)$.
- *Verträglichkeit mit den Multiplikationen.* Für $f, g \in K[X]$, $x \in K$ ist $(fg)(x) = f(x)\, g(x)$.
- *Verträglichkeit der Einselemente.* Für $x \in K$ ist $1(x) = 1$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

Grad eines Polynoms

Es seien $f \in K[X]\setminus\{0\}$ und $a \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ gegeben. Wegen $f \neq 0$ ist $a \neq 0$ und wegen $a \in K^{(\mathbb{N}_0)}$ gibt es ein $n \in \mathbb{N}_0$ mit $a_n \neq 0$ und $a_i = 0$ für $i > n$. Somit ist

$$f = \sum_{i\in[0,n]} a_i X^i.$$

Wir wollen nun etwas Terminologie für diese endliche Darstellung eines Polynoms festlegen.

(11.6) Definition (Grad, Leitkoeffizient, normiertes Polynom)**.** Es seien $f \in K[X] \setminus \{0\}$ und $a \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ gegeben.

(a) Der *Grad* von f ist definiert als

$$\deg f := \max\{i \in \mathbb{N}_0 \mid a_i \neq 0\}.$$

(b) Der Koeffizient $\mathrm{lc}(f) := a_{\deg f}$ von f heißt *Leitkoeffizient* von f.

(c) Wir sagen, dass f ein *normiertes* Polynom ist, falls $\mathrm{lc}(f) = 1$ ist.

Wir betonen, dass das Nullpolynom keinen Grad hat.

(11.7) Beispiel.

(a) Das Polynom $X^2 - 1$ über $\mathbb{Q}$ hat den Grad 2 und den Leitkoeffizienten 1 und ist daher normiert.

(b) Das Polynom $-X^3 + 2X^2 + X + 1$ über $\mathbb{Q}$ hat den Grad 3 und den Leitkoeffizienten -1 und ist daher nicht normiert.

(11.8) Bemerkung. Es seien $f, g \in K[X] \setminus \{0\}$ gegeben.

(a) Wenn $f + g \neq 0$ ist, gilt

$$\deg(f + g) \leq \max(\deg f, \deg g).$$

Wenn $\deg f \neq \deg g$ ist, dann ist $f + g \neq 0$ und

$$\deg(f + g) = \max(\deg f, \deg g).$$

(b) Es gilt $fg \neq 0$ und

$$\deg(fg) = \deg f + \deg g.$$

Beweis. Es seien $a, b \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ und $g = \sum_{i\in\mathbb{N}_0} b_i X^i$ gegeben.

(a) Es ist $f + g = \sum_{i\in\mathbb{N}_0}(a_i + b_i)X^i$. Für $i \in \mathbb{N}_0$ mit $i > \max(\deg f, \deg g)$ gilt $a_i + b_i = 0 + 0 = 0$. Wenn also $f + g \neq 0$ ist, dann ist

$$\deg(f + g) = \max\{i \in \mathbb{N}_0 \mid a_i + b_i \neq 0\} \leq \max(\deg f, \deg g).$$

Wenn $\deg f < \deg g$ ist, so gilt $a_{\deg g} = 0$ und

$$a_{\deg g} + b_{\deg g} = 0 + b_{\deg g} = b_{\deg g} \neq 0,$$

also $f + g \neq 0$ und

$$\deg(f + g) = \max\{i \in \mathbb{N}_0 \mid a_i + b_i \neq 0\} = \deg g = \max(\deg f, \deg g).$$

Analog gilt: Wenn $\deg f > \deg g$ ist, so ist $f + g \neq 0$ und $\deg(f + g) = \deg f = \max(\deg f, \deg g)$.
Folglich impliziert $\deg f \neq \deg g$ stets $f + g \neq 0$ und $\deg(f + g) = \max(\deg f, \deg g)$.

(b) Es ist $fg = \sum_{k\in\mathbb{N}_0}(\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i b_j)X^k$. Für $k \in \mathbb{N}_0$ mit $k \geq \deg f + \deg g$ gilt

$$\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i b_j = \begin{cases} a_{\deg f} b_{\deg g}, & \text{falls } k = \deg f + \deg g, \\ 0, & \text{falls } k > \deg f + \deg g. \end{cases}$$

Folglich ist $fg \neq 0$ und $\deg(fg) = \deg f + \deg g$. □

(11.9) Korollar. Es ist

$$K[X]^\times = K^\times.$$

Beweis. Für $f \in K[X]^\times$ gilt

$$\deg f + \deg f^{-1} = \deg(ff^{-1}) = \deg 1 = 0,$$

also $\deg f = \deg f^{-1} = 0$ und damit $f, f^{-1} \in K^\times$. Folglich ist $K[X]^\times \subseteq K^\times$. Da jedes in K invertierbare Element insbesondere in $K[X]$ invertierbar ist, gilt umgekehrt auch $K^\times \subseteq K[X]^\times$. Insgesamt ist also $K[X]^\times = K^\times$. □

(11.10) Korollar. Der Polynomring $K[X]$ ist ein Integritätsbereich.

Beweis. Dies gilt nach Bemerkung (11.8)(b). □

Manchmal betrachten wir nur Polynome bis zum einem gegebenen Grad n. Wir legen eine Schreibweise fest:

(11.11) Notation. Für $n \in \mathbb{N}_0$ setzen wir

$$K[X]_{<n} := \{f \in K[X] \mid f = 0 \text{ oder } \deg f < n\}.$$

(11.12) Bemerkung. Für $n \in \mathbb{N}_0$ ist

$$K[X]_{<n} = \{\sum_{i\in[0,n-1]} a_i X^i \mid a \in K^{[0,n-1]}\}.$$

Insbesondere gilt $K[X]_{<0} = \{0\}$ und $K[X]_{<1} = K$.

(11.13) Definition (konstantes Polynom, lineares Polynom, quadratisches Polynom, kubisches Polynom)**.** Es sei $f \in K[X]$ gegeben.

(a) Wir nennen f ein *konstantes* Polynom, falls $f = 0$ oder $\deg f = 0$ ist.

(b) Wir nennen f ein *lineares* Polynom, falls $\deg f = 1$ ist.

(c) Wir nennen f ein *quadratisches* Polynom, falls $\deg f = 2$ ist.

(d) Wir nennen f ein *kubisches* Polynom, falls $\deg f = 3$ ist.

(11.14) Beispiel.

(a) Das Polynom 2 über $\mathbb{Q}$ ist konstant.

(b) Das Polynom $2X + 3$ über $\mathbb{Q}$ ist linear.

Nullstellen

Unter allen Körperelementen, die man in ein gegebenes Polynom einsetzen kann, sind diejenigen von besonderem Interesse, welche die Null als Wert annehmen:

(11.15) Definition (Nullstelle)**.** Es sei $f \in K[X]$ gegeben. Eine *Nullstelle* von f ist ein $a \in K$ mit

$$f(a) = 0.$$

(11.16) Beispiel. Es sei $f \in \mathbb{Q}[X]$ gegeben durch $f = X^2 - 1$. Dann sind 1 und -1 Nullstellen von f.

Beweis. Es gilt $f(1) = 1^2 - 1 = 0$ und $f(-1) = (-1)^2 - 1 = 0$. Folglich sind 1 und -1 Nullstellen von f. □

(11.17) Definition (algebraisch abgeschlossen)**.** Wir nennen K *algebraisch abgeschlossen*, falls jedes Polynom über K, welches nicht konstant ist, eine Nullstelle hat.

(11.18) Beispiel. Der Körper der reellen Zahlen $\mathbb{R}$ ist nicht algebraisch abgeschlossen.

Beweis. Für alle $a \in \mathbb{R}$ gilt $a^2 + 1 \geq 0 + 1 = 1 > 0$ und damit insbesondere $a^2 + 1 \neq 0$, d.h. das Polynom $X^2 + 1$ über $\mathbb{R}$ hat keine Nullstelle. Folglich ist $\mathbb{R}$ nicht algebraisch abgeschlossen. □

Der *Fundamentalsatz der Algebra*, welchen wir im Rahmen dieser Vorlesung nicht beweisen können, besagt, dass der Körper der komplexen Zahlen $\mathbb{C}$, siehe Definition (13.30), algebraisch abgeschlossen ist.

12 Teilbarkeitslehre

Ziel dieses Abschnitts ist es zu sehen, dass es starke formale Ähnlichkeiten zwischen dem Ring der ganzen Zahlen $\mathbb{Z}$ und dem Polynomring $K[X]$ über einem Körper K gibt.

Division mit Rest

Wir beginnen mit der (zumindest in Spezialfällen aus der Schule bekannten) Division mit Rest, für welche es sowohl eine Version für ganze Zahlen als auch für Polynome mit Koeffizienten in einem Körper gibt.

(12.1) Satz (Ganzzahldivision, Polynomdivision)**.**

(a) Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gegeben. Ferner seien Folgen $(q_i)_{i\in\mathbb{N}_0}$ und $(r_i)_{i\in\mathbb{N}_0}$ in $\mathbb{Z}$ rekursiv definiert durch

$$q_i := \begin{cases} 0 & \text{für } i = 0, \\ q_{i-1} + (\operatorname{sgn} r_{i-1})(\operatorname{sgn} b) & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \notin [0, |b| - 1], \\ q_{i-1} & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \in [0, |b| - 1], \end{cases}$$

$$r_i := \begin{cases} a & \text{für } i = 0, \\ r_{i-1} - (\operatorname{sgn} r_{i-1})|b| & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \notin [0, |b| - 1], \\ r_{i-1} & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \in [0, |b| - 1]. \end{cases}$$

(i) Für alle $i \in \mathbb{N}_0$ gilt

$$a = q_i b + r_i.$$

(ii) Es existiert ein $n \in [0, \max(0, |a| - |b| + 1)]$ mit $r_n \in [0, |b| - 1]$ und $q_i = q_n$, $r_i = r_n$ für $i \in \mathbb{N}_0$ mit $i \geq n$.

(b) Es seien ein Körper K und $f \in K[X]$, $g \in K[X] \setminus \{0\}$ gegeben. Ferner seien Folgen $(q_i)_{i\in\mathbb{N}_0}$ und $(r_i)_{i\in\mathbb{N}_0}$ in $K[X]$ rekursiv definiert durch

$$q_i := \begin{cases} 0, & \text{für } i = 0, \\ q_{i-1} + \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g}, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \notin K[X]_{<\deg g}, \\ q_{i-1}, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \in K[X]_{<\deg g}, \end{cases}$$

$$r_i := \begin{cases} f, & \text{für } i = 0, \\ r_{i-1} - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \notin K[X]_{<\deg g}, \\ r_{i-1}, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \in K[X]_{<\deg g}. \end{cases}$$

(i) Für alle $i \in \mathbb{N}_0$ gilt

$$f = q_i g + r_i.$$

(ii) Es existiert ein $n \in \mathbb{N}_0$ mit $r_n \in K[X]_{<\deg g}$ und $q_i = q_n$, $r_i = r_n$ für $i \in \mathbb{N}_0$ mit $i \geq n$. Wenn $f \neq 0$ ist, dann kann $n \in \mathbb{N}_0$ so gewählt werden, dass zusätzlich $n \leq \max(0, \deg f - \deg g + 1)$ gilt.

Beweis.

(a) (i) Wir führen Induktion nach i. Für $i = 0$ gilt

$$q_i b + r_i = q_0 b + r_0 = 0 \cdot b + a = a.$$

Nun sei $i \in \mathbb{N}$ so gegeben, dass $a = q_{i-1}b + r_{i-1}$ gilt. Dann erhalten wir auch

$$\begin{aligned} q_i b + r_i &= \begin{Bmatrix} (q_{i-1} + (\operatorname{sgn} r_{i-1})(\operatorname{sgn} b))b + r_{i-1} - (\operatorname{sgn} r_{i-1})|b|, & \text{falls } r_{i-1} \notin [0, |b| - 1], \\ q_{i-1}b + r_{i-1}, & \text{falls } r_{i-1} \in [0, |b| - 1] \end{Bmatrix} \\ &= \begin{Bmatrix} q_{i-1}b + (\operatorname{sgn} r_{i-1})(\operatorname{sgn} b)b + r_{i-1} - (\operatorname{sgn} r_{i-1})|b|, & \text{falls } r_{i-1} \notin [0, |b| - 1], \\ q_{i-1}b + r_{i-1}, & \text{falls } r_{i-1} \in [0, |b| - 1] \end{Bmatrix} \\ &= q_{i-1}b + r_{i-1} = a. \end{aligned}$$

Nach dem Induktionsprinzip gilt $a = q_i b + r_i$ für alle $i \in \mathbb{N}_0$.

(ii) Zunächst sei $i \in \mathbb{N}$ mit $r_{i-1} \notin [-|b|, |b| - 1]$ gegeben. Dann gilt

$$\begin{aligned} |r_i| = |r_{i-1} - (\operatorname{sgn} r_{i-1})|b|| &= \begin{Bmatrix} |r_{i-1} - |b||, & \text{falls } r_{i-1} \geq |b|, \\ |r_{i-1} + |b||, & \text{falls } r_{i-1} < -|b| \end{Bmatrix} \\ = \begin{Bmatrix} r_{i-1} - |b|, & \text{falls } r_{i-1} \geq |b|, \\ -(r_{i-1} + |b|), & \text{falls } r_{i-1} < -|b| \end{Bmatrix} &= \begin{Bmatrix} r_{i-1} - |b|, & \text{falls } r_{i-1} \geq |b|, \\ -r_{i-1} - |b|, & \text{falls } r_{i-1} < -|b| \end{Bmatrix} = |r_{i-1}| - |b| \\ < |r_{i-1}|. \end{aligned}$$

Für $i \in \mathbb{N}$ mit $r_{i-1} \in [-|b|, -1]$ gilt $r_i = r_{i-1} - (\operatorname{sgn} r_{i-1})|b| = r_{i-1} + |b| \in [0, |b| - 1]$. Für $i \in \mathbb{N}$ mit $r_{i-1} \in [0, |b| - 1]$ gilt $r_i = r_{i-1}$ und damit ebenfalls $r_i \in [0, |b| - 1]$.
Falls $a \notin [0, |b| - 1]$ ist, erhalten wir induktiv $r_{|a|-|b|+1} \in [0, |b| - 1]$. Falls hingegen $a \in [0, |b| - 1]$ ist, gilt $r_0 = a \in [0, |b| - 1]$. Es sei $n := \min\{i \in \mathbb{N}_0 \mid r_i \in [0, |b| - 1]\}$. Per Induktion folgt $q_i = q_n$ und $r_i = r_n$ für $i \in \mathbb{N}_0$ mit $i \geq n$. Wenn $a \notin [0, |b|-1]$ ist, gilt $n \leq |a|-|b|+1$, und wenn $a \in [0, |b|-1]$ ist, gilt $n = 0$. Insgesamt gilt also stets $n \leq \max(0, |a|-|b|+1)$ und damit $n \in [0, \max(0, |a|-|b|+1)]$.

(b) (i) Wir führen Induktion nach i. Für $i = 0$ gilt

$$q_i g + r_i = q_0 g + r_0 = 0 \cdot g + f = f.$$

Nun sei $i \in \mathbb{N}$ so gegeben, dass $f = q_{i-1}g + r_{i-1}$ gilt. Dann erhalten wir auch

$$\begin{aligned} q_i g + r_i &= \begin{Bmatrix} (q_{i-1} + \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g})g & & \\ \qquad + r_{i-1} - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g, & \text{falls } r_{i-1} \notin K[X]_{<\deg g}, \\ q_{i-1}g + r_{i-1}, & \text{falls } r_{i-1} \in K[X]_{<\deg g} \end{Bmatrix} \\ &= \begin{Bmatrix} q_{i-1}g + \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g & & \\ \qquad + r_{i-1} - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g, & \text{falls } r_{i-1} \notin K[X]_{<\deg g}, \\ q_{i-1}g + r_{i-1}, & \text{falls } r_{i-1} \in K[X]_{<\deg g} \end{Bmatrix} \\ &= q_{i-1}g + r_{i-1} = f. \end{aligned}$$

Nach dem Induktionsprinzip gilt $f = q_i g + r_i$ für alle $i \in \mathbb{N}_0$.

(ii) Zunächst sei $i \in \mathbb{N}$ mit $r_{i-1} \notin K[X]_{<\deg g}$ gegeben. Dann gilt

$$\begin{aligned} \deg(\operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g) &= \deg X^{\deg r_{i-1} - \deg g} + \deg g \\ &= \deg r_{i-1} - \deg g + \deg g = \deg r_{i-1} \end{aligned}$$

nach Bemerkung (11.8)(b) und damit $r_i = 0$ oder $r_i \neq 0$ und

$$\deg r_i = \deg(r_{i-1} - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g)$$

$$\leq \max(\deg r_{i-1}, \deg(\operatorname{lc}(r_{i-1})\operatorname{lc}(g)^{-1} X^{\deg r_{i-1}-\deg g} g)) = \deg r_{i-1}$$

nach Bemerkung (11.8)(a). Da der Koeffizient von $r_i = r_{i-1} - \operatorname{lc}(r_{i-1})\operatorname{lc}(g)^{-1} X^{\deg r_{i-1}-\deg g} g$ an der Stelle $\deg r_{i-1}$ durch $\operatorname{lc}(r_{i-1}) - \operatorname{lc}(r_{i-1})\operatorname{lc}(g)^{-1}\operatorname{lc}(g) = 0$ gegeben ist, gilt sogar $r_i = 0$ oder $r_i \neq 0$ und $\deg r_i < \deg r_{i-1}$, d.h. es ist $r_i \in K[X]_{<\deg r_{i-1}}$.
Für $i \in \mathbb{N}$ mit $r_{i-1} \in K[X]_{<\deg g}$ gilt hingegen $r_i = r_{i-1}$ und damit $r_i \in K[X]_{<\deg g}$.
Falls $f \notin K[X]_{<\deg g}$ ist, erhalten wir induktiv $r_{\deg f - \deg g + 1} \in K[X]_{<\deg g}$. Falls hingegen $f \in K[X]_{<\deg g}$ ist, gilt $r_0 = f \in K[X]_{<\deg g}$. Es sei $n := \min\{i \in \mathbb{N}_0 \mid r_i \in K[X]_{<\deg g}\}$. Per Induktion folgt $q_i = q_n$ und $r_i = r_n$ für $i \in \mathbb{N}_0$ mit $i \geq n$. Wenn $f \notin K[X]_{<\deg g}$ ist, gilt $n \leq \deg f - \deg g + 1$, und wenn $f \in K[X]_{<\deg g} \setminus \{0\}$ ist, gilt $n = 0$. Insgesamt gilt also, sofern $f \neq 0$ ist, stets $n \leq \max(0, \deg f - \deg g + 1)$. □

(12.2) Satz (Division mit Rest)**.**

(a) Für alle $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gibt es eindeutige $q \in \mathbb{Z}$, $r \in [0, |b| - 1]$ mit

$$a = qb + r.$$

(b) Es sei ein Körper K gegeben. Für alle $f \in K[X]$, $g \in K[X] \setminus \{0\}$ gibt es eindeutige $q \in K[X]$, $r \in K[X]_{<\deg g}$ mit

$$f = qg + r.$$

Beweis.

(a) Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gegeben. Nach Satz (12.1)(a) gibt es $q \in \mathbb{Z}$, $r \in [0, |b| - 1]$ mit $a = qb + r$. Für die Eindeutigkeit seien $q, q' \in \mathbb{Z}$, $r, r' \in [0, |b| - 1]$ mit $x = qb + r = q'b + r'$ gegeben. Dann ist

$$|q - q'|\,|b| = |(q - q')b| = |qb - q'b| = |r' - r| < |b|.$$

Wegen $b \neq 0$ impliziert dies $|q - q'| < 1$, also $|q - q'| = 0$. Folglich ist $q - q' = 0$, d.h. es gilt $q = q'$ und damit auch $r = a - qb = a - q'b = r'$.

(b) Es seien $f \in K[X]$, $g \in K[X] \setminus \{0\}$ gegeben. Nach Satz (12.1)(b) gibt es $q \in K[X]$, $r \in K[X]_{<\deg g}$ mit $f = qg + r$. Für die Eindeutigkeit seien $q, q' \in K[X]$, $r, r' \in K[X]_{<\deg g}$ mit $f = qg + r = q'g + r'$ gegeben. Dann ist

$$(q - q')g = qg - q'g = r' - r \in K[X]_{<\deg g}$$

und damit $(q - q')g = 0$ nach Bemerkung (11.8)(b). Wegen $g \neq 0$ impliziert dies aber bereits $q - q' = 0$, d.h. es gilt $q = q'$ und damit auch $r = f - qg = f - q'g = r'$. □

(12.3) Definition (ganzer Anteil, Rest)**.**

(a) Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gegeben und es seien $q \in \mathbb{Z}$, $r \in [0, |b| - 1]$ die eindeutigen ganzen Zahlen mit $a = qb + r$. Dann heißt $a \operatorname{div} b := q$ der *ganzzahlige Anteil* (oder der *ganze Anteil*) und $a \bmod b := r$ der *Rest* bei der *Ganzzahldivision* von a durch b.

(b) Es seien ein Körper K sowie $f \in K[X]$, $g \in K[X] \setminus \{0\}$ gegeben und es seien $q, r \in K[X]$ die eindeutigen Polynome mit $f = qg + r$ und mit $r = 0$ oder $r \neq 0$, $\deg r < \deg g$. Dann heißt $f \operatorname{div} g := q$ der *ganze Anteil* und $f \bmod g := r$ der *Rest* bei der *Polynomdivision* von f durch g.

(12.4) Beispiel.

(a) In $\mathbb{Z}$ ist $(-47) \operatorname{div} 9 = -6$ und $(-47) \bmod 9 = 7$.

(b) In $\mathbb{Q}[X]$ ist $(6X^3 + X^2 + 7) \operatorname{div} (2X^2 + X - 3) = 3X - 1$ und $(6X^3 + X^2 + 7) \bmod (2X^2 + X - 3) = 10X + 4$.

Beweis.

(a) Eine Ganzzahldivision liefert

$$\begin{aligned}-47 &= 0 \cdot 9 + (-47) = (-1) \cdot 9 + (-38) = (-2) \cdot 9 + (-29) = (-3) \cdot 9 + (-20) = (-4) \cdot 9 + (-11) \\ &= (-5) \cdot 9 + (-2) = (-6) \cdot 9 + 7.\end{aligned}$$

Folglich ist $(-47) \operatorname{div} 9 = -6$ und $(-47) \bmod 9 = 7$.

(b) Eine Polynomdivision liefert

$$\begin{aligned}6X^3 + X^2 + 7 &= 0 \cdot (2X^2 + X - 3) + 6X^3 + X^2 + 7 = 3X \cdot (2X^2 + X - 3) + (-2X^2 + 9X + 7) \\ &= (3X - 1) \cdot (2X^2 + X - 3) + (10X + 4).\end{aligned}$$

Folglich ist $(6X^3+X^2+7)\operatorname{div}(2X^2+X-3) = 3X-1$ und $(6X^3+X^2+7) \bmod (2X^2+X-3) = 10X+4$. □

Teilbarkeit

Als nächstes studieren wir die Teilbarkeitsrelation in $\mathbb{Z}$ und in $K[X]$ für einen Körper K.

(12.5) Definition (Teilbarkeit)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben. Wir sagen a *teilt* b (oder dass a ein *Teiler* von b ist oder dass a ein *Faktor* von b ist oder dass b ein *Vielfaches* von a ist), geschrieben $a \mid b$, falls ein $q \in R$ mit $b = qa$ existiert. Wenn a kein Teiler von b ist, so schreiben wir $a \nmid b$.

(12.6) Beispiel.

(a) In $\mathbb{Z}$ gilt $3 \mid 6$ und $4 \nmid 6$.

(b) In $\mathbb{Q}[X]$ gilt $X - 1 \mid X^2 - 1$ und $X \nmid X^2 - 1$.

Beweis.

(a) Es gilt $6 = 2 \cdot 3$, also $3 \mid 6$. Wegen $6 = 1 \cdot 4 + 2$ gibt es nach dem Satz über die Division mit Rest (12.2)(a) kein $q \in \mathbb{Z}$ mit $6 = q \cdot 4$, so dass $4 \nmid 6$ folgt.

(b) Es gilt $X^2 - 1 = (X + 1)(X - 1)$, also $X - 1 \mid X^2 - 1$. Wegen $X^2 - 1 = X \cdot X + (-1)$ gibt es nach dem Satz über die Division mit Rest (12.2)(b) kein $q \in \mathbb{Q}[X]$ mit $X^2 - 1 = q \cdot X$, so dass $X \nmid X^2 - 1$ folgt. □

(12.7) Bemerkung. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a \in R \setminus \{0\}$, $b \in R$ gegeben. Genau dann gilt $a \mid b$, wenn $b \bmod a = 0$ ist.

Beweis. Wenn $a \mid b$ gilt, dann gibt es ein $q \in R$ mit $b = qa = qa + 0$ und nach dem Satz über die Division mit Rest (12.2) folgt $b \bmod a = 0$. Gilt umgekehrt $b \bmod a = 0$, so folgt $b = (b \operatorname{div} a)a + (b \bmod a) = (b \operatorname{div} a)a$ und damit $a \mid b$. □

(12.8) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Die Teilbarkeitsrelation $\mid$ auf R ist eine Präordnung.

Beweis. Es seien $a, b, c \in R$ mit $a \mid b$ und $b \mid c$ gegeben, d.h. es gebe $p, q \in R$ mit $b = pa$ und $c = qb$. Dann folgt

$$c = qb = q(pa) = (qp)a,$$

also $a \mid c$. Folglich ist $\mid$ transitiv.
Für $a \in R$ gilt $a = 1 \cdot a$, also $a \mid a$. Folglich ist $\mid$ reflexiv.
Insgesamt ist $\mid$ eine Präordnung auf R. □

Wir studieren weitere Eigenschaften der Teilbarkeitsrelation.

(12.9) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K.

(a) Für $a, b, c \in R$ gilt: Wenn $a \mid b$ und $a \mid c$, dann auch $a \mid b + c$.

(b) Für $a \in R$ gilt $a \mid 0$.

(c) Für $a, b, c \in R$ gilt: Wenn $a \mid b$, dann auch $a \mid cb$.

Beweis.

(a) Es seien $a, b, c \in R$ mit $a \mid b$ und $a \mid c$ gegeben, d.h. es gebe $p, q \in R$ mit $b = pa$ und $c = qa$. Dann folgt

$$b + c = pa + qa = (p + q)a,$$

also $a \mid b + c$.

(b) Für $a \in R$ gilt $0 = 0 \cdot a$, also $a \mid 0$.

(c) Es seien $a, b, c \in R$ gegeben und es gelte $a \mid b$. Da auch $b \mid cb$ gilt, folgt $a \mid cb$ nach Proposition (12.8). □

(12.10) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Für $a, b, c \in R$ gilt genau dann $ca \mid cb$, wenn $c = 0$ ist oder $a \mid b$ gilt.

Beweis. Dies sei dem Leser zur Übung überlassen. □

Assoziiertheit

Nach Proposition (12.8) ist die Teilbarkeitsrelation $\mid$ eine Präordnung auf $\mathbb{Z}$ bzw. auf $K[X]$ für einen Körper K. Im Allgemeinen gilt jedoch keine Antisymmetrie, es kann in diesen Ringen Elemente a und b mit $a \mid b$ und $b \mid a$ und $a \neq b$ geben. Wir vergeben folgende Terminologie:

(12.11) Definition (assoziierte Elemente)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben. Wir sagen, dass a *assoziiert* zu b ist, wenn $a \mid b$ und $b \mid a$ gilt.

(12.12) Beispiel.

(a) In $\mathbb{Z}$ ist 3 assoziiert zu -3.

(b) In $\mathbb{Q}[X]$ ist $X - 1$ assoziiert zu $2X - 2$.

Beweis.

(a) Wegen $-3 = (-1) \cdot 3$ gilt $3 \mid -3$ und wegen $3 = (-1) \cdot (-3)$ gilt $-3 \mid 3$. Folglich ist 3 assoziiert zu -3.

(b) Wegen $2X - 2 = 2(X - 1)$ gilt $X - 1 \mid 2X - 2$ und wegen $X - 1 = \frac{1}{2}(2X - 2)$ gilt $2X - 2 \mid X - 1$. Folglich ist $X - 1$ assoziiert zu $2X - 2$. □

(12.13) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist a assoziiert zu b.

(b) Es gibt ein $u \in R^\times$ mit $b = ua$.

(c) Im Fall $R = \mathbb{Z}$ gilt $|a| = |b|$. Im Fall $R = K[X]$ gilt entweder $a = b = 0$ oder $\mathrm{lc}(a)^{-1}a = \mathrm{lc}(b)^{-1}b$.

Beweis. Zunächst gelte Bedingung (a), d.h. es sei a assoziiert zu b. Dann gilt $a \mid b$ und $b \mid a$, d.h. es gibt $p, q \in R$ mit $b = pa$ und $a = qb$. Wir erhalten

$$a = qb = q(pa) = (qp)a.$$

Da R nach Beispiel (6.49) bzw. nach Korollar (11.10) ein Integritätsbereich ist, folgt $a = 0$ oder $qp = 1$ nach Bemerkung (6.50). Wenn $a = 0$ ist, dann ist $b = pa = 0 = 1 \cdot a$ und es ist $1 \in R^\times$ nach Proposition (6.27)(b) auf Grund der Kommutativität des Rings R. Wenn $qp = 1$ ist, dann ist $p \in R^\times$. In jedem Fall gibt es ein $u \in R^\times$ mit $b = ua$, d.h. es gilt Bedingung (b).
Umgekehrt, wenn Bedingung (b) gilt, d.h. wenn es ein $u \in R^\times$ mit $b = ua$ gibt, dann gilt auch $a = u^{-1}b$ und damit $a \mid b$ und $b \mid a$, d.h. auch Bedingung (a) gilt.
Wir haben gezeigt, dass Bedingung (a) und Bedingung (b) äquivalent sind.

Um zu zeigen, dass Bedingung (b) und Bedingung (c) äquivalent sind, betrachten wir zunächst den Fall $R = \mathbb{Z}$. Dann ist $R^\times = \mathbb{Z}^\times = \{1, -1\}$. Folglich gibt es genau dann ein $u \in R^\times$ mit $b = ua$, wenn $|a| = |b|$ gilt, d.h. Bedingung (b) und Bedingung (c) sind in diesem Fall äquivalent.
Schließlich betrachten wir den Fall $R = K[X]$ für einen Körper K. Dann ist $R^\times = K[X]^\times = K^\times$. Folglich gibt es genau dann ein $u \in R^\times$ mit $b = ua$, wenn $a = b = 0$ oder $\mathrm{lc}(a)^{-1}a = \mathrm{lc}(b)^{-1}b$ gilt, d.h. Bedingung (b) und Bedingung (c) sind auch in diesem Fall äquivalent.
Wir haben gezeigt, dass Bedingung (b) und Bedingung (c) äquivalent sind.
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

Teilbarkeit und Nullstellen von Polynomen

Mit Hilfe der Teilbarkeitsrelation lassen sich Nullstellen von Polynomen über einem Körper charakterisieren:

(12.14) Definition (Linearfaktor)**.** Es seien ein Körper K und ein $f \in K[X]$ gegeben. Ein *Linearfaktor* von f ist ein lineares Polynom über K, welches ein Teiler von f ist.

Ein Linearfaktor eines Polynoms f über einem Körper K ist also insbesondere ein Polynom von der Form $aX+b$ für gewisse $a \in K \setminus \{0\} = K^\times$, $b \in K$.

(12.15) Beispiel. In $\mathbb{Q}[X]$ ist $X - 1$ ein Linearfaktor von $X^2 - 1$.

Beweis. Nach Beispiel (12.6)(b) gilt $X-1 \mid X^2-1$. Wegen $\deg(X-1) = 1$ ist $X-1$ ferner ein lineares Polynom, also ein Linearfaktor von $X^2 - 1$. □

(12.16) Proposition. Es seien ein Körper K, $f \in K[X]$ und $a \in K$ gegeben. Genau dann ist a eine Nullstelle von f, wenn $X - a$ ein Linearfaktor von f ist.

Beweis. Es sei $q := f \operatorname{div} (X - a)$ und $r := f \bmod (X - a)$. Dann gilt

$$f = (f \operatorname{div} (X - a)) \cdot (X - a) + f \bmod (X - a) = q \cdot (X - a) + r$$

und damit

$$f(a) = q(a) \cdot (a - a) + r(a) = r(a)$$

nach Proposition (11.5). Wegen $\deg(X - a) = 1$ ist $r \in K[X]_{<\deg(X-a)} = K[X]_{<1} = K$, also $r = r(a) = f(a)$. Somit ist a genau dann eine Nullstelle von f, wenn $r = 0$ ist, d.h. wenn $X - a$ ein Linearfaktor von f ist. □

Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

Als nächstes thematisieren wir die aus der Schule bekannten Begriffe des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen, wobei wir diese über die Teilbarkeitsrelation definieren.

(12.17) Definition (gemeinsamer Teiler, gemeinsames Vielfaches)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben.

(a) Ein *gemeinsamer Teiler* von a und b ist ein $d \in R$ so, dass $d \mid a$ und $d \mid b$ gilt.

(b) Ein *gemeinsames Vielfaches* von a und b ist ein $m \in R$ so, dass $a \mid m$ und $b \mid m$ gilt.

(12.18) Beispiel.

(a) (i) In $\mathbb{Z}$ sind 1, 2, -6 gemeinsame Teiler von 12 und 18.
(ii) In $\mathbb{Q}[X]$ sind 1, $X + 1$, $2X + 2$ gemeinsame Teiler von $X^2 - 1$ und $X^2 + 2X + 1$.

(b) (i) In $\mathbb{Z}$ sind 12 und -24 gemeinsame Vielfache von 4 und 6.
(ii) In $\mathbb{Q}[X]$ sind $X^3 - X^2 - X + 1$ und $-\frac{1}{2}X^4 + X^3 - X + \frac{1}{2}$ gemeinsame Vielfache von $X^2 - 2X + 1$ und $X^2 - 1$.

Beweis.

(a) (i) Wegen $12 = 12 \cdot 1$ gilt $1 \mid 12$ und wegen $18 = 18 \cdot 1$ gilt $1 \mid 18$. Folglich ist 1 ein gemeinsamer Teiler von 12 und 18.

Wegen $12 = 6 \cdot 2$ gilt $2 \mid 12$ und wegen $18 = 9 \cdot 2$ gilt $2 \mid 18$. Folglich ist 2 ein gemeinsamer Teiler von 12 und 18.

Wegen $12 = (-2) \cdot (-6)$ gilt $-6 \mid 12$ und wegen $18 = (-3) \cdot (-6)$ gilt $-6 \mid 18$. Folglich ist -6 ein gemeinsamer Teiler von 12 und 18.

(ii) Wegen $X^2-1 = (X^2-1)\cdot 1$ gilt $1 \mid X^2-1$ und wegen $X^2+2X+1 = (X^2+2X+1)\cdot 1$ gilt $1 \mid X^2+2X+1$. Folglich ist 1 ein gemeinsamer Teiler von X^2-1 und X^2+2X+1.

Wegen $X^2-1 = (X-1)(X+1)$ gilt $X+1 \mid X^2-1$ und wegen $X^2+2X+1 = (X+1)(X+1)$ gilt $X+1 \mid X^2+2X+1$. Folglich ist $X+1$ ein gemeinsamer Teiler von X^2-1 und X^2+2X+1.

Wegen $X^2-1 = (\frac{1}{2}X-\frac{1}{2})(2X+2))$ gilt $2X+2 \mid X^2-1$ und wegen $X^2+2X+1 = (\frac{1}{2}X+\frac{1}{2})(2X+2)$ gilt $2X+2 \mid X^2+2X+1$. Folglich ist $2X+2$ ein gemeinsamer Teiler von X^2-1 und X^2+2X+1.

(b) (i) Wegen $12 = 3\cdot 4$ gilt $4 \mid 12$ und wegen $12 = 2\cdot 6$ gilt $6 \mid 12$. Folglich ist 12 ein gemeinsames Vielfaches von 4 und 6.

Wegen $-24 = (-6) \cdot 4$ gilt $4 \mid -24$ und wegen $-24 = (-4) \cdot 6$ gilt $6 \mid -24$. Folglich ist -24 ein gemeinsames Vielfaches von 4 und 6.

(ii) Wegen $X^3 - X^2 - X + 1 = (X+1) \cdot (X^2 - 2X + 1)$ gilt $X^2 - 2X + 1 \mid X^3 - X^2 - X + 1$ und wegen $X^3-X^2-X+1 = (X-1)\cdot(X^2-1)$ gilt $X^2-1 \mid X^3-X^2-X+1$. Folglich ist X^3-X^2-X+1 ein gemeinsames Vielfaches von X^2-2X+1 und X^2-1.

Wegen $-\frac{1}{2}X^4+X^3-X+\frac{1}{2} = (-\frac{1}{2}X^2+\frac{1}{2})\cdot(X^2-2X+1)$ gilt $X^2-2X+1 \mid -\frac{1}{2}X^4+X^3-X+\frac{1}{2}$ und wegen $-\frac{1}{2}X^4+X^3-X+\frac{1}{2} = (-\frac{1}{2}X^2+X-\frac{1}{2})\cdot(X^2-1)$ gilt $X^2-1 \mid -\frac{1}{2}X^4+X^3-X+\frac{1}{2}$. Folglich ist $-\frac{1}{2}X^4+X^3-X+\frac{1}{2}$ ein gemeinsames Vielfaches von X^2-2X+1 und X^2-1. □

(12.19) Definition (größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben.

(a) Ein *größter gemeinsamer Teiler* von a und b ist ein gemeinsamer Teiler g von a und b derart, dass jeder gemeinsame Teiler d von a und b auch ein Teiler von g ist.

(b) Ein *kleinstes gemeinsames Vielfaches* von a und b ist ein gemeinsames Vielfaches l von a und b derart, dass jedes gemeinsame Vielfache m von a und b auch ein Vielfaches von l ist.

Ein größter gemeinsamer Teiler ist also ein größtes Element in der prägeordneten Menge der gemeinsamen Teiler zusammen mit der Teilbarkeitsrelation, vgl. Definition (8.15)(b).

(12.20) Beispiel.

(a) In $\mathbb{Z}$ ist -6 ein größter gemeinsamer Teiler von 12 und 18.

(b) In $\mathbb{Z}$ ist 12 ein kleinstes gemeinsames Vielfaches von 4 und 6.

Beweis.

(a) Es sei $T := \{d \in \mathbb{Z} \mid d \mid 12 \text{ und } d \mid 18\}$ die Menge der gemeinsamen Teiler von 12 und 18. Nach Beispiel (12.18)(a)(i) ist $-6 \in T$. Da für $a \in \mathbb{Z}$ aus $a \mid 12$ stets $|a| \leq |12| = 12$ folgt, gilt ferner $T \subseteq [-12, 12]$. Durch Ausrechnen ergibt sich

$$T = \{-6, -3, -2, -1, 1, 2, 3, 6\}.$$

Da für alle $d \in T$ auch $d \mid -6$ gilt, ist -6 somit ein größter gemeinsamer Teiler von 12 und 18.

(b) Es sei $I := \{m \in \mathbb{Z} \mid 4 \mid m \text{ und } 6 \mid m\}$ die Menge der gemeinsamen Vielfache von 4 und 6. Nach Beispiel (12.18)(b)(i) ist $12 \in I$. Es sei ein beliebiges gemeinsames Vielfaches m von 4 und 6 gegeben. Dann gilt $4 \mid m$ und $6 \mid m$, nach Proposition (12.9)(a) also auch $4 \mid m - (m \operatorname{div} 12) \cdot 12 = m \bmod 12$ und $6 \mid m - (m \operatorname{div} 12) \cdot 12 = m \bmod 12$. Folglich ist $m \bmod 12 \in I$. Durch Ausrechnen ergibt sich ferner $[0, 11] \cap I = \{0\}$, so dass $m \bmod 12 = 0$ folgt. Somit ist m ein Vielfaches von 12. Insgesamt ist 12 daher ein kleinstes gemeinsames Vielfaches von 4 und 6. □

Im Beweis von Beispiel (12.20) haben wir an entscheidender Stelle benutzt, dass die ganzzahligen Intervalle $[-12, 12]$ bzw. $[0, 11]$ endliche Mengen sind. Eine effizientere Methode zur Berechnung von größten gemeinsamen Teilern, welche sich auch für Polynome über Körpern eignet, werden wir in Satz (12.27) kennenlernen. Unter Ausnutzung von Satz (12.25) wird dies auch eine Möglichkeit zur effizienten Berechnung von kleinsten gemeisamen Vielfachen liefern.

(12.21) Bemerkung. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben.

(a) Es sei ein größter gemeinsamer Teiler g von a und b sowie $g' \in R$ gegeben. Die folgenden Bedingungen sind äquivalent.

(i) Das Element g' ist ein größter gemeinsamer Teiler von a und b.

(ii) Es ist g' ein gemeinsamer Teiler von a und b und für jeden gemeinsamen Teiler d von a und b mit $g' \mid d$ gilt auch $d \mid g'$.

(iii) Es ist g assoziiert zu g'.

(iv) Es ist g' ein gemeinsamer Teiler von a und b und es gilt $g \mid g'$.

(b) Es sei ein kleinstes gemeinsames Vielfaches l von a und b sowie $l' \in R$ gegeben. Die folgenden Bedingungen sind äquivalent.

(i) Das Element l' ist ein kleinstes gemeinsames Vielfaches von a und b.

(ii) Es ist l' ein gemeinsames Vielfaches von a und b und für jedes gemeinsame Vielfache m von a und b mit $m \mid l'$ gilt auch $l' \mid m$.

(iii) Es ist l assoziiert zu l'.

(iv) Es ist l' ein gemeinsames Vielfaches von a und b und es gilt $l' \mid l$.

Beweis.

(a) Größte gemeinsame Teiler von a und b sind größte Elemente in der prägeordneten Menge

$$\{d \in R \mid d \text{ ist ein gemeinsamer Teiler von } a \text{ und } b\}$$

zusammen mit der Teilbarkeitsrelation. Die Äquivalenz von Bedingung (i), Bedingung (ii), Bedingung (iii) und Bedingung (iv) folgt aus Proposition (8.18)(b).

(b) Dies lässt sich dual zu (a) beweisen. □

(12.22) Lemma (Lemma von Bézout)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben.

(a) Es sei $I := \{d \in R \mid \text{es gibt } x, y \in R \text{ mit } d = xa + yb\}$.

(i) Falls $a = 0$ und $b = 0$, sei $g = 0$. Falls $a \neq 0$ oder $b \neq 0$, sei $g \in I \setminus \{0\}$ so, dass folgendes gilt: Im Fall $R = \mathbb{Z}$ gelte

$$|g| = \min\{|d| \mid d \in I \setminus \{0\}\}.$$

Im Fall $R = K[X]$ für einen Körper K gelte

$$\deg g = \min\{\deg d \mid d \in I \setminus \{0\}\}.$$

Dann ist g ein größter gemeinsamer Teiler von a und b. Insbesondere existiert ein größter gemeinsamer Teiler von a und b.

(ii) Es sei $g \in R$ ein größter gemeinsamer Teiler von a und b. Dann ist $g \in I$.

(b) Es sei $I := \{m \in R \mid \text{es gibt } x, y \in R \text{ mit } m = xa \text{ und } m = yb\}$.

(i) Falls $a = 0$ oder $b = 0$, sei $l = 0$. Falls $a \neq 0$ und $b \neq 0$, sei $l \in I \setminus \{0\}$ so, dass folgendes gilt: Im Fall $R = \mathbb{Z}$ gelte

$$|l| = \min\{|m| \mid m \in I \setminus \{0\}\}.$$

Im Fall $R = K[X]$ für einen Körper K gelte

$$\deg l = \min\{\deg m \mid m \in I \setminus \{0\}\}.$$

Dann ist l ein kleinstes gemeinsames Vielfaches von a und b. Insbesondere existiert ein kleinstes gemeinsames Vielfaches von a und b.

(ii) Es sei $l \in R$ ein kleinstes gemeinsames Vielfaches von a und b. Dann ist $l \in I$.

Beweis.

(a) (i) Wenn $a = 0$ und $b = 0$ ist, so ist $g = 0$ ein größter gemeinsamer Teiler von a und b. Im Folgenden sei daher $a \neq 0$ oder $b \neq 0$, so dass auch $g \neq 0$ gilt. Da $g \in I$ ist, gibt es $x, y \in R$ mit $g = xa + yb$. Folglich ist

$$a \bmod g = a - (a \operatorname{div} g)g = a - (a \operatorname{div} g)(xa + yb) = (1 - (a \operatorname{div} g)x)a + (a \operatorname{div} g)yb \in I,$$

also $a \bmod g = 0$ nach Wahl von g. Somit ist g ein Teiler von a. Analog lässt sich zeigen, dass g ein Teiler von b ist. Ferner ist jeder gemeinsame Teiler d von a und b nach Proposition (12.9)(a), (c) auch ein Teiler von $xa + yb = g$. Insgesamt ist g daher ein größter gemeinsamer Teiler von a und b.

(ii) Nach (i) gibt es einen größten gemeinsamen Teiler g' von a und b mit $g' \in I$, also derart, dass $g' = x'a + y'b$ für gewisse $x', y' \in R$. Da sowohl g als auch g' ein größter gemeinsamer Teiler von a und b ist, sind g und g' nach Bemerkung (12.21)(a) zueinander assoziiert. Nach Proposition (12.13) gibt es ein $u \in R^\times$ mit

$$g = ug' = u(x'a + y'b) = (ux')a + (uy')b.$$

Folglich ist auch $g \in I$. □

(b) (i) Wenn $a = 0$ oder $b = 0$ ist, so ist $l = 0$ ein kleinstes gemeinsames Vielfaches von a und b. Im Folgenden sei daher $a \neq 0$ und $b \neq 0$, so dass auch $l \neq 0$ gilt. Da $l \in I$ ist, gibt es $x, y \in R$ mit $l = xa = yb$, d.h. l ist ein gemeinsames Vielfaches von a und b. Es sei ein beliebiges gemeinsames Vielfaches m von a und b gegeben. Dann gilt $a \mid m$ und $b \mid m$, nach Proposition (12.9)(a), (c) also auch $a \mid m - (m \operatorname{div} l)l = m \bmod l$ und $b \mid m - (m \operatorname{div} l)l = m \bmod l$. Folglich ist $m \bmod l \in I$, also $m \bmod l = 0$ nach Wahl von l. Somit ist m ein Vielfaches von l. Insgesamt ist l daher ein kleinstes gemeinsames Vielfaches von a und b.

(ii) Da l als kleinstes gemeinsames Vielfaches von a und b insbesondere ein gemeinsames Vielfaches von a und b ist, gibt es $x, y \in R$ mit $l = xa = yb$. Folglich ist $l \in I$.

Nach dem Lemma von Bézout (12.22) gibt es für jedes Paar ganzer Zahlen bzw. von Polynomen über einem Körper einen größten gemeinsamen Teiler sowie ein kleinstes gemeinsames Vielfaches, und nach Bemerkung (12.21) sind diese eindeutig bis auf Assoziiertheit. Im Folgenden legen wir eine Notation für einen ausgezeichneten größten gemeinsamen Teiler und ein ausgezeichnetes kleinstes gemeinsames Vielfaches fest.

(12.23) Notation.

(a) (i) Es seien $a, b \in \mathbb{Z}$ gegeben. Den nicht-negativen größten gemeinsamen Teiler von a und b notieren wir als $\gcd(a, b) = \gcd^{\mathbb{Z}}(a, b)$.

(ii) Es seien ein Körper K und $f, g \in K[X]$ gegeben. Falls $f = 0$ und $g = 0$ ist, so setzen wir $\gcd(f, g) = \gcd^{K[X]}(f, g) := 0$. Falls $f \neq 0$ oder $g \neq 0$ ist, so notieren wir den normierten größten gemeinsamen Teiler von f und g als $\gcd(f, g) = \gcd^{K[X]}(f, g)$.

(b) (i) Es seien $a, b \in \mathbb{Z}$ gegeben. Das nicht-negative kleinste gemeinsame Vielfache von a und b notieren wir als $\operatorname{lcm}(a, b) = \operatorname{lcm}^{\mathbb{Z}}(a, b)$.

(ii) Es seien ein Körper K und $f, g \in K[X]$ gegeben. Falls $f = 0$ oder $g = 0$ ist, so setzen wir $\operatorname{lcm}(f, g) = \operatorname{lcm}^{K[X]}(f, g) := 0$. Falls $f \neq 0$ und $g \neq 0$ ist, so notieren wir das normierte kleinste gemeinsame Vielfache von f und g als $\operatorname{lcm}(f, g) = \operatorname{lcm}^{K[X]}(f, g)$.

Wir haben also in den Fällen $R = \mathbb{Z}$ und $R = K[X]$ für einen Körper K wohldefinierte Abbildungen

$$\begin{aligned} &\gcd\colon R \times R \to R, \\ &\operatorname{lcm}\colon R \times R \to R \end{aligned}$$

konstruiert.

(12.24) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b, d, p, q \in R$ mit $a = pd$ und $b = qd$ gegeben.

(a) Es ist $\gcd(a, b)$ assoziiert zu $\gcd(p, q)d$.

(b) Es ist $\operatorname{lcm}(a, b)$ assoziiert zu $\operatorname{lcm}(p, q)d$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(12.25) Satz. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben. Dann ist ab assoziiert zu $\gcd(a, b) \operatorname{lcm}(a, b)$.

Beweis. Zunächst gelte $\gcd(a, b) = 1$. Nach dem Lemma von Bézout (12.22) gibt es dann $x, y \in R$ mit $1 = xa + yb$. Da $\operatorname{lcm}(a, b)$ ein gemeinsames Vielfaches von a und b ist, gibt es ferner $p, q \in R$ mit $\operatorname{lcm}(a, b) = pa = qb$. Es folgt

$$(xq + yp)ab = xqab + ypab = qbxa + payb = \operatorname{lcm}(a, b)xa + \operatorname{lcm}(a, b)yb = \operatorname{lcm}(a, b)(xa + yb) = \operatorname{lcm}(a, b),$$

also $ab \mid \operatorname{lcm}(a, b)$. Andererseits ist aber auch ab ein gemeinsames Vielfaches von a und b, und da $\operatorname{lcm}(a, b)$ ein kleinstes gemeinsames Vielfaches von a und b ist, folgt $\operatorname{lcm}(a, b) \mid ab$. Folglich ist ab assoziiert zu $\operatorname{lcm}(a, b) = \gcd(a, b) \operatorname{lcm}(a, b)$.
Nun sei $\gcd(a, b)$ beliebig. Wenn $a = 0$ und $b = 0$ ist, so gilt

$$ab = 0 \cdot 0 = \gcd(a, b) \operatorname{lcm}(a, b).$$

Es sei also im Folgenden $a \neq 0$ oder $b \neq 0$, so dass $\gcd(a, b) \neq 0$ ist. Da $\gcd(a, b)$ ein gemeinsamer Teiler von a und b ist, gibt es $p, q \in R$ mit $a = p \gcd(a, b)$ und $b = q \gcd(a, b)$. Nach Proposition (12.24) gilt $\gcd(p, q) = 1$ und $\operatorname{lcm}(a, b) = \gcd(a, b) \operatorname{lcm}(p, q)$. Nach dem bereits bewiesenen Spezialfall ist pq assoziiert zu $\gcd(p, q) \operatorname{lcm}(p, q) = \operatorname{lcm}(p, q)$. Folglich ist auch $ab = p \gcd(a, b)\, q \gcd(a, b) = \gcd(a, b)^2\, pq$ assoziiert zu $\gcd(a, b)^2 \operatorname{lcm}(p, q) = \gcd(a, b) \operatorname{lcm}(a, b)$. □

Alternativer Beweis von Beispiel (12.20)(b). Es sei $T := \{d \in \mathbb{Z} \mid d \mid 4 \text{ und } d \mid 6\}$ die Menge der gemeinsamen Teiler von 4 und 6. Wegen $4 = 2 \cdot 2$ und $6 = 3 \cdot 2$ ist $2 \in T$. Da für $a \in \mathbb{Z}$ aus $a \mid 6$ stets $|a| \leq |6| = 6$ folgt, gilt ferner $T \subseteq [-6, 6]$. Durch Ausrechnen ergibt sich

$$T = \{-2, -1, 1, 2\}.$$

Da für alle $d \in T$ auch $d \mid 2$ gilt und $2 \geq 0$ gilt, ist somit $\gcd(4, 6) = 2$.
Nach Satz (12.25) folgt

$$\operatorname{lcm}(4, 6) = \frac{4 \cdot 6}{\gcd(4, 6)} = \frac{4 \cdot 6}{2} = 12.$$ □

Der euklidische Algorithmus

Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Nach dem Lemma von Bézout (12.22)(a)(ii) wissen wir, dass es für $a, b \in R$ stets $x, y \in R$ mit $\gcd(a, b) = xa + yb$ gibt. Wir wollen nun einen Algorithmus herleiten, welcher zum einen $\gcd(a, b)$ und zum anderen eine solche Darstellung $(x, y) \in R \times R$ berechnet.

(12.26) Lemma. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Für $a \in R$, $b \in R \setminus \{0\}$ ist

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

Beweis. Es seien $a, b \in R$ gegeben. Für $d \in R$ mit $d \mid b$ gilt nach Proposition (12.9)(a), (c) genau dann $d \mid a$, wenn $d \mid a - (a \operatorname{div} b)b = a \bmod b$ gilt. Somit sind die gemeinsamen Teiler von a und b genau die gemeinsamen Teiler von b und $a \bmod b$. Als größte Elemente in der prägeordneten Menge der gemeinsamen Teiler von a und b mit der Teilbarkeitsrelation sind dann aber auch die größten gemeinsamen Teiler von a und b genau die größten gemeinsamen Teiler von b und $a \bmod b$. Folglich gilt auch $\gcd(a, b) = \gcd(b, a \bmod b)$. □

(12.27) Satz (erweiterter euklidischer Algorithmus)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a \in R$, $b \in R \setminus \{0\}$ gegeben. Es seien Folgen $(r_i)_{i\in\mathbb{N}_0}$, $(x_i)_{i\in\mathbb{N}_0}$, $(y_i)_{i\in\mathbb{N}_0}$ in R rekursiv definiert durch

$$r_i := \begin{cases} a, & \text{für } i = 0, \\ b, & \text{für } i = 1, \\ r_{i-2} \bmod r_{i-1}, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} \neq 0, \\ 0, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} = 0, \end{cases}$$

$$x_i := \begin{cases} 1, & \text{für } i = 0, \\ 0, & \text{für } i = 1, \\ x_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})x_{i-1}, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} \neq 0, \\ 0, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} = 0, \end{cases}$$

$$y_i := \begin{cases} 0, & \text{für } i = 0, \\ 1, & \text{für } i = 1, \\ y_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})y_{i-1}, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} \neq 0, \\ 0, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} = 0. \end{cases}$$

(a) Für alle $i \in \mathbb{N}_0$ gilt

$$r_i = x_i a + y_i b.$$

(b) Es existiert ein $n \in \mathbb{N}$ so, dass r_n assoziiert zu $\gcd(a, b)$ ist und $r_i = 0$ für $i > n$ gilt. Im Fall $R = \mathbb{Z}$ kann $n \in \mathbb{N}$ so gewählt werden, dass $n \leq |b| + 1$ gilt. Im Fall $R = K[X]$ für einen Körper K kann $n \in \mathbb{N}$ so gewählt werden, dass $n \leq \deg b + 2$ gilt.

Beweis.

(a) Um $x_i a + y_i b = r_i$ für alle $i \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach i. Zunächst gilt

$$x_0 a + y_0 b = 1 \cdot a + 0 \cdot b = a = r_0,$$
$$x_1 a + y_1 b = 0 \cdot a + 1 \cdot b = b = r_1,$$

also $x_i a + y_i b = r_i$ für $i \in \{0, 1\}$. Es sei also ein $i \in \mathbb{N}_0$ mit $i \geq 2$ gegeben und gelte $x_{i-2}a + y_{i-2}b = r_{i-2}$ sowie $x_{i-1}a + y_{i-1}b = r_{i-1}$. Wenn $r_{i-1} \neq 0$ ist, erhalten wir

$$\begin{aligned} x_i a + y_i b &= (x_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})x_{i-1})a + (y_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})y_{i-1})b \\ &= x_{i-2}a - (r_{i-2} \operatorname{div} r_{i-1})x_{i-1}a + y_{i-2}b - (r_{i-2} \operatorname{div} r_{i-1})y_{i-1}b \\ &= x_{i-2}a + y_{i-2}b - (r_{i-2} \operatorname{div} r_{i-1})(x_{i-1}a + y_{i-1}b) = r_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})r_{i-1} = r_i. \end{aligned}$$

Wenn $r_{i-1} = 0$ ist, erhalten wir ebenfalls

$$x_i a + y_i b = 0 \cdot a + 0 \cdot b = 0 = r_i.$$

Nach dem Induktionsprinzip gilt $x_i a + y_i b = r_i$ für alle $i \in \mathbb{N}_0$.

(b) Im Fall $R = \mathbb{Z}$ gilt für $i \geq 2$ stets $r_i = 0$ oder $r_i \neq 0$, $|r_i| = |r_{i-2} \bmod r_{i-1}| < |r_{i-1}|$, per Induktion also $r_{|b|+1} = 0$. Im Fall $R = K[X]$ für einen Körper K gilt für $i \geq 2$ stets $r_i = 0$ oder $r_i \neq 0$, $\deg r_i = \deg(r_{i-2} \bmod r_{i-1}) < \deg r_{i-1}$, per Induktion also $r_{(\deg b)+2} = 0$.

Wir setzen $n := \min\{i \in \mathbb{N} \mid r_i = 0\} - 1$. Dann ist $r_{n+1} = 0$, induktiv also $r_i = 0$ für alle $i \in \mathbb{N}_0$ mit $i > n$. Nach Lemma (12.26) gilt ferner

$$\gcd(r_{i-2}, r_{i-1}) = \gcd(r_{i-1}, r_{i-2} \bmod r_{i-1}) = \gcd(r_{i-1}, r_i)$$

für $i \in \mathbb{N}_0$, $i \geq 2$ mit $r_{i-1} \neq 0$. Induktiv erhalten wir

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_n, r_{n+1}) = \gcd(r_n, 0).$$

Nun ist aber r_n assoziiert zu $\gcd(r_n, 0) = \gcd(a, b)$. □

(12.28) Beispiel.

(a) In $\mathbb{Z}$ ist $\gcd(2238, 168) = 6$ und

$$6 = (-3) \cdot 2238 + 40 \cdot 168.$$

(b) In $\mathbb{Q}[X]$ ist $\gcd(X^3 + X^2 - X - 1, X^2 - 2X + 1) = X - 1$ und

$$X - 1 = \frac{1}{4}(X^3 + X^2 - X - 1) + (-\frac{1}{4}X - \frac{3}{4})(X^2 - 2X + 1).$$

Beweis.

(a) Wir berechnen $\gcd(2238, 168)$ mit dem euklidischen Algorithmus:

$$\begin{aligned} 2238 &= 13 \cdot 168 + 54, \\ 168 &= 3 \cdot 54 + 6, \\ 54 &= 9 \cdot 6 + 0. \end{aligned}$$

Nach Satz (12.27)(b) ist $\gcd(2238, 168) = 6$. Wir setzen

$$\begin{aligned} r_0 &:= 2238, & & \\ r_1 &:= 168, & q_1 &:= 13, \\ r_2 &:= 54, & q_2 &:= 3, \\ r_3 &:= 6, & q_3 &:= 9, \end{aligned}$$

und berechnen $x_i, y_i \in \mathbb{Z}$ für $i \in \{0, 1, 2, 3\}$ mit dem erweiterten euklidischen Algorithmus:

$$\begin{aligned} x_0 &:= 1, & y_0 &:= 0, \\ x_1 &:= 0, & y_1 &:= 1, \\ x_2 &:= x_0 - q_1 x_1 = 1 - 13 \cdot 0 = 1, & y_2 &:= y_0 - q_1 y_1 = 0 - 13 \cdot 1 = -13, \\ x_3 &:= x_1 - q_2 x_2 = 0 - 3 \cdot 1 = -3, & y_3 &:= y_1 - q_2 y_2 = 1 - 3 \cdot (-13) = 40. \end{aligned}$$

Nach Satz (12.27)(a) ist

$$6 = r_3 = x_3 \cdot 2238 + y_3 \cdot 168 = (-3) \cdot 2238 + 40 \cdot 168.$$

(b) Wir berechnen $\gcd(X^3 + X^2 - X - 1, X^2 - 2X + 1)$ mit dem euklidischen Algorithmus:

$$\begin{aligned} X^3 + X^2 - X - 1 &= (X + 3)(X^2 - 2X + 1) + 4X - 4, \\ X^2 - 2X + 1 &= (\frac{1}{4}X - \frac{1}{4})(4X - 4) + 0. \end{aligned}$$

Nach Satz (12.27)(b) ist $\gcd(X^3+X^2-X-1, X^2-2X+1)$ assoziiert zu $4X-4$, also

$$\gcd(X^3+X^2-X-1, X^2-2X+1) = \frac{1}{4}(4X-4) = X-1.$$

Wir setzen

$$\begin{aligned} r_0 &:= X^3+X^2-X-1, & & \\ r_1 &:= X^2-2X+1, & q_1 &:= X+3, \\ r_2 &:= 4X-4, & q_2 &:= \frac{1}{4}X - \frac{1}{4}, \end{aligned}$$

und berechnen $h_i, k_i \in \mathbb{Q}[X]$ für $i \in \{0,1,2\}$ mit dem erweiterten euklidischen Algorithmus:

$$\begin{aligned} h_0 &:= 1, & k_0 &:= 0, \\ h_1 &:= 0, & k_1 &:= 1, \\ h_2 &:= h_0 - q_1 h_1 = 1 - (X+3)\cdot 0 = 1, & k_2 &:= k_0 - q_1 k_1 = 0 - (X+3)\cdot 1 = -X-3. \end{aligned}$$

Nach Satz (12.27)(a) ist

$$4X-4 = r_2 = h_2 f + k_2 g = 1(X^3+X^2-X-1) + (-X-3)(X^2-2X+1)$$

und damit

$$X-1 = \frac{1}{4}(4X-4) = \frac{1}{4}(X^3+X^2-X-1) + (-\frac{1}{4}X - \frac{3}{4})(X^2-2X+1). \qquad \square$$

Lineare Gleichungen in 2 Unbekannten

Als Anwendung des Lemma von Bézout (12.22)(a) sowie des erweiterten euklidischen Algorithmus (12.27) betrachten wir folgendes Kriterium zur Bestimmung der Lösungen einer linearen Gleichung in 2 Unbekannten über $\mathbb{Z}$ bzw. über $K[X]$ für einen Körper K an:

(12.29) Satz (Lösbarkeitskriterium und Lösungsbestimmung für lineare Gleichungen in 2 Unbekannten)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b, c \in R$ gegeben.

(a) Genau dann gibt es $x, y \in R$ mit $xa + yb = c$, wenn

$$\gcd(a,b) \mid c$$

gilt.

(b) Es seien $p, q, r \in R$ mit $a = p\gcd(a,b)$, $b = q\gcd(a,b)$ und $c = r\gcd(a,b)$ gegeben. Ferner seien $x', y' \in R$ mit $x'a + y'b = \gcd(a,b)$ gegeben. Dann ist

$$\begin{aligned} \{(x,y) \in R \times R \mid xa+yb = c\} &= \begin{cases} R \times R, & \text{falls } (a,b) = (0,0), \\ \{(rx' + mq, ry' - mp) \mid m \in R\}, & \text{falls } (a,b) \neq (0,0) \end{cases} \\ &= \begin{cases} R \times R, & \text{falls } (a,b) = (0,0), \\ (rx', ry') + R\,(q,-p), & \text{falls } (a,b) \neq (0,0). \end{cases} \end{aligned}$$

Beweis. Dies sei dem Leser zur Übung überlassen. $\square$

(12.30) Beispiel.

(a) Es ist

$$\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \cdot 2238 + y \cdot 168 = -24\} = (12,-160) + \mathbb{Z}\,(28,-373).$$

(b) Es ist

$$\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \cdot 2238 + y \cdot 168 = 4\} = \emptyset.$$

Beweis. Nach Beispiel (12.28)(a) ist $\gcd(2238, 168) = 6 = (-3) \cdot 2238 + 40 \cdot 168$.

(a) Wegen $2238 = 373 \cdot 6$, $168 = 28 \cdot 6$ und $-24 = -4 \cdot 6$ gilt

$$\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \cdot 2238 + y \cdot 168 = -24\} = (12, -160) + \mathbb{Z}\,(28, -373).$$

nach Satz (12.29).

(b) Wegen $6 \nmid 4$ gilt

$$\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \cdot 2238 + y \cdot 168 = 4\} = \emptyset$$

nach Satz (12.29)(a). □

Irreduzibilität

Zum Ende dieses Abschnittes wollen wir die elementaren Bausteine bzgl. der Teilbarkeitsrelation näher betrachten.

(12.31) Definition ((ir)reduzibles Element)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $p \in R \setminus (\{0\} \dot\cup R^\times)$ gegeben. Wir nennen p *irreduzibel*, falls für $x, y \in R$ aus $p = xy$ stets $x \in R^\times$ oder $y \in R^\times$ folgt, ansonsten *reduzibel*.

Die folgende Bemerkung besagt, dass ein Element genau dann irreduzibel ist, wenn es keine Teiler außer den unvermeidlichen hat: invertierbare und zum gegebenen Element assoziierte Elemente.

(12.32) Bemerkung. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $p \in R \setminus (\{0\} \dot\cup R^\times)$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist p irreduzibel.

(b) Jeder Teiler von p ist entweder invertierbar oder assoziiert zu p.

(c) Im Fall $R = \mathbb{Z}$ ist jeder positive Teiler von p entweder gleich 1 oder gleich $|p|$. Im Fall $R = K[X]$ ist jeder normierte Teiler von p entweder gleich 1 oder gleich $\mathrm{lc}(p)^{-1}\, p$.

Beweis. Zunächst gelte Bedingung (a), d.h. p sei irreduzibel. Ferner sei ein Teiler d von p gegeben, so dass es ein $q \in R$ mit $p = qd$ gibt. Die Irreduzibilität von p impliziert $d \in R^\times$ oder $q \in R^\times$. Wenn $q \in R^\times$ ist, so ist d nach Proposition (12.13) zu p assoziiert. Folglich gilt Bedingung (b).
Umgekehrt gelte Bedingung (b), d.h. jeder Teiler von p sei entweder invertierbar oder assoziiert zu p. Um zu zeigen, dass p irreduzibel ist, seien $x, y \in R$ mit $p = xy$ gegeben. Dann gilt $y \mid p$. Nach Voraussetzung ist also $y \in R^\times$ oder y ist assoziiert zu p. Wenn y assoziiert zu p ist, so gibt es nach Proposition (12.13) ein $u \in R^\times$ mit $y = up$ und daher mit $p = xy = xup$. Da $p \neq 0$ und R ein Integritätsbereich ist, folgt $xu = 1$ nach Bemerkung (6.50) und damit $x = u^{-1} \in R^\times$. Somit gilt $x \in R^\times$ oder $y \in R^\times$. Folglich ist p irreduzibel, d.h. es gilt Bedingung (a).
Wir haben gezeigt, dass Bedingung (a) und Bedingung (b) äquivalent sind.
Um zu zeigen, dass Bedingung (b) und Bedingung (c) äquivalent sind, betrachten wir zunächst den Fall $R = \mathbb{Z}$. Nach Proposition (12.13) ist dann jeder Teiler von p assoziiert zu einem positiven Teiler von p. Jeder positive Teiler von p ist aber genau dann invertierbar, wenn er gleich 1 ist, und genau dann assoziiert zu p, wenn er gleich $|p|$ ist. Somit sind Bedingung (b) und Bedingung (c) in diesem Fall äquivalent.
Schließlich betrachten wir den Fall $R = K[X]$ für einen Körper K. Nach Proposition (12.13) ist dann jeder Teiler von p assoziiert zu einem normierten Teiler von p. Jeder normierte Teiler von p ist aber genau dann invertierbar, wenn er gleich 1 ist, und genau dann assoziiert zu p, wenn er gleich $\mathrm{lc}(p)^{-1}\, p$ ist. Somit sind Bedingung (b) und Bedingung (c) auch in diesem Fall äquivalent.
Wir haben gezeigt, dass Bedingung (b) und Bedingung (c) äquivalent sind.
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

In $\mathbb{Z}$ ist ein Element $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ nach Bemerkung (12.32) genau dann irreduzibel, wenn für jeden positiven Teiler d von p stets $d = 1$ oder $d = |p|$ gilt. Damit sind die positiven irreduziblen ganzen Zahlen genau die Primzahlen.

(12.33) Beispiel.

(a) In $\mathbb{Z}$ ist -3 irreduzibel und 12 reduzibel.

(b) In $\mathbb{Q}[X]$ ist X^2+1 irreduzibel und X^2-1 reduzibel.

Beweis.

(a) Es sei $T := \{d \in \mathbb{Z} \mid d \mid -3\}$ die Menge der Teiler von -3. Da für $d \in \mathbb{Z}$ aus $d \mid -3$ stets $|d| \leq |-3| = 3$ folgt, gilt $T \subseteq [-3,3]$. Durch Ausrechnen ergibt sich $T = \{-3,-1,1,3\}$. Nach Bemerkung (12.32) ist -3 irreduzibel.

Hingegen ist $12 = 3 \cdot 4$ und $3, 4 \notin \mathbb{Z}^\times$. Folglich ist 12 reduzibel.

(b) Es sei d ein Teiler von X^2+1. Wegen $a^2+1 \geq 0+1 = 1 > 0$ für $a \in \mathbb{Q}$ hat X^2+1 keine Nullstelle. Nach Proposition (12.16) ist daher $\deg d \neq 1$. Also ist $\deg d = 0$ oder $\deg d = 2$. Nach Bemerkung (12.32) ist X^2+1 irreduzibel.

Hingegen ist $X^2-1 = (X-1)(X+1)$ und $X-1, X+1 \notin \mathbb{Q}[X]^\times$. Folglich ist X^2-1 reduzibel. □

(12.34) Notation.

(a) Wir setzen

$$\mathbb{P} = \mathbb{P}_{\mathbb{Z}} := \{p \in \mathbb{Z} \mid p \text{ ist irreduzibel und positiv}\}.$$

(b) Es sei ein Körper K gegeben. Wir setzen

$$\mathbb{P}_{K[X]} := \{p \in K[X] \mid p \text{ ist irreduzibel und normiert}\}.$$

Für Polynome über Körpern von kleinem Grad gibt es einfache Irreduzibilitätskriterien:

(12.35) Bemerkung. Es sei ein Körper K gegeben.

(a) Jedes lineare Polynom über K ist irreduzibel.

(b) Jedes quadratische Polynom und jedes kubische Polynom über K ist genau dann irreduzibel, wenn es keine Nullstellen hat.

Beweis.

(a) Da jeder Teiler eines linearen Polynoms f über K den Grad 0 oder den Grad 1 hat, folgt die Irreduzibilität von f aus Bemerkung (12.32).

(b) Es sei $f \in K[X]$ mit $\deg f = 2$ oder $\deg f = 3$ gegeben. Nach Bemerkung (12.32) ist f genau dann irreduzibel, wenn jeder Teiler von f entweder invertierbar oder zu f assoziiert ist, also genau dann, wenn für jeden Teiler d von f entweder $\deg d = 0$ oder $\deg d = \deg f$ gilt. Nach Bemerkung (11.8)(b) ist dies aber dazu äquivalent, dass es keine Linearfaktoren von f gibt, nach Proposition (12.16) also dazu, dass f keine Nullstellen hat. □

Wir werden nun zeigen, dass sich von Null verschiedene Elemente von $\mathbb{Z}$ bzw. $K[X]$ für einen Körper K eindeutig in irreduzible Elemente zerlegen lassen, siehe Satz (12.37). Der wesentliche Schritt im Beweis ist folgende Aussage:

(12.36) Lemma. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $p \in R \setminus (\{0\} \dot\cup R^\times)$ gegeben. Genau dann ist p irreduzibel, wenn für $a, b \in R$ mit $p \mid ab$ stets auch $p \mid a$ oder $p \mid b$ gilt.

Beweis. Zunächst sei p irreduzibel und es seien $a, b \in R$ mit $p \mid ab$ gegeben. Ferner gelte $p \nmid a$ und damit insbesondere $a \neq 0$. Nach Bemerkung (12.32) ist $\gcd(p,a)$ als Teiler von p entweder invertierbar oder zu p assoziiert. Wegen $p \nmid a$ und $\gcd(p,a) \mid a$ ist $\gcd(p,a)$ aber nicht zu p assoziiert, also invertierbar. Nach Satz (12.25) ist daher $\operatorname{lcm}(p,a)$ assoziiert zu pa. Nun ist aber ab ein gemeinsames Vielfaches von p und a, also auch ein Vielfaches von $\operatorname{lcm}(p,a)$ und damit von pa. Da $a \neq 0$ ist, folgt $p \mid b$ nach Proposition (12.10).
Nun gelte umgekehrt für $a, b \in R$ mit $p \mid ab$ stets $p \mid a$ oder $p \mid b$. Ferner seien $x, y \in R$ mit $p = xy$ gegeben. Dann gilt insbesondere $p \mid p = xy$ nach Proposition (12.8), also $p \mid x$ oder $p \mid y$. Da wegen $p = xy$ aber auch $x \mid p$ und $y \mid p$ gilt, ist p assoziiert zu x oder zu y, nach Proposition (12.13) gibt es also ein $u \in R^\times$ mit $p = ux$ oder $p = uy$. Da R ein Integritätsbereich ist, folgt $y = u \in R^\times$ oder $x = u \in R^\times$ und damit die Irreduzibilität von p. □

(12.37) Satz. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Für jedes $a \in R \setminus \{0\}$ gibt es genau ein $u \in R^\times$ und genau ein $k \in \mathbb{N}_0^{(\mathbb{P}_R)}$ mit

$$a = u \prod_{p \in \mathbb{P}_R} p^{k_p}.$$

Im Fall $R = \mathbb{Z}$ ist u das Vorzeichen und im Fall $R = K[X]$ für einen Körper K ist u der Leitkoeffizient von a.

Beweis. Um zu zeigen, dass es für jedes $a \in R \setminus \{0\}$ ein $u \in R^\times$ und ein $k \in \mathbb{N}_0^{(\mathbb{P}_R)}$ mit $a = u \prod_{p \in \mathbb{P}_R} p^{k_p}$ gibt, führen wir Induktion nach $|a|$ im Fall $R = \mathbb{Z}$ bzw. nach $\deg a$ im Fall $R = K[X]$ für einen Körper K.
Für $|a| = 1$ im Fall $R = \mathbb{Z}$ bzw. für $\deg a = 0$ im Fall $R = K[X]$ gilt $a \in R^\times$ und damit $a = a \prod_{p \in \mathbb{P}_R} p^0$.
Es sei also ein $a \in R \setminus \{0\}$ mit $|a| > 1$ im Fall $R = \mathbb{Z}$ bzw. mit $\deg a > 0$ im Fall $R = K[X]$ gegeben und es sei angenommen, dass es für jedes $b \in R \setminus \{0\}$ mit $|b| < |a|$ im Fall $R = \mathbb{Z}$ bzw. mit $\deg b < \deg a$ im Fall $R = K[X]$ ein $v \in R^\times$ und ein $l \in \mathbb{N}_0^{(\mathbb{P}_R)}$ mit $b = v \prod_{p \in \mathbb{P}_R} p^{l_p}$ gibt. Wenn a irreduzibel ist, so gibt es ein $u \in R^\times$ und ein $q \in \mathbb{P}_R$ mit

$$a = uq = u \prod_{p \in \mathbb{P}} p^{\delta_{p,q}}.$$

Andernfalls ist a reduzibel, es gibt also $b, c \in R \setminus (\{0\} \dot\cup R^\times)$ mit $a = bc$. Im Fall $R = \mathbb{Z}$ ist dann aber $|b| < |a|$ und $|c| < |a|$, und im Fall $R = K[X]$ ist $\deg b < \deg a$ und $\deg c < \deg a$. Nach Induktionsvoraussetzung gibt es daher $v, w \in R^\times$ und $l, m \in \mathbb{N}_0^{(\mathbb{P}_R)}$ mit $b = v \prod_{p \in \mathbb{P}_R} p^{l_p}$ und $c = w \prod_{p \in \mathbb{P}_R} p^{m_p}$. Es folgt

$$a = bc = v \prod_{p \in \mathbb{P}_R} p^{l_p}\, w \prod_{p \in \mathbb{P}_R} p^{m_p} = vw \prod_{p \in \mathbb{P}_R} p^{l_p + m_p}.$$

Nach dem Induktionsprinzip gibt es für jedes $a \in R \setminus \{0\}$ ein $u \in R^\times$ und ein $k \in \mathbb{N}_0^{(\mathbb{P}_R)}$ mit $a = u \prod_{p \in \mathbb{P}_R} p^{k_p}$.
Zum Nachweis der Eindeutigkeit seien zunächst $u, v \in R^\times$, $k, l \in \mathbb{N}_0^{(\mathbb{P}_R)}$ mit $u \prod_{p \in \mathbb{P}_R} p^{k_p} = v \prod_{p \in \mathbb{P}_R} p^{l_p}$ gegeben. Im Fall $R = \mathbb{Z}$ sind $\prod_{p \in \mathbb{P}_R} p^{k_p}$ und $\prod_{p \in \mathbb{P}_R} p^{l_p}$ positiv und damit

$$u = \operatorname{sgn}(u \prod_{p \in \mathbb{P}_R} p^{k_p}) = \operatorname{sgn}(v \prod_{p \in \mathbb{P}_R} p^{l_p}) = v.$$

Im Fall $R = K[X]$ für einen Körper K sind $\prod_{p \in \mathbb{P}_R} p^{k_p}$ und $\prod_{p \in \mathbb{P}_R} p^{l_p}$ normiert und damit

$$u = \operatorname{lc}(u \prod_{p \in \mathbb{P}_R} p^{k_p}) = \operatorname{lc}(v \prod_{p \in \mathbb{P}_R} p^{l_p}) = v.$$

In jedem Fall gilt $u = v$ und damit $\prod_{p \in \mathbb{P}_R} p^{k_p} = \prod_{p \in \mathbb{P}_R} p^{l_p}$.
Um zu zeigen, dass für $k, l \in \mathbb{N}_0^{(\mathbb{P}_R)}$ mit $\prod_{p \in \mathbb{P}_R} p^{k_p} = \prod_{p \in \mathbb{P}_R} p^{l_p}$ stets $k = l$ folgt, führen wir Induktion nach $\sum_{p \in \mathbb{P}_R} k_p$. Es seien $k, l \in \mathbb{N}_0^{(\mathbb{P}_R)}$ mit $\prod_{p \in \mathbb{P}_R} p^{k_p} = \prod_{p \in \mathbb{P}_R} p^{l_p}$ und $\sum_{p \in \mathbb{P}_R} k_p = 0$ gegeben. Dann gilt notwendigerweise $k_p = 0$ für alle $p \in \mathbb{P}_R$, also $\prod_{p \in \mathbb{P}_R} p^{l_p} = \prod_{p \in \mathbb{P}_R} p^{k_p} = 1$. Da irreduzible Elemente keine Einheiten sind, impliziert dies aber bereits $l_p = 0$ für alle $p \in \mathbb{P}_R$. Folglich ist $k = l$.
Nun seien $k, l \in \mathbb{N}_0^{(\mathbb{P}_R)}$ mit $\prod_{p \in \mathbb{P}_R} p^{k_p} = \prod_{p \in \mathbb{P}_R} p^{l_p}$ gegeben und $\sum_{p \in \mathbb{P}_R} k_p > 0$ gegeben und für $k', l' \in \mathbb{N}_0^{(\mathbb{P}_R)}$ mit $\prod_{p \in \mathbb{P}_R} p^{k'_p} = \prod_{p \in \mathbb{P}_R} p^{l'_p}$ und $\sum_{p \in \mathbb{P}_R} k'_p < \sum_{p \in \mathbb{P}_R} k_p$ gelte $k' = l'$. Ferner sei $q \in \mathbb{P}_R$ gegeben. Nach Lemma (12.36) gilt genau dann $q \mid \prod_{p \in \mathbb{P}_R} p^{k_p}$, wenn $k_q > 0$ ist. Entsprechend gilt genau dann $q \mid \prod_{p \in \mathbb{P}_R} p^{l_p}$, wenn $l_q > 0$ ist. Wenn nun $k_q = 0$ ist, so folgt $q \nmid \prod_{p \in \mathbb{P}_R} p^{k_p} = \prod_{p \in \mathbb{P}_R} p^{l_p}$, also $l_q = 0 = k_q$. Es sei also im Folgenden $k_q > 0$, so dass $q \mid \prod_{p \in \mathbb{P}_R} p^{k_p} = \prod_{p \in \mathbb{P}_R} p^{l_p}$ und damit auch $l_q > 0$ folgt. Dies impliziert jedoch $q^{k_q - 1} \prod_{p \in \mathbb{P}_R \setminus \{q\}} p^{k_p} = q^{l_q - 1} \prod_{p \in \mathbb{P}_R \setminus \{q\}} p^{l_p}$. Nach Induktionsvoraussetzung gilt $k_q - 1 = l_q - 1$ sowie $k_p = l_p$ für alle $p \in \mathbb{P}_R \setminus \{q\}$, also $k_p = l_p$ für alle $p \in \mathbb{P}_R$. □

(12.38) Beispiel.

(a) In $\mathbb{Z}$ gilt

$$-18 = (-1) \cdot 2 \cdot 3^2.$$

(b) In $\mathbb{Q}[X]$ gilt

$$2X^2 - 2 = 2(X-1)(X+1).$$

(12.39) Definition (p-adische Bewertung)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a \in R \setminus \{0\}$ und $k \in \mathbb{N}_0^{(\mathbb{P}_R)}$ derart gegeben, dass es ein $u \in R^\times$ mit $a = u \prod_{p \in \mathbb{P}_R} p^{k_p}$ gibt. Für $p \in \mathbb{P}_R$ heißt

$$\mathrm{v}_p(a) := k_p$$

die *p-adische Bewertung* von a.

(12.40) Beispiel.

(a) Es ist

$$\mathrm{v}_p(-18) = \begin{cases} 1, & \text{für } p = 2, \\ 2, & \text{für } p = 3, \\ 0, & \text{für } p \in \mathbb{P} \setminus \{2,3\}. \end{cases}$$

(b) Es sei $f \in \mathbb{Q}[X]$ gegeben durch $f = 2X^2 - 2$. Dann ist

$$\mathrm{v}_p(f) = \begin{cases} 1, & \text{für } p \in \{X-1, X+1\}, \\ 0, & \text{für } p \in \mathbb{P}_{\mathbb{Q}[X]} \setminus \{X-1, X+1\}. \end{cases}$$

Beweis.

(a) Es gilt $-18 = (-1) \cdot 2 \cdot 3^2$. Folglich ist $\mathrm{sgn}(-18) = -1$, $\mathrm{v}_2(-18) = 1$, $\mathrm{v}_3(-18) = 2$ und $\mathrm{v}_p(-18) = 0$ für $p \in \mathbb{P} \setminus \{2,3\}$.

(b) Es gilt $f = 2X^2 - 2 = 2(X-1)(X+1)$. Folglich ist $\mathrm{lc}(f) = 2$, $\mathrm{v}_{X-1}(f) = 1$, $\mathrm{v}_{X+1}(f) = 1$ und $\mathrm{v}_p(f) = 0$ für $p \in \mathbb{P}_{\mathbb{Q}[X]} \setminus \{X-1, X+1\}$. □

(12.41) Bemerkung. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a \in R \setminus \{0\}$ gegeben. Für $p \in \mathbb{P}_R$ ist

$$\mathrm{v}_p(a) = \max\{k \in \mathbb{N}_0 \mid a \text{ ist ein Vielfaches von } p^k\}.$$

Vielfachheiten von Nullstellen von Polynomen

Da lineare Polynome nach Bemerkung (12.35)(a) stets irreduzibel sind und Linearfaktoren eines Polynoms den Nullstellen des Polynoms entsprechen, liefert der Bewertungsbegriff aus Definition (12.39) einen Begriff für Nullstellen:

(12.42) Definition (Vielfachheit einer Nullstelle)**.** Es seien ein Körper K und ein $f \in K[X] \setminus \{0\}$ gegeben. Für $a \in K$ heißt

$$\mathrm{m}_a(f) := \mathrm{v}_{X-a}(f)$$

die *Vielfachheit* (oder *Multiplizität*) von a als Nullstelle von f.

(12.43) Beispiel. Es sei $f \in \mathbb{Q}[X]$ gegeben durch $f = 2X^2 - 2$. Dann ist

$$\mathrm{m}_a(f) = \begin{cases} 1, & \text{für } a \in \{1,-1\}, \\ 0, & \text{für } a \in \mathbb{Q} \setminus \{-1,1\}. \end{cases}$$

Beweis. Nach Beispiel (12.40)(b) ist

$$\mathrm{m}_a(f) = \mathrm{v}_{X-a}(f) = \begin{cases} 1, & \text{für } a \in \{1,-1\}, \\ 0, & \text{für } a \in \mathbb{Q} \setminus \{-1,1\}. \end{cases}$$ □

(12.44) Bemerkung. Es seien ein Körper K und ein $f \in K[X] \setminus \{0\}$ gegeben. Für $a \in K$ ist

$$\mathrm{m}_a(f) = \max\{k \in \mathbb{N}_0 \mid f \text{ ist ein Vielfaches von } (X-a)^k\}.$$

(12.45) Bemerkung. Es seien ein Körper K und $f \in K[X] \setminus \{0\}$, $a \in K$ gegeben. Genau dann ist a eine Nullstelle von f, wenn $\mathrm{m}_a(f) \geq 1$ ist.

Beweis. Nach Proposition (12.16) ist a genau dann eine Nullstelle von f, wenn $X - a$ ein Linearfaktor von f ist. Dies ist aber dazu äquivalent, dass $\mathrm{m}_a(f) = \mathrm{v}_{X-a}(f) \geq 1$ ist. □

(12.46) Definition (Zerfällung in Linearfaktoren)**.** Es seien ein Körper K und ein $f \in K[X] \setminus \{0\}$ gegeben. Wir sagen, dass f in *Linearfaktoren zerfällt*, falls $\mathrm{v}_p(f) = 0$ für alle nicht linearen $p \in \mathbb{P}_{K[X]}$ ist.

(12.47) Beispiel.

(a) Es sei ein Körper K gegeben. Das Polynom $X^2 - 1$ über K zerfällt in Linearfaktoren.

(b) Das Polynom $X^2 + 1$ über $\mathbb{Q}$ zerfällt nicht in Linearfaktoren.

Beweis.

(a) Es gilt $X^2 - 1 = (X-1)(X+1)$ in $K[X]$.

(b) Nach Beispiel (12.33)(b) ist $X^2 + 1$ irreduzibel über $\mathbb{Q}$. □

(12.48) Bemerkung. Es seien ein Körper K und ein $f \in K[X] \setminus \{0\}$ gegeben. Dann ist

$$\sum_{a \in K} \mathrm{m}_a(f) \leq \deg f.$$

Genau dann gilt

$$\sum_{a \in K} \mathrm{m}_a(f) = \deg f,$$

wenn f in Linearfaktoren zerfällt.

Beweis. Es gilt

$$\prod_{a \in K} (X-a)^{\mathrm{m}_a(f)} = \prod_{a \in K} (X-a)^{\mathrm{v}_{X-a}(f)} \mid \mathrm{lc}(f) \prod_{p \in \mathbb{P}_R} p^{\mathrm{v}_p(f)} = f,$$

nach Bemerkung (11.8)(b) also

$$\deg f \geq \deg \prod_{a \in K} (X-a)^{\mathrm{m}_a(f)} = \sum_{a \in K} \mathrm{m}_a(f) \deg(X-a) = \sum_{a \in K} \mathrm{m}_a(f).$$

Genau dann gilt $\deg f = \sum_{a \in K} \mathrm{m}_a(f)$, wenn $\prod_{a \in K} (X-a)^{\mathrm{v}_{X-a}(f)} = \prod_{p \in \mathbb{P}_R} p^{\mathrm{v}_p(f)}$ ist, d.h. wenn f in Linearfaktoren zerfällt. □

(12.49) Proposition. Es sei ein Körper K gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Der Körper K ist algebraisch abgeschlossen.

(b) Die irreduziblen Polynome über K sind genau die linearen Polynome über K.

(c) Jedes von 0 verschiedene Polynom über K zerfällt in Linearfaktoren.

Beweis. Zunächst gelte Bedingung (a), d.h. K sei algebraisch abgeschlossen. Um Bedingung (b) zu zeigen, sei zunächst ein irreduzibles Polynom f über K gegeben. Dann ist f nicht konstant und hat demnach eine Nullstelle in K, d.h. es gibt ein $a \in K$ mit $f(a) = 0$. Nach Proposition (12.16) ist $X - a$ ein Linearfaktor von f. Da f irreduzibel ist, folgt $f = b \cdot (X-a) = bX - a$ für ein $b \in K[X]^\times = K^\times$. Insbesondere ist f linear. Nach Bemerkung (12.35)(a) sind umgekehrt alle linearen Polynome auch irreduzibel. Folglich gilt Bedingung (b).

Als nächstes gelte Bedingung (b), d.h. die irreduziblen Polynome über K seien genau die linearen Polynome über K. Nach Satz (12.37) zerfällt dann jedes von 0 verschiedene Polynom über K in Linearfaktoren, d.h. es gilt Bedingung (c).
Schließlich gelte Bedingung (c), d.h. jedes $f \in K[X] \setminus \{0\}$ zerfalle in Linearfaktoren. Um zu zeigen, dass K algebraisch abgeschlossen ist, sei ein nicht konstantes Polynom f über K gegeben. Nach Annahme zerfällt f in Linearfaktoren, es gilt also $\sum_{a \in K} \mathrm{m}_a(f) = \deg f$ nach Bemerkung (12.48). Wegen $\deg f \geq 1$ gibt es daher ein $a \in K$ mit $\mathrm{m}_a(f) \geq 1$, nach Bemerkung (12.45) also so, dass a eine Nullstelle von f ist. Folglich ist K algebraisch abgeschlossen, d.h. Bedingung (a) gilt.
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

13 Kongruenzen und Restklassenringe

In diesem Abschnitt wollen wir eine ganze Serie von neuen Ringen konstruieren, sogenannte Restklassenringe. Hierzu betrachten wir Äquivalenzrelationen auf dem Ring der ganzen Zahlen $\mathbb{Z}$ bzw. auf dem Polynomring $K[X]$ für einen Körper K, welche verträglich mit der jeweiligen Ringstruktur sind, und dadurch die Definition einer Ringstruktur auf der jeweiligen Quotientenmenge zulassen. Einige dieser Restklassenringe werden de facto Körper sein, und wir werden ein Kriterium herleiten, welches diesen Fall charakterisiert.

Kongruenzen

Wir beginnen mit der Einführung gewisser Äquivalenzrelationen auf $\mathbb{Z}$ bzw. auf $K[X]$ für einen Körper K.

(13.1) Definition (Kongruenz)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $m \in R$ gegeben. Für $a, b \in R$ sagen wir, dass a *kongruent* b modulo m ist, geschrieben $a \equiv_m b$, wenn $m \mid a - b$ gilt, und sonst, dass a *inkongruent* b modulo m ist, geschrieben $a \not\equiv_m b$.

(13.2) Beispiel.

(a) In $\mathbb{Z}$ ist $7 \equiv_7 0$, $1 \equiv_7 8$, $1 \equiv_7 -6$, $3 \equiv_7 10$, $2 \equiv_7 9$, $2 \equiv_7 16$, $2 \equiv_7 -5$, $16 \equiv_7 -5$.

(b) In $\mathbb{Q}[X]$ ist $X^2 - 1 \equiv_{X^2-1} 0$, $X^2 \equiv_{X^2-1} 1$, $X^4 - X^2 + 1 \equiv_{X^2-1} 1$.

Beweis.

(a) Es gilt $7 \mid 7 = 7 - 0$, also $7 \equiv_7 0$. Es gilt $7 \mid -7 = 1 - 8$, also $1 \equiv_7 8$. Es gilt $7 \mid -7 = 3 - 10$, also $3 \equiv_7 10$. Es gilt $7 \mid 7 = 1 - (-6)$, also $1 \equiv_7 -6$. Es gilt $7 \mid -7 = 2 - 9$, also $2 \equiv_7 9$. Es gilt $7 \mid -14 = 2 - 16$, also $2 \equiv_7 16$. Es gilt $7 \mid 7 = 2 - (-5)$, also $2 \equiv_7 -5$. Es gilt $7 \mid 21 = 16 - (-5)$, also $16 \equiv_7 -5$.

(b) Es gilt $X^2 - 1 \mid X^2 - 1 = X^2 - 1 - 0$, also $X^2 - 1 \equiv_{X^2-1} 0$. Es gilt $X^2 - 1 \mid X^2 - 1$, also $X^2 \equiv_{X^2-1} 1$. Es gilt $X^2 - 1 \mid X^4 - X^2 = X^4 - X^2 + 1 - 1$, also $X^4 - X^2 + 1 \equiv_{X^2-1} 1$. □

Wir beginnen mit dem Nachweis, dass Kongruenz modulo einem Element eine Äquivalenzrelation ist.

(13.3) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $m \in R$ gegeben. Dann ist $\equiv_m$ eine Äquivalenzrelation auf R.

Beweis. Es seien $a, b, c \in R$ mit $a \equiv_m b$ und $b \equiv_m c$ gegeben, so dass $m \mid a - b$ und $m \mid b - c$ gilt. Dann gilt jedoch auch $m \mid (a - b) + (b - c) = a - c$ nach Proposition (12.9)(a), d.h. $a \equiv_m c$. Folglich ist $\equiv_m$ transitiv.
Für alle $a \in R$ gilt $m \mid 0 = a - a$ nach Proposition (12.9)(b), also $a \equiv_m a$. Folglich ist $\equiv_m$ reflexiv.
Es seien $a, b \in R$ mit $a \equiv_m b$ gegeben, so dass $m \mid a - b$ gilt. Dann gilt auch $m \mid b - a = -(a - b)$ nach Proposition (12.9)(c), d.h. $b \equiv_m a$. Folglich ist $\equiv_m$ symmetrisch.
Insgesamt ist $\equiv_m$ eine Äquivalenzrelation auf R. □

Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $m \in R$ gegeben. Da $\equiv_m$ nach Proposition (13.3) eine Äquivalenzrelation ist, können wir die Quotientenmenge $R/\equiv_m = \{[x] \mid x \in R\}$ betrachten.

(13.4) Beispiel.

(a) In $\mathbb{Z}/\equiv_7$ ist $[7] = [0]$, $[1] = [8] = [-6]$, $[3] = [10]$, $[2] = [9] = [16] = [-5]$.

(b) In $\mathbb{Q}[X]/\equiv_{X^2-1}$ ist $[X^2 - 1] = [0]$, $[X^2] = [1]$, $[X^4 - X^2 + 1] = [1]$.

Beweis.

(a) Dies folgt aus Beispiel (13.2)(a).

(b) Dies folgt aus Beispiel (13.2)(b). □

Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $m \in R$ gegeben. Wir wollen auf $R/\equiv_m$ eine Ringstruktur konstruieren, und zwar so, dass wir repräsentantenweise rechnen können. Für die Addition wollen wir also etwa, dass in $R/\equiv_m$ die Gleichung $[x] + [y] = [x + y]$ für $x, y \in R$ gilt. Analog für die Multiplikation. Um $[x] + [y] = [x + y]$ in $R/\equiv_m$ für $x, y \in R$ zu erreichen, muss für $(x, y), (\tilde{x}, \tilde{y}) \in R \times R$ mit $([x], [y]) = ([\tilde{x}], [\tilde{y}])$ in $R/\equiv_m \times R/\equiv_m$ stets $[x + y] = [\tilde{x} + \tilde{y}]$ in $R/\equiv_m$ gelten. Nun ist aber genau dann $[x] = [\tilde{x}]$ in $R/\equiv_m$, wenn $x \equiv_m \tilde{x}$ gilt, es ist genau dann $[y] = [\tilde{y}]$ in $R/\equiv_m$, wenn $y \equiv_m \tilde{y}$ gilt, und es ist genau dann $[x+y] = [\tilde{x}+\tilde{y}]$ in $R/\equiv_m$, wenn $x+y \equiv_m \tilde{x}+\tilde{y}$ gilt. Folglich muss notwendigerweise aus $x \equiv_m \tilde{x}$ und $y \equiv_m \tilde{y}$ stets $x+y \equiv_m \tilde{x}+\tilde{y}$ folgen. Analog für die Multiplikation.

(13.5) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $m \in R$ gegeben. Für $a, \tilde{a}, b, \tilde{b} \in R$ mit $a \equiv_m \tilde{a}$ und $b \equiv_m \tilde{b}$ gilt auch $a + b \equiv_m \tilde{a} + \tilde{b}$ und $ab \equiv_m \tilde{a}\tilde{b}$.

Beweis. Es seien $a, \tilde{a}, b, \tilde{b} \in R$ mit $a \equiv_m \tilde{a}$ und $b \equiv_m \tilde{b}$ gegeben, so dass $m \mid a - \tilde{a}$ und $m \mid b - \tilde{b}$ gilt. Nach Proposition (12.9)(a), (c) gilt dann auch

$$m \mid (a - \tilde{a}) + (b - \tilde{b}) = (a + b) - (\tilde{a} + \tilde{b}),$$
$$m \mid (a - \tilde{a})b + \tilde{a}(b - \tilde{b}) = ab - \tilde{a}b + \tilde{a}b - \tilde{a}\tilde{b} = ab - \tilde{a}\tilde{b},$$

also $a + b \equiv_m \tilde{a} + \tilde{b}$ und $ab \equiv_m \tilde{a}\tilde{b}$. □

Proposition (13.5) lässt sich benutzen, um Polynome bzgl. Kongruenz zu „reduzieren“ und so einfachere Repräsentanten der zugehörigen Äquivalenzklasse zu berechnen:

(13.6) Beispiel. In $\mathbb{Q}[X]$ ist

$$X^5 - 3X^4 + 2X^3 - X^2 + 2 \equiv_{X^2-1} 3X - 2$$

und in $\mathbb{Q}[X]/\equiv_{X^2-1}$ ist

$$[X^5 - 3X^4 + 2X^3 - X^2 + 2] = [3X - 2].$$

Beweis. In $\mathbb{Q}[X]$ ist $X^2 \equiv_{X^2-1} 1$, also

$$X^3 = X \cdot X^2 \equiv_{X^2-1} X \cdot 1 = X,$$
$$X^4 = X \cdot X^3 \equiv_{X^2-1} X \cdot X = X^2 \equiv_{X^2-1} 1,$$
$$X^5 = X \cdot X^4 \equiv_{X^2-1} X \cdot 1 = X$$

und damit

$$X^5 - 3X^4 + 2X^3 - X^2 + 2 \equiv_{X^2-1} X - 3 \cdot 1 + 2X - 1 + 2 = 3X - 2.$$

Folglich gilt $[X^5 - 3X^4 + 2X^3 - X^2 + 2] = [3X - 2]$ in $\mathbb{Q}[X]/\equiv_{X^2-1}$. □

Konstruktion der Restklassenringe

Da wir nach Proposition (13.5) wissen, dass Kongruenzrelationen im Sinne von Definition (13.1) mit der Addition und der Multiplikation auf $\mathbb{Z}$ bzw. auf $K[X]$ für einen Körper K verträglich sind, können wir nun eine Ringstruktur auf der Quotientenmenge konstruieren:

(13.7) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $m \in R$ gegeben. Die Menge $R/\equiv_m$ wird ein kommutativer Ring mit Addition und Multiplikation gegeben durch

$$[x] +^{R/\equiv_m} [y] = [x +^R y],$$
$$[x] \cdot^{R/\equiv_m} [y] = [x \cdot^R y]$$

für $x, y \in R$. Die Null und die Eins von $R/\equiv_m$ sind gegeben durch

$$0^{R/\equiv_m} = [0^R],$$
$$1^{R/\equiv_m} = [1^R].$$

Für $x \in R$ ist das Negative von $[x]$ in $R/\equiv_m$ gegeben durch

$$(-[x])^{R/\equiv_m} = [(-x)^R].$$

Beweis. Um zu zeigen, dass die beschriebene Addition und die beschriebene Multiplikation wohldefiniert sind, seien $x, \tilde{x}, y, \tilde{y} \in R$ mit $[x] = [\tilde{x}]$ und $[y] = [\tilde{y}]$ gegeben. Dann gilt $x \equiv_m \tilde{x}$ und $y \equiv_m \tilde{y}$, also auch $x + y \equiv_m \tilde{x} + \tilde{y}$ und $xy \equiv_m \tilde{x}\tilde{y}$ nach Proposition (13.5) und damit $[x + y] = [\tilde{x} + \tilde{y}]$ und $[xy] = [\tilde{x}\tilde{y}]$ in $R/\equiv_m$.
Somit erhalten wir wohldefinierte Verknüpfungen

$$+\colon R/\equiv_m \times R/\equiv_m \to R/\equiv_m,\ ([x],[y]) \mapsto [x +^R y],$$
$$\cdot\colon R/\equiv_m \times R/\equiv_m \to R/\equiv_m,\ ([x],[y]) \mapsto [x \cdot^R y].$$

Wir wollen zeigen, dass $R/\equiv_m$ ein kommutativer Ring mit Addition $+$ und Multiplikation $\cdot$ wird. Hierzu verifizieren wir die Ringaxiome.

- *Assoziativität der Addition.* Für $x, y, z \in R$ gilt

  $$[x] + ([y] + [z]) = [x] + [y + z] = [x + (y + z)] = [(x + y) + z] = [x + y] + [z] = ([x] + [y]) + [z].$$

  Folglich ist $+$ assoziativ.

- *Kommutativität der Addition.* Für $x, y \in R$ gilt

  $$[x] + [y] = [x + y] = [y + x] = [y] + [x].$$

  Folglich ist $+$ kommutativ.

- *Existenz der Null.* Für $x \in R$ gilt

  $$[0] + [x] = [0 + x] = [x].$$

  Wegen der Kommutativität von $+$ ist $[0]$ ein neutrales Element in $R/\equiv_m$ bzgl. $+$.

- *Existenz der Negativen.* Für $x \in R$ gilt

  $$[-x] + [x] = [(-x) + x] = [0].$$

  Wegen der Kommutativität von $+$ ist $[-x]$ ein zu $[x]$ inverses Element bzgl. $+$.

- *Assoziativität der Multiplikation.* Für $x, y, z \in R$ gilt

  $$[x]([y][z]) = [x][yz] = [x(yz)] = [(xy)z] = [xy][z] = ([x][y])[z].$$

  Folglich ist $\cdot$ assoziativ.

- *Kommutativität der Multiplikation.* Für $x, y \in R$ gilt

  $$[x][y] = [xy] = [yx] = [y][x].$$

  Folglich ist $\cdot$ kommutativ.

- *Existenz der Eins.* Für $x \in R$ gilt

  $$[1][x] = [1x] = [x].$$

  Wegen der Kommutativität von $\cdot$ ist $[1]$ ein neutrales Element in $R/\equiv_m$ bzgl. $\cdot$.

- *Distributivität.* Für $x, y, z \in R$ gilt

$$[x]([y]+[z]) = [x][y+z] = [x(y+z)] = [xy+xz] = [xy]+[xz] = [x][y]+[x][z],$$
$$([x]+[y])[z] = [x+y][z] = [(x+y)z] = [xz+yz] = [xz]+[yz] = [x][z]+[y][z].$$

Insgesamt wird $R/\equiv_m$ ein kommutativer Ring mit Addition und Multiplikation gegeben durch $[x]+[y] = [x+y]$ und $[x][y] = [xy]$ für $x, y \in R$, Null $0 = [0]$, Eins $1 = [1]$ und Negativen $-[x] = [-x]$ für $x \in R$. □

(13.8) Definition (Restklassenring)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $m \in R$ gegeben. Der kommutative Ring $R/m := R/\equiv_m$ mit Addition und Multiplikation gegeben wie in Proposition (13.7) heißt *Restklassenring* von R modulo m. Für $x \in R$ wird die Äquivalenzklasse $[x]_m := [x]_{\equiv_m}$ auch die *Restklasse* von x modulo m genannt.

Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $m \in R$ gegeben. Der Restklassenring R/m wird in der Literatur oft auch als $R/mR = R/Rm$ oder als $R/(m)$ bezeichnet und über die Menge der Vielfachen $(m) = mR = Rm = \{qm \mid q \in R\}$ konstruiert.

(13.9) Beispiel.

(a) In $\mathbb{Z}/7$ ist $[5]+[4] = [2]$, $[3]\cdot[4] = [5]$, $[13]\cdot[13] = [1]$.

(b) In $\mathbb{Q}[X]/(X^2-1)$ ist $[X^5-X^3-3][X^4-X^2+2] = -[6]$ und $[X-1][X+1] = [0]$.

Beweis.

(a) In $\mathbb{Z}/7$ ist

$$[5]+[4] = [9] = [2],$$
$$[3]\cdot[4] = [12] = [5],$$
$$[13]\cdot[13] = [-1]\cdot[-1] = [1].$$

(b) In $\mathbb{Q}[X]/(X^2-1)$ ist

$$[X^5-X^3-3][X^4-X^2+2] = [-3][2] = [-6] = -[6],$$
$$[X-1][X+1] = [X^2-1] = [0].$$ □

Es sei ein Ring R gegeben. Nach Notation (9.15) schreiben wir $k = k^R = k \cdot 1^R$ für $k \in \mathbb{Z}$. Es ist also etwa $2^R = 2 \cdot 1^R = 1^R + 1^R$, $3^R = 3 \cdot 1^R = 1^R + 1^R + 1^R$, usw. in R.
In Restklassenringen von $\mathbb{Z}$ erhalten wir folgenden Zusammenhang:

(13.10) Bemerkung. Es sei $n \in \mathbb{Z}$ gegeben. Für $k \in \mathbb{Z}$ gilt

$$k^{\mathbb{Z}/n} = [k^{\mathbb{Z}}].$$

Beweis. Für $k \in \mathbb{N}_0$ gilt

$$k^{\mathbb{Z}/n} = k \cdot 1^{\mathbb{Z}/n} = \sum_{i\in[1,k]} 1^{\mathbb{Z}/n} = \sum_{i\in[1,k]} [1^{\mathbb{Z}}] = [\sum_{i\in[1,k]} 1^{\mathbb{Z}}] = [k^{\mathbb{Z}}]$$

und

$$(-k)^{\mathbb{Z}/n} = -k^{\mathbb{Z}/n} = -[k^{\mathbb{Z}}] = [-k^{\mathbb{Z}}].$$ □

Es sei $n \in \mathbb{Z}$ gegeben. Im Folgenden schreiben wir für $x \in \mathbb{Z}$ daher unter Missbrauch der Notation manchmal kurz x statt $[x]_n$ für die Restklasse von x modulo n, und sagen dann immer dazu, sobald x als Element von $\mathbb{Z}/n$ anzusehen ist. Für $x, y \in \mathbb{Z}$ gilt also genau dann $x = y$ in $\mathbb{Z}/n$, wenn $x \equiv_n y$ in $\mathbb{Z}$ gilt.
Im Fall von Restklassenringen kann man K in $K[X]/f$ wie folgt „einbetten“:

(13.11) Proposition. Es seien ein Körper K und $f \in K[X]$ gegeben. Ferner sei

$$\iota\colon K \to K[X]/f,\ a \mapsto [a].$$

Dann gilt:

- *Verträglichkeit mit den Additionen.* Für $a, a' \in K$ ist $\iota(a + a') = \iota(a) + \iota(a')$.
- *Verträglichkeit der Nullen.* Es ist $\iota(0) = 0$.
- *Verträglichkeit der Negative.* Für $a \in K$ ist $\iota(-a) = -\iota(a)$.
- *Verträglichkeit mit den Multiplikationen.* Für $a, a' \in K$ ist $\iota(aa') = \iota(a)\,\iota(a')$.
- *Verträglichkeit der Einselemente.* Es ist $\iota(1) = 1$.
- *Verträglichkeit der Inversen.* Für $a \in K^\times$ ist $\iota(a) \in (K[X]/f)^\times$ mit $\iota(a^{-1}) = (\iota(a))^{-1}$.

Genau dann ist ι injektiv, wenn $f \notin K^\times$ ist.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(13.12) Konvention. Es seien ein Körper K und $f \in K[X] \setminus K^\times$ gegeben. Von jetzt an identifizieren wir K mit dem Bild der injektiven Abbildung $\iota\colon K \to K[X]/f,\ a \mapsto [a]$ aus Proposition (13.11). Das heißt, unter Missbrauch der Notationen schreiben wir K anstatt $\operatorname{Im}\iota$, und für $a \in K$ notieren wir das Bild $\iota(a) = [a]$ von a auch als a.

Unter Benutzung von Konvention (13.12) sind die Elemente von $K[X]/f$ für einen Körper K und ein $f \in K[X]$ also wieder „polynomielle Ausdrücke“, nur diesmal in $[X]$ statt X: Für $a \in K^{(\mathbb{N}_0)}$ gilt

$$[\sum_{i\in\mathbb{N}_0} a_i X^i] = \sum_{i\in\mathbb{N}_0} [a_i X^i] = \sum_{i\in\mathbb{N}_0} [a_i]\,[X]^i = \sum_{i\in\mathbb{N}_0} a_i [X]^i.$$

Hierbei sind in $K[X]/f$ solche Ausdrücke gleich, für welche die entsprechenden Elemente in $K[X]$ kongruent modulo f sind. Insbesondere können unterschiedliche Elemente in $K[X]$, also unterschiedliche Polynome, gleiche Elemente in $K[X]/f$ induzieren.

(13.13) Beispiel.

(a) In $\mathbb{Z}/7$ ist $7 = 0$, $1 = 8 = -6$, $3 = 10$, $2 = 9 = 16 = -5$.

(b) In $\mathbb{Q}[X]/(X^2 - 1)$ ist $[X]^2 = [1]$, $[X]^4 - [X]^2 + 1 = 1$, $[X]^5 - 3[X]^4 + 2[X]^3 - [X]^2 + 2 = 3[X] - 2$.

Beweis.

(a) Dies folgt aus Beispiel (13.4)(a).

(b) Dies folgt aus Beispiel (13.4)(b) und Beispiel (13.6). □

In der nachfolgenden Bemerkung leiten wir eine konkrete Beschreibung der Äquivalenzklassen her. Zugleich betonen wir, dass die „Beschaffenheit“ der Äquivalenzklassen für das Rechnen im Quotientenring vollkommen irrelevant ist: da die Rechnung repräsentantenweise geschieht, genügt es, stets einen Repräsentanten zu kennen, ein Überblick über alle Elemente der Restklasse ist zum Rechnen nicht notwendig.

(13.14) Bemerkung. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $m \in R$ gegeben. Für $a \in R$ ist

$$[a]_m = a + Rm.$$

Beweis. Für $a \in R$ ist

$$[a] = \{\tilde{a} \in R \mid \tilde{a} \equiv_m a\} = \{\tilde{a} \in R \mid \text{es gibt ein } q \in R \text{ mit } \tilde{a} = qm + a\} = \{a + qm \mid q \in R\} = a + Rm. \quad \square$$

Kongruenzen und Division mit Rest

Die Bezeichnung Restklasse bzw. Restklassenring kommt daher, dass jedes Element im Restklassenring, also jede Restklasse modulo einem Element, durch den Rest eines beliebigen Repräsentanten bei Division mit Rest durch dieses Element repräsentiert wird, wie wir nun sehen werden.

(13.15) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $m \in R \setminus \{0\}$ gegeben.

(a) Für $a \in R$ ist $a \equiv_m a \bmod m$ in R und $[a] = [a \bmod m]$ in R/m.

(b) Es seien $a, b \in R$ gegeben. Die folgenden Aussagen sind äquivalent.

(i) Es ist $[a] = [b]$ in R/m.

(ii) Es ist $a \equiv_m b$ in R.

(iii) Es ist $a \bmod m = b \bmod m$ in R.

Beweis.

(a) Für $a \in R$ gilt $a = (a \operatorname{div} m)m + (a \bmod m)$ nach dem Satz über die Division mit Rest (12.2), also $a \equiv_m a \bmod m$ in R und damit $[a] = [a \bmod m]$ in R/m nach Proposition (5.7)(b).

(b) Zunächst sind Bedingung (i) und Bedingung (ii) äquivalent nach Proposition (5.7)(b). Somit genügt es, die Äquivalenz von Bedingung (ii) und Bedingung (iii) zu zeigen.

Nach (a) gilt $a \equiv_m a \bmod m$ sowie $b \equiv_m b \bmod m$. Folglich gilt genau dann $a \equiv_m b$, wenn $a \bmod m \equiv_m b \bmod m$ ist. Dies wiederum ist äquivalent zu $m \mid (a \bmod m) - (b \bmod m)$. Nach Definition (12.3) gilt $a \bmod m \in [0, |m| - 1]$ und $b \bmod m \in [0, |m| - 1]$ im Fall $R = \mathbb{Z}$ sowie $a \bmod m \in K[X]_{<\deg m}$ und $b \bmod m \in K[X]_{<\deg m}$ im Fall $R = K[X]$. In beiden Fällen ist $m \mid (a \bmod m) - (b \bmod m)$ gleichbedeutend mit $(a \bmod m) - (b \bmod m) = 0$, d.h. mit $a \bmod m = b \bmod m$. □

(13.16) Korollar.

(a) Es sei $n \in \mathbb{Z} \setminus \{0\}$ gegeben. Dann ist $[0, |n| - 1]$ eine Transversale von $\mathbb{Z}/n$. Insbesondere gilt

$$\mathbb{Z}/n = \{[r] \mid r \in [0, |n| - 1]\}.$$

(b) Es seien ein Körper K und $f \in K[X] \setminus \{0\}$ gegeben. Dann ist $K[X]_{<\deg f}$ eine Transversale von $K[X]/f$. Insbesondere gilt

$$K[X]/f = \{[r] \mid r \in K[X]_{<\deg f}\} = \{\sum_{i \in [0, \deg f - 1]} a_i [X]^i \mid a \in K^{[0, \deg f - 1]}\}.$$

Beweis.

(a) Für $x \in \mathbb{Z}$ ist $x \bmod n \in [0, |n| - 1]$. Nach Proposition (13.15)(a) gibt es somit für jedes $x \in \mathbb{Z}$ ein $r \in [0, |n| - 1]$ mit $[x] = [r]$, d.h. es gilt

$$\mathbb{Z}/n = \{[r] \mid r \in [0, |n| - 1]\}.$$

Ferner gilt für $r, r' \in [0, |n| - 1]$ nach Proposition (13.15)(b) genau dann $[r] = [r']$, wenn $r = r \bmod n = r' \bmod n = r'$ ist. Insgesamt ist $[0, |n| - 1]$ eine Transversale von $\mathbb{Z}/n$.

(b) Für $g \in K[X]$ ist $g \bmod f \in K[X]_{<\deg f}$. Nach Proposition (13.15)(a) gibt es somit für jedes $g \in K[X]$ ein $r \in K[X]_{<\deg f}$ mit $[g] = [r]$, d.h. es gilt

$$K[X]/f = \{[r] \mid r \in K[X]_{<\deg f}\} = \{\sum_{i \in [0, \deg f - 1]} a_i [X]^i \mid a \in K^{[0, \deg f - 1]}\}.$$

Ferner gilt für $r, r' \in K[X]_{<\deg f}$ nach Proposition (13.15)(b) genau dann $[r] = [r']$, wenn $r = r \bmod f = r' \bmod f = r'$ ist. Insgesamt ist $K[X]_{<\deg f}$ eine Transversale von $K[X]/f$. □

(13.17) Beispiel.

(a) Es ist

$$\mathbb{Z}/7 = \{[0], [1], [2], [3], [4], [5], [6]\} = \{0, 1, 2, 3, 4, 5, 6\}.$$

(b) Es ist

$$\mathbb{Q}[X]/(X^2 - 1) = \{a[X] + b \mid a, b \in \mathbb{Q}\}.$$

(13.18) Definition (Standardtransversale)**.**

(a) Für $n \in \mathbb{Z}\backslash\{0\}$ heißt $[0, |n|-1]$ die *Standardtransversale* (oder das *Standardrepräsentantensystem*) von $\mathbb{Z}/n$.

(b) Für $f \in K[X] \setminus \{0\}$ heißt $K[X]_{<\deg f}$ die *Standardtransversale* (oder das *Standardrepräsentantensystem*) von $K[X]/f$.

(13.19) Beispiel.

(a) Die Standardtransversale von $\mathbb{Z}/7$ ist $[0, 6] = \{0, 1, 2, 3, 4, 5, 6\}$.

(b) Die Standardtransversale von $\mathbb{Q}[X]/(X^2 - 1)$ ist $\mathbb{Q}[X]_{<2} = \{aX + b \mid a, b \in \mathbb{Q}\}$.

(13.20) Beispiel. Die Werte der Addition und Multiplikation von $\mathbb{Z}/4 = \{0, 1, 2, 3\}$ sind wie folgt gegeben.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Lineare Kongruenzgleichungen in einer Unbekannten

Als nächstes betrachten wir lineare Kongruenzgleichungen in einer Unbekannten:

(13.21) Satz (Lösbarkeitskriterium und Lösungsbestimmung für lineare Kongruenzgleichungen in einer Unbekannten)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $m, a, b \in R$ gegeben.

(a) Genau dann gibt es ein $x \in R$ mit $xa \equiv_m b$, wenn

$$\gcd(m, a) \mid b$$

gilt.

(b) Es seien $p, q, r \in R$ mit $m = p\gcd(m, a)$, $a = q\gcd(m, a)$ und $b = r\gcd(m, a)$ gegeben. Ferner sei $x' \in R$ mit $x'q \equiv_p 1$ gegeben. Dann ist

$$\begin{aligned}\{x \in R \mid xa \equiv_m b\} &= \left\{\begin{matrix} R, & \text{falls } (m, a) = (0, 0), \\ \{rx' + np \mid n \in R\}, & \text{falls } (m, a) \neq (0, 0) \end{matrix}\right\} \\ &= \begin{cases} R, & \text{falls } (m, a) = (0, 0), \\ rx' + Rp, & \text{falls } (m, a) \neq (0, 0). \end{cases}\end{aligned}$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(13.22) Beispiel.

(a) Es ist

$$\{x \in \mathbb{Z} \mid x \cdot 168 \equiv_{2238} -24\} = -160 + \mathbb{Z} \cdot 373.$$

(b) Es ist

$$\{x \in \mathbb{Z} \mid x \cdot 168 \equiv_{2238} 4\} = \emptyset.$$

Beweis. Nach Beispiel (12.28)(a) ist $\gcd(2238, 168) = 6 = (-3) \cdot 2238 + 40 \cdot 168 \equiv_{2238} 40 \cdot 168$.

(a) Wegen $2238 = 373 \cdot 6$, $168 = 28 \cdot 6$, $-24 = -4 \cdot 6$ und $1 = (-3) \cdot 373 + 40 \cdot 28 \equiv_{373} 40 \cdot 28$ gilt

$$\{x \in \mathbb{Z} \mid x \cdot 168 \equiv_{2238} -24\} = -160 + \mathbb{Z} \cdot 373$$

nach Satz (13.21).

(b) Wegen $6 \nmid 4$ gilt

$$\{x \in \mathbb{Z} \mid x \cdot 168 \equiv_{2238} 4\} = \emptyset$$

nach Satz (13.21)(a). □

Invertierbare Elemente

Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Per Konstruktion ist der Restklassenring R/m für $m \in R$ ein kommutativer Ring. Es stellt sich die Frage, für welche $m \in R$ dieser kommutative Ring ein Körper ist und, noch etwas allgemeiner, was im Allgemeinen die invertierbaren Elemente in R/m sind.
Wir beginnen mit einem Beispiel.

(13.23) Beispiel.

(a) In $\mathbb{Z}/30$ ist 17 invertierbar mit

$$17^{-1} = 23.$$

(b) In $\mathbb{Q}[X]/(X^2 - 1)$ ist $2 + [X]$ invertierbar mit

$$(2 + [X])^{-1} = \frac{2}{3} - \frac{1}{3}[X].$$

Beweis.

(a) Es ist

$$17 \cdot 23 = 391 = 1 + 13 \cdot 30 \equiv_{30} 1$$

in $\mathbb{Z}$ und damit $17 \cdot 23 = 1$ in $\mathbb{Z}/30$. Wegen der Kommutativität von $\mathbb{Z}/30$ ist folglich $17 \in (\mathbb{Z}/30)^\times$ mit $17^{-1} = 23$.

(b) Es ist

$$(2 + X)(\frac{2}{3} - \frac{1}{3}X) = \frac{4}{3} - \frac{2}{3}X + \frac{2}{3}X - \frac{1}{3}X^2 = \frac{4}{3} - \frac{1}{3}X^2 = 1 + \frac{1}{3}(1 - X^2) \equiv_{X^2-1} 1$$

in $\mathbb{Q}[X]$ und damit $(2+[X])(\frac{2}{3}-\frac{1}{3}[X]) = 1$ in $\mathbb{Q}[X]/(X^2-1)$. Wegen der Kommutativität von $\mathbb{Q}[X]/(X^2-1)$ ist folglich $2 + [X] \in (\mathbb{Q}[X]/(X^2 - 1))^\times$ mit $(2 + [X])^{-1} = \frac{2}{3} - \frac{1}{3}[X]$. □

Das vorangegangene Beispiel haben wir durch Verifikation der Invertierbarkeit anhand des inversen Elements im Restklassenring nachgewiesen, welches wir hierzu natürlich kennen mussten. Im Nachfolgenden wollen wir ein Kriterium herleiten, welches uns ermöglicht, Elemente eines Restklassenrings auf Invertierbarkeit zu testen und gegebenenfalls das Inverse zu berechnen.

(13.24) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $m \in R$ gegeben. Dann ist

$$(R/m)^\times = \{[a] \mid a \in R \text{ mit } \gcd(m, a) = 1\}.$$

Für $a, x, y \in R$ mit $xm + ya = \gcd(m, a) = 1$ ist $[a]^{-1} = [y]$ in R/m.

Beweis. Nach dem Lösbarkeitskriterium für Kongruenzgleichungen (13.21)(a) ist

$$\begin{aligned}(R/m)^\times &= \{[a] \mid a \in R \text{ so, dass es ein } y \in R \text{ mit } [y][a] = 1 \text{ in } R/m \text{ gibt}\}\\ &= \{[a] \mid a \in R \text{ so, dass es ein } y \in R \text{ mit } ya \equiv_m 1 \text{ in } R \text{ gibt}\}\\ &= \{[a] \mid a \in R \text{ mit } \gcd(m,a) \mid 1 \text{ in } R\} = \{[a] \mid a \in R \text{ mit } \gcd(m,a) = 1 \text{ in } R\}.\end{aligned}$$

□

Alternativer Beweis von Beispiel (13.23).

(a) Wir verwenden den erweiterten euklidischen Algorithmus. Hierzu setzen wir

$$\begin{aligned}r_0 &:= 30,\\ r_1 &:= 17, && q_1 := r_0 \operatorname{div} r_1 = 30 \operatorname{div} 17 = 1,\\ r_2 &:= r_0 \bmod r_1 = 30 \bmod 17 = 13, && q_2 := r_1 \operatorname{div} r_2 = 17 \operatorname{div} 13 = 1,\\ r_3 &:= r_1 \bmod r_2 = 17 \bmod 13 = 4, && q_3 := r_2 \operatorname{div} r_3 = 13 \operatorname{div} 4 = 3,\\ r_4 &:= r_2 \bmod r_3 = 13 \bmod 4 = 1, && q_4 := r_3 \operatorname{div} r_4 = 4 \operatorname{div} 1 = 4,\\ r_5 &:= r_3 \bmod r_4 = 4 \bmod 1 = 0\end{aligned}$$

sowie

$$\begin{aligned}y_0 &:= 0,\\ y_1 &:= 1,\\ y_2 &:= y_0 - q_1 y_1 = 0 - 1 \cdot 1 = -1,\\ y_3 &:= y_1 - q_2 y_2 = 1 - 1 \cdot (-1) = 2,\\ y_4 &:= y_2 - q_3 y_3 = -1 - 3 \cdot 2 = -7.\end{aligned}$$

Nach Satz (12.27)(b) ist $\gcd(30, 17) = 1$ und es gibt ein $x_4 \in \mathbb{Z}$ mit

$$1 = r_4 = x_4 \cdot 30 + y_4 \cdot 17 = x_4 \cdot 30 + (-7) \cdot 17.$$

Nach Proposition (13.24) ist somit $17 \in (\mathbb{Z}/30)^\times$ mit

$$17^{-1} = -7 = 23$$

in $\mathbb{Z}/30$.

(b) Wir verwenden den erweiterten euklidischen Algorithmus. Hierzu setzen wir

$$\begin{aligned}r_0 &:= X^2 - 1,\\ r_1 &:= X + 2, && q_1 := r_0 \operatorname{div} r_1 = (X^2 - 1) \operatorname{div} (X + 2) = X - 2,\\ r_2 &:= r_0 \bmod r_1 = (X^2 - 1) \bmod (X + 2) = 3, && q_2 := r_1 \operatorname{div} r_2 = (X + 2) \operatorname{div} 3 = \frac{1}{3}X + \frac{2}{3},\\ r_3 &:= r_1 \bmod r_2 = (X + 2) \bmod 3 = 0\end{aligned}$$

sowie

$$\begin{aligned}k_0 &:= 0,\\ k_1 &:= 1,\\ k_2 &:= k_0 - q_1 k_1 = 0 - (X - 2) \cdot 1 = -X + 2.\end{aligned}$$

Nach Satz (12.27)(b) ist $\gcd(X^2 - 1, X + 2) = 1$ und es gibt ein $h_2 \in \mathbb{Q}[X]$ mit

$$3 = r_2 = h_2 \cdot (X^2 - 1) + k_2 \cdot (X + 2) = h_2 \cdot (X^2 - 1) + (-X + 2) \cdot (X + 2),$$

also mit

$$1 = \frac{1}{3}h_2 \cdot (X^2 - 1) + (-\frac{1}{3}X + \frac{2}{3}) \cdot (X + 2).$$

Nach Proposition (13.24) ist somit $2 + [X] \in (\mathbb{Q}[X]/(X^2 - 1))^\times$ mit

$$(2 + [X])^{-1} = \frac{2}{3} - \frac{1}{3}[X]$$

in $\mathbb{Q}[X]/(X^2 - 1)$. □

(13.25) Beispiel. Es ist

$$(\mathbb{Z}/8)^\times = \{[1],[3],[5],[7]\} = \{1,3,5,7\}.$$

Beweis. Nach Korollar (13.16)(a) ist $\mathbb{Z}/8 = \{[0],[1],[2],[3],[4],[5],[6],[7]\}$. Es gilt $\gcd(8,0) = 8$, $\gcd(8,1) = 1$, $\gcd(8,2) = 2$, $\gcd(8,3) = 1$, $\gcd(8,4) = 4$, $\gcd(8,5) = 1$, $\gcd(8,6) = 2$, $\gcd(8,7) = 1$. Nach Proposition (13.24) ist daher $(\mathbb{Z}/8)^\times = \{[1],[3],[5],[7]\}$. □

(13.26) Satz. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner sei $m \in R$ gegeben. Genau dann ist R/m ein Körper, wenn m irreduzibel ist.

Beweis. Es ist R/m stets ein kommutativer Ring. Wenn $m = 0$ ist, so ist $[a] = \{a\}$ für $a \in R$ und damit $R/0$ kein Körper. Wenn $m \in R^\times$ ist, so ist $[a] = [b]$ für $a, b \in R$ und damit $R/m = \{0\}$ ebenfalls kein Körper.
Im Folgenden sei also $m \in R \setminus (\{0\} \dot\cup R^\times)$. Wir betrachten die Standardtransversale T von R bzgl. $\equiv_m$, also die Menge aller möglichen Reste bei der Division mit Rest durch m. Wegen $m \notin R^\times$ gilt stets $0 = [0] \neq [1] = 1$ in R/m. Somit ist R/m genau dann ein Körper, wenn $[a]$ für jedes $a \in T \setminus \{0\}$ invertierbar in R/m ist. Nach Proposition (13.24) gilt dies aber genau dann, wenn für $a \in T \setminus \{0\}$ stets $\gcd(m,a) = 1$ ist. Dies gilt genau dann, wenn m irreduzibel ist. □

Endliche Primkörper

Da die Primzahlen gerade die positiven irreduziblen Elemente im Ring der ganzen Zahlen $\mathbb{Z}$ sind, ist $\mathbb{Z}/p$ nach Satz (13.26) stets ein Körper.

(13.27) Definition (endlicher Primkörper)**.** Für $p \in \mathbb{P}$ heißt $\mathbb{F}_p := \mathbb{Z}/p$ der *Primkörper* zur Primzahl p.

Wir wollen einige Beispiele dieser allgemeinen Konstruktion näher betrachten:

(13.28) Beispiel.

(a) Die Werte der Addition und Multiplikation von $\mathbb{F}_2 = \mathbb{Z}/2 = \{0,1\}$ sind wie folgt gegeben.

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

(b) Die Werte der Addition und Multiplikation von $\mathbb{F}_3 = \mathbb{Z}/3 = \{0,1,2\}$ sind wie folgt gegeben.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

(c) Die Werte der Addition und Multiplikation von $\mathbb{F}_5 = \mathbb{Z}/5 = \{0,1,2,3,4\}$ sind wie folgt gegeben.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Restklassenkörper von Polynomringen

Als nächstes betrachten wir Restklassenringe von Polynomringen über Körpern modulo einem irreduziblen Polynom. Nach Satz (13.26) handelt es sich auch bei diesen Restklassenringen um Körper.
Das berühmteste Beispiel ist der Körper der komplexen Zahlen:

(13.29) Beispiel. Der Restklassenring $\mathbb{R}[X]/(X^2+1)$ ist ein Körper.

Beweis. Wegen $a^2 + 1 \geq 0 + 1 = 1 > 0$ für $a \in \mathbb{R}$ hat das Polynom $X^2 + 1$ über $\mathbb{R}$ keine Nullstelle. Nach Bemerkung (12.35)(b) ist daher $X^2 + 1$ im Polynomring $\mathbb{R}[X]$ irreduzibel und damit $\mathbb{R}[X]/(X^2 + 1)$ nach Satz (13.26) ein Körper. □

(13.30) Definition (Körper der komplexen Zahlen)**.** Wir nennen $\mathbb{C} := \mathbb{R}[X]/(X^2 + 1)$ den *Körper der komplexen Zahlen*. Ein Element von $\mathbb{C}$ wird *komplexe Zahl* genannt. Das Element $\mathrm{i} := [X] \in \mathbb{C}$ wird *imaginäre Einheit* (oder *imaginäre Zahl*) genannt.

(13.31) Bemerkung. Es gilt

$$\mathbb{C} = \{a + b\mathrm{i} \mid a, b \in \mathbb{R}\}.$$

Für $a, b, a', b' \in \mathbb{R}$ gilt genau dann

$$a + b\mathrm{i} = a' + b'\mathrm{i}$$

in $\mathbb{C}$, wenn $a = a'$ und $b = b'$ in $\mathbb{R}$ gilt. Für $a, b, c, d \in \mathbb{R}$ gilt

$$\begin{aligned}(a + b\mathrm{i}) + (c + d\mathrm{i}) &= (a + c) + (b + d)\mathrm{i},\\ (a + b\mathrm{i}) \cdot (c + d\mathrm{i}) &= (ac - bd) + (ad + bc)\mathrm{i}\end{aligned}$$

in $\mathbb{C}$.

Beweis. Nach Korollar (13.16)(b) ist $\mathbb{R}[X]_{<\deg(X^2+1)} = \mathbb{R}[X]_{<2}$ eine Transversale von $\mathbb{R}[X]$ bzgl. $\equiv_{X^2+1}$ und es gilt

$$\mathbb{C} = \mathbb{R}[X]/(X^2 + 1) = \{a + b[X] \mid a, b \in \mathbb{R}\} = \{a + b\mathrm{i} \mid a, b \in \mathbb{R}\}.$$

Folglich gilt für $a, b, a', b' \in \mathbb{R}$ genau dann $a + b\mathrm{i} = a' + b'\mathrm{i}$ in $\mathbb{C}$, wenn $a + bX = a' + b'X$ in $\mathbb{R}[X]$ gilt, und dies ist äquivalent zu $a = a'$ und $b = b'$ in $\mathbb{R}$.
Ferner ist

$$\mathrm{i}^2 + 1 = [X]^2 + 1 = [X^2 + 1] = [0] = 0$$

und damit $\mathrm{i}^2 = -1$ in $\mathbb{C}$. Für $a, b, c, d \in \mathbb{R}$ folgt

$$\begin{aligned}(a + b\mathrm{i}) + (c + d\mathrm{i}) &= (a + c) + (b + d)\mathrm{i},\\ (a + b\mathrm{i}) \cdot (c + d\mathrm{i}) &= ac + ad\mathrm{i} + bc\mathrm{i} + bd\mathrm{i}^2 = ac + ad\mathrm{i} + bc\mathrm{i} - bd = (ac - bd) + (ad + bc)\mathrm{i}\end{aligned}$$

in $\mathbb{C}$. □

(13.32) Definition (Realteil, Imaginärteil)**.** Es seien $z \in \mathbb{C}$ und $a, b \in \mathbb{R}$ mit $z = a + b\mathrm{i}$ gegeben. Wir nennen a den *Realteil* von z und schreiben $\operatorname{Re} z := a$. Wir nennen b den *Imaginärteil* von z und schreiben $\operatorname{Im} z := b$.

(13.33) Beispiel. Es ist $\operatorname{Re}(2 - \mathrm{i}) = 2$ und $\operatorname{Im}(2 - \mathrm{i}) = -1$.

(13.34) Definition (konjugierte komplexe Zahl)**.** Es sei $z \in \mathbb{C}$ gegeben. Wir nennen

$$\overline{z} := \operatorname{Re} z - (\operatorname{Im} z)\mathrm{i}$$

die zu z *konjugierte komplexe Zahl* (oder die zu z *komplex Konjugierte*).

(13.35) Beispiel. Es ist $\overline{3 - 2\mathrm{i}} = 3 + 2\mathrm{i}$.

Analog zu den komplexen Zahlen als Restklassenkörper von $\mathbb{R}[X]$ können wir auch Restklassenkörper von Polynomringen über endlichen Körpern betrachten und so neue endliche Körper konstruieren:

(13.36) Beispiel.

(a) Der Restklassenring $\mathbb{F}_2[X]/(X^2 + X + 1)$ ist ein Körper.

(b) Der Restklassenring $\mathbb{F}_2[X]/(X^3 + X + 1)$ ist ein Körper.

(c) Der Restklassenring $\mathbb{F}_3[X]/(X^2+1)$ ist ein Körper.

Beweis.

(a) Wegen $0^2+0+1=1$ und $1^2+1+1=1$ in $\mathbb{F}_2$ hat das Polynom X^2+X+1 über $\mathbb{F}_2$ keine Nullstelle. Nach Bemerkung (12.35)(b) ist daher X^2+X+1 im Polynomring $\mathbb{F}_2[X]$ irreduzibel und damit $\mathbb{F}_2[X]/(X^2+X+1)$ nach Satz (13.26) ein Körper.

(b) Dies sei dem Leser zur Übung überlassen.

(c) Dies sei dem Leser zur Übung überlassen. □

(13.37) Notation.

(a) Wir setzen $\mathbb{F}_4 := \mathbb{F}_2[X]/(X^2+X+1)$ und $\alpha := [X]_{X^2+X+1}$.

(b) Wir setzen $\mathbb{F}_8 := \mathbb{F}_2[X]/(X^3+X+1)$ und $\beta := [X]_{X^3+X+1}$.

(c) Wir setzen $\mathbb{F}_9 := \mathbb{F}_3[X]/(X^2+1)$ und $\iota := [X]_{X^2+1}$.

Analog zu Bemerkung (13.31) lassen sich Beschreibungen von $\mathbb{F}_4$, $\mathbb{F}_8$ und $\mathbb{F}_9$ herleiten. Wir beschränken uns auf $\mathbb{F}_4$ und überlassen die beiden anderen Fälle zur Übung.

(13.38) Bemerkung. Es gilt

$$\mathbb{F}_4 = \{a+b\alpha \mid a,b \in \mathbb{F}_2\}.$$

Für $a,b,a',b' \in \mathbb{F}_2$ gilt genau dann

$$a+b\alpha = a'+b'\alpha$$

in $\mathbb{F}_4$, wenn $a=a'$ und $b=b'$ in $\mathbb{F}_2$ gilt. Für $a,b,c,d \in \mathbb{F}_2$ gilt

$$\begin{aligned}(a+b\alpha)+(c+d\alpha) &= (a+c)+(b+d)\alpha,\\ (a+b\alpha)\cdot(c+d\alpha) &= (ac+bd)+(ad+bc+bd)\alpha\end{aligned}$$

in $\mathbb{F}_4$.

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Beweis. Nach Korollar (13.16)(b) ist $\mathbb{F}_2[X]_{<\deg(X^2+X+1)} = \mathbb{F}_2[X]_{<2}$ eine Transversale von $\mathbb{F}_2[X]$ bzgl. $\equiv_{X^2+X+1}$ und es gilt

$$\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1) = \{a+b[X] \mid a,b \in \mathbb{F}_2\} = \{a+b\alpha \mid a,b \in \mathbb{F}_2\}.$$

Folglich gilt für $a,b,a',b' \in \mathbb{F}_2$ genau dann $a+b\alpha = a'+b'\alpha$ in $\mathbb{F}_4$, wenn $a+bX = a'+b'X$ in $\mathbb{F}_2[X]$ gilt, und dies ist äquivalent zu $a=a'$ und $b=b'$ in $\mathbb{F}_2$.
Ferner ist

$$\alpha^2+\alpha+1 = [X]^2+[X]+1 = [X^2+X+1] = [0] = 0$$

und damit $\alpha^2 = -1-\alpha = 1+\alpha$ in $\mathbb{F}_4$. Für $a,b,c,d \in \mathbb{F}_2$ folgt

$$\begin{aligned}(a+b\alpha)+(c+d\alpha) &= (a+c)+(b+d)\alpha,\\ (a+b\alpha)\cdot(c+d\alpha) &= ac+ad\alpha+bc\alpha+bd\alpha^2 = ac+ad\alpha+bc\alpha+bd+bd\alpha\\ &= (ac+bd)+(ad+bc+bd)\alpha\end{aligned}$$

in $\mathbb{F}_4$. □

Wir betonen, dass $\mathbb{F}_4 \neq \mathbb{Z}/4$ ist. Während $\mathbb{F}_4$ ein Körper und damit insbesondere ein Integritätsbereich ist, gilt im kommutativen Ring $\mathbb{Z}/4$ die Gleichung $2\cdot 2 = 0$.
Der Körper $\mathbb{F}_2 = \{0,1\}$ hat zwei Elemente, welche sich in der Informatik als Bits interpretieren lassen. Die Elemente des Körpers $\mathbb{F}_{2^8} := \mathbb{F}_2[X]/(X^8+X^4+X^3+X+1)$ lassen sich hingegen als Bytes interpretieren. Dieser Körper kommt beispielsweise bei der Codierungstheorie einer CD oder beim AES-Algorithmus in der Kryptographie zur Anwendung.

Euler-Funktion

Um eine Anwendung der Kongruenzrechnung, das RSA-Kryptosystem, formulieren zu können, müssen wir zunächst nachfolgende Abbildung studieren.

(13.39) Definition (Euler-Funktion)**.** Die *Euler-Funktion* (oder *Eulersche Funktion* oder *Eulersche Phi-Funktion*) ist definiert als

$$\varphi\colon \mathbb{N} \to \mathbb{N},\ n \mapsto |(\mathbb{Z}/n)^\times|.$$

(13.40) Beispiel. Es ist $\varphi(8) = 4$.

Beweis. Nach Beispiel (13.25) ist $(\mathbb{Z}/8)^\times = \{1, 3, 5, 7\}$ und damit $\varphi(8) = 4$. □

(13.41) Bemerkung. Für $n \in \mathbb{N}$ ist

$$\varphi(n) = |\{x \in [0, n-1] \mid \gcd(n, x) = 1\}| = |\{x \in [1, n] \mid \gcd(n, x) = 1\}|.$$

Beweis. Es sei $n \in \mathbb{N}$ gegeben. Dann sind $[0, n-1]$ und $[1, n]$ Transversalen von $\mathbb{Z}$ bzgl. $\equiv_n$. Für jede Transversale T von $\mathbb{Z}$ bzgl. $\equiv_n$ gilt nach Proposition (13.24) jedoch

$$(\mathbb{Z}/n)^\times = \{[x] \mid x \in \mathbb{Z} \text{ mit } \gcd(n, x) = 1\} = \{[x] \mid x \in T \text{ mit } \gcd(n, x) = 1\}$$

und damit

$$\varphi(n) = |(\mathbb{Z}/n)^\times| = |\{[x] \mid x \in T \text{ mit } \gcd(n, x) = 1\}| = |\{x \in T \mid \gcd(n, x) = 1\}|.$$ □

(13.42) Proposition.

(a) Für $p, q \in \mathbb{P}$ mit $p \neq q$ ist

$$\varphi(pq) = (p-1)(q-1).$$

(b) Für $p \in \mathbb{P}$ ist

$$\varphi(p) = p - 1.$$

Beweis.

(a) Dies sei dem Leser zur Übung überlassen.

(b) Für $p \in \mathbb{P}$ ist $\mathbb{Z}/p = \mathbb{F}_p$ nach Satz (13.26) ein Körper und damit

$$\varphi(p) = |(\mathbb{Z}/p)^\times| = |{\mathbb{F}_p}^\times| = |\mathbb{F}_p \setminus \{0\}| = |\mathbb{F}_p| - 1 = p - 1.$$ □

(13.43) Lemma. Es sei eine endliche kommutative Gruppe G gegeben. Für $x \in G$ gilt

$$x^{|G|} = 1.$$

Beweis. Es sei $x \in G$ gegeben. Dann ist $G \to G,\ y \mapsto xy$ eine Bijektion. Auf Grund der Kommutativität von G erhalten wir

$$\prod_{y \in G} y = \prod_{y \in G} (xy) = \Big(\prod_{y \in G} x\Big)\Big(\prod_{y \in G} y\Big)$$

und damit

$$x^{|G|} = \prod_{y \in G} x = 1$$

nach Korollar (6.30). □

Ohne Beweis sei angemerkt, dass Lemma (13.43) auch für nicht kommutative endliche Gruppen gilt.

(13.44) Satz (Satz von Euler)**.** Für $n \in \mathbb{N}$, $a \in \mathbb{Z}$ mit $\gcd(n, a) = 1$ gilt

$$a^{\varphi(n)} \equiv_n 1.$$

Beweis. Es seien $n \in \mathbb{N}$, $a \in \mathbb{Z}$ mit $\gcd(n, a) = 1$ gegeben. Wegen $\gcd(n, a) = 1$ ist $[a] \in (\mathbb{Z}/n)^\times$ nach Proposition (13.24). Nach Lemma (13.43) folgt

$$[a^{\varphi(n)}] = [a]^{\varphi(n)} = [a]^{|(\mathbb{Z}/n)^\times|} = 1$$

in $\mathbb{Z}/n$ und damit $a^{\varphi(n)} \equiv_n 1$ in $\mathbb{Z}$. □

(13.45) Korollar. Für $p \in \mathbb{P}$, $a \in \mathbb{Z}$ mit $p \nmid a$ gilt

$$a^{p-1} \equiv_p 1.$$

Beweis. Es seien $p \in \mathbb{P}$, $a \in \mathbb{Z}$ mit $p \nmid a$ gegeben. Wegen $p \nmid a$ und der Irreduzibilität von p ist $\gcd(p, a) = 1$. Nach Proposition (13.42)(b) ist ferner $\varphi(p) = p - 1$, so dass aus dem Satz von Euler (13.44) bereits

$$a^{p-1} = a^{\varphi(p)} \equiv_p 1$$

folgt. □

(13.46) Korollar (kleiner Satz von Fermat)**.** Für $p \in \mathbb{P}$, $a \in \mathbb{Z}$ gilt

$$a^p \equiv_p a.$$

Beweis. Es seien $p \in \mathbb{P}$, $a \in \mathbb{Z}$ gegeben. Wenn $p \nmid a$ gilt, dann ist $a^{p-1} \equiv_p 1$ nach Korollar (13.45). Dies impliziert nach Proposition (13.5) jedoch bereits

$$a^p = a \cdot a^{p-1} \equiv_p a \cdot 1 = a.$$

Wenn hingegen $p \mid a$ gilt, so haben wir $a \equiv_p 0$, also

$$a^p \equiv_p 0^p = 0 \equiv_p a$$

nach Proposition (13.5). Folglich gilt in jedem Fall $a^p \equiv_p a$. □

Anwendung: RSA-Kryptosystem

Zum Schluss dieses Abschnitts über Kongruenzrechnung wollen wir als Anwendung ein Verfahren zum Ver- und Entschlüsseln von Nachrichten kennenlernen. Die Ausgangssituation ist wie folgt: Ein Sender verschlüsselt einen gegebenen Text und sendet das Chiffrat danach über einen unsicheren Kanal an einen Empfänger, welcher den Geheimtext anschließend wieder entschlüsselt und so den ursprünglichen Text erhält. ([47])

Hierzu betrachten ein sogenanntes *Public-Key-Kryptosystem*, bestehend aus einer Menge von *Klartexten* $\mathcal{P}$, einer Menge von *Geheimtexten* (oder *Chiffraten*) $\mathcal{C}$, einem *öffentlichen Schlüssel* K_{publ} und einem *privaten Schlüssel* K_{priv}. Die beiden Schlüssel bedingen ihrerseits eine Abbildung $e\colon \mathcal{P} \to \mathcal{C}$, die *Verschlüsselungsfunktion*, und eine Abbildung $d\colon \mathcal{C} \to \mathcal{P}$, die *Entschlüsselungsfunktion*, mit

$$d \circ e = \mathrm{id}_{\mathcal{P}}.$$

Der öffentliche Schlüssel wird zum Versenden von Nachrichten benutzt und hierzu öffentlich publiziert, etwa auf der persönlichen Homepage des Empfängers. Entsprechend darf die Verschlüsselungsfunktion $e\colon \mathcal{P} \to \mathcal{C}$ eines Public-Key-Kryptosystems nur vom öffentlichen Schlüssel abhängen. Der private Schlüssel ist hingegen nur dem Empfänger bekannt und wird von diesem geheimgehalten. Damit ein Public-Key-Kryptosystem sicher ist, darf es in der Praxis unter vertretbarem Aufwand nicht möglich sein, den privaten Schlüssel aus dem öffentlichen Schlüssel zu berechnen.

Im Folgenden wird die Menge der Klartexte durch $\mathcal{P} = [0, n-1]$ für ein hinreichend großes $n \in \mathbb{N}$ gegeben sein. In der Praxis muss ein zu verschlüsselnder Text also zunächst in ein Element oder eine Folge von Elementen aus $\mathcal{P}$ umgewandelt werden. Diesen Prozess werden wir hier nicht näher thematisieren.

Bevor wir in Anwendung (13.49) ein konkretes Verfahren vorstellen, wollen wir zunächst die dahinterstehende Theorie herleiten.

[47] Das hier betrachtete RSA-Kryptosystem und weitere Verfahren zur Nachrichtenverschlüsselung werden in Vorlesungen über *Kryptographie* eingehender studiert. Grundlagen hierzu werden an der RWTH Aachen üblicherweise im Rahmen des Kurses *Datenkommunikation und Sicherheit* (ab etwa 4. Semester im Studiengang B.Sc. Informatik) vermittelt.

(13.47) Proposition. Es seien $p, q \in \mathbb{P}$ mit $p \neq q$ gegeben. Ferner seien $a, b \in \mathbb{Z}$ mit $ab \equiv_{\varphi(pq)} 1$ gegeben. Für alle $x \in \mathbb{Z}$ gilt dann

$$x^{ab} \equiv_{pq} x.$$

Beweis. Es sei $x \in \mathbb{Z}$ gegeben.
Zunächst gelte $p \nmid x$. Nach Korollar (13.45) gilt dann $x^{p-1} \equiv_p 1$. Nun ist nach Proposition (13.42)(a) jedoch $\varphi(pq) = (p-1)(q-1)$, es gilt also auch

$$x^{\varphi(pq)} = x^{(p-1)(q-1)} = (x^{p-1})^{q-1} \equiv_p 1.$$

Wegen $ab \equiv_{\varphi(pq)} 1$ impliziert dies $x^{ab} \equiv_p x$.
Gilt hingegen $p \mid x$, so haben wir $x \equiv_p 0$, also

$$x^{ab} \equiv_p 0 \equiv_p x.$$

Es gilt also in jedem Fall $x^{ab} \equiv_p x$, d.h. $p \mid x^{ab} - x$. Analog ist auch $x^{ab} \equiv_q x$, d.h. $q \mid x^{ab} - x$. Da p und q verschiedene Primzahlen sind, impliziert dies bereits $pq \mid x^{ab} - x$ und damit $x^{ab} \equiv_{pq} x$. □

(13.48) Korollar. Es seien $p, q \in \mathbb{P}$ mit $p \neq q$ und $a, b \in \mathbb{Z}$ mit $ab \equiv_{\varphi(pq)} 1$ gegeben. Dann sind

$$\mathbb{Z}/(pq) \to \mathbb{Z}/(pq),\ [x] \mapsto [x]^a,$$
$$\mathbb{Z}/(pq) \to \mathbb{Z}/(pq),\ [y] \mapsto [y]^b$$

sich gegenseitig invertierende Bijektionen.

Das vorangegangene Korollar ist Grundlage des nachfolgenden Verschlüsselungsverfahrens.

(13.49) Anwendung (RSA-Kryptosystem; Rivest, Shamir, Adleman; 1977)**.**

- Initialisierung:
  - Wähle geeignete große Primzahlen p und q mit $p \neq q$ (ungefähr 250 Stellen).
  - Berechne $n := pq$ und $\varphi(n) = (p-1)(q-1)$.
  - Wähle geeignetes $a \in [1, \varphi(n)]$ mit $\gcd(\varphi(n), a) = 1$.
  - Berechne $b \in [1, \varphi(n)]$ mit $ab \equiv_{\varphi(n)} 1$.
  - Publiziere den öffentlichen Schlüssel $K_{\text{publ}} := (n, a)$ (zum Beispiel auf persönlicher Homepage).
  - Halte den privaten Schlüssel $K_{\text{priv}} := b$ geheim.
  - Die Menge der Klartexte ist $\mathcal{P} := [0, n-1]$. Die Menge der Geheimtexte ist $\mathcal{C} := [0, n-1]$.
- Verschlüsselung eines Klartexts $x \in \mathcal{P}$:
  - Berechne
    $$e(x) = x^a \bmod n.$$
- Entschlüsselung eines Geheimtexts $y \in \mathcal{C}$:
  - Berechne
    $$d(y) = y^b \bmod n.$$
- Beispiel:
  - Wir wählen $p = 3$, $q = 11$. Dann ist $n = pq = 3 \cdot 11 = 33$ und $\varphi(n) = (p-1)(q-1) = 2 \cdot 10 = 20$. Wir wählen $a = 3$. Dann ist $3 \cdot 7 = 21 \equiv_{20} 1$, also $b = 7$. Der öffentliche Schlüssel ist
    $$K_{\text{publ}} = (n, a) = (33, 3).$$
    Der private Schlüssel ist
    $$K_{\text{priv}} = b = 7.$$

– Die Verschlüsselung des Klartexts $x = 13$ ergibt

$$e(x) = x^a \bmod n = 13^3 \bmod 33 = (13 \cdot 169) \bmod 33 = (13 \cdot 4) \bmod 33 = 52 \bmod 33 = 19.$$

– Die Entschlüsselung des Geheimtexts $y = 19$ ergibt

$$\begin{aligned} d(y) = y^b \bmod n &= 19^7 \bmod 33 = (-14)^7 \bmod 33 = (196^3(-14)) \bmod 33 \\ &= ((-2)^3(-14)) \bmod 33 = (8 \cdot 14) \bmod 33 = 112 \bmod 33 = 13. \end{aligned}$$

Die Sicherheit des RSA-Kryptosystems beruht auf der Schwierigkeit, große natürliche Zahlen zu faktorisieren. Könnte ein Angreifer aus der Kenntnis des öffentlichen Schlüssels $K_{\text{publ}} = (n, a)$ in Anwendung (13.49) die Primfaktoren von n ermitteln, so könnte er auch $\varphi(n)$ und damit mit Hilfe des erweiterten euklidischen Algorithmus' (12.27) den privaten Schlüssel $K_{\text{priv}} = b$ berechnen.

14 Die symmetrische Gruppe

Als nächstes studieren wir mit den symmetrischen Gruppen eine Beispielklasse von Gruppen, welche als Gruppen der invertierbaren Elemente in Abbildungsmonoiden auftauchen.

Begriffsbildung

Es sei eine Menge X gegeben. Nach Bemerkung (6.22) wird $\mathrm{Map}(X, X)$ ein Monoid mit Monoidverknüpfung $(g, f) \mapsto g \circ f$ und Einselement id_X. Wir interessieren uns für die Gruppe der invertierbaren Elemente in $\mathrm{Map}(X, X)$:

(14.1) Definition (symmetrische Gruppe)**.**

(a) Es sei eine Menge X gegeben. Die Gruppe

$$\mathrm{S}_X := \mathrm{Map}(X, X)^\times$$

heißt *symmetrische Gruppe* auf X. Ein Element von S_X wird eine *Permutation* von X genannt.

(b) Es sei $n \in \mathbb{N}_0$ gegeben. Wir nennen

$$\mathrm{S}_n := \mathrm{S}_{[1,n]}$$

auch die *symmetrische Gruppe* vom Grad n. Für $\pi \in \mathrm{S}_n$ schreiben wir

$$\left(\begin{smallmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{smallmatrix}\right) := \pi.$$

Nach Satz (3.29)(c) besteht S_X für eine Menge X aus allen bijektiven Abbildungen von X nach X.
Permutationen, also die Elemente einer symmetrischen Gruppe, tauchen in der Informatik etwa bei Sortieralgorithmen ([48]) auf.

(14.2) Beispiel.

(a) Es ist

$$\mathrm{S}_0 = \{\mathrm{id}_\emptyset\} = \{(\ )\}.$$

(b) Es ist

$$\mathrm{S}_1 = \{\mathrm{id}_{\{1\}}\} = \left\{\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)\right\}.$$

(c) Es ist

$$\mathrm{S}_2 = \{\mathrm{id}_{\{1,2\}}, (1 \mapsto 2,\ 2 \mapsto 1)\} = \left\{\left(\begin{smallmatrix} 1 & 2 \\ 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right)\right\}.$$

[48] Sortieralgorithmen werden an der RWTH Aachen bspw. im Rahmen des Kurses *Datenstrukturen und Algorithmen* (etwa 2. Semester im Studiengang B.Sc. Informatik) studiert.

(d) Es ist

$$S_3 = \{\left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right)\}.$$

Man beachte, dass wir beim Bilden von Komposita – wie immer – von rechts nach links lesen:

(14.3) Beispiel. In S_3 ist

$$\left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right) \circ \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right),$$
$$\left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right) \circ \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right).$$

Zykelschreibweise

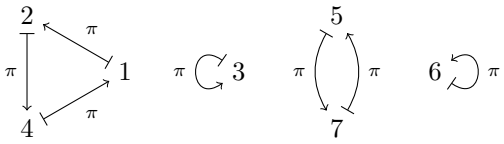
Die klassische Schreibweise für Permutationen ist für viele Zwecke noch etwas schwerfällig. Um die sogenannte Zykelschreibweise einzuführen, studieren wir die iterierte Anwendung einer gegebenen Permutation.
Betrachten wir etwa $\pi \in S_7$ gegeben durch $\pi = \left(\begin{smallmatrix}1&2&3&4&5&6&7\\2&4&3&1&7&6&5\end{smallmatrix}\right)$. Die iterierte Anwendung von π auf das Element 1 ergibt

$$\begin{aligned}
\pi(1) &= 2,\\
\pi^2(1) &= \pi(\pi(1)) = \pi(2) = 4,\\
\pi^3(1) &= \pi(\pi^2(1)) = \pi(4) = 1,\\
\pi^4(1) &= \pi(\pi^3(1)) = \pi(1) = 2,\\
\pi^5(1) &= \pi(\pi^4(1)) = \pi(2) = 4,\\
\pi^6(1) &= \pi(\pi^5(1)) = \pi(4) = 1,\\
\pi^7(1) &= \pi(\pi^6(1)) = \pi(1) = 2,
\end{aligned}$$

und so weiter. Wir erhalten also periodisch immer wieder die Werte 1, 2, 4, wobei sich die Werte nach jeder dritten Anwendung wiederholen. Bei der iterierten Anwendung von π^{-1} erhalten wir wieder nur die Werte 1, 2, 4 im Wechsel, lediglich die Reihenfolge des Auftretens ändert sich. Somit gilt also

$$\{\pi^k(1) \mid k \in \mathbb{Z}\} = \{1, 2, 4\}.$$

Dasselbe Resultat ergibt sich, wenn wir mit dem Element 2 oder dem Element 4 beginnen, lediglich das Auftreten der einzelnen Werte ist um ein oder zwei Stellen verschoben. Wenn wir hingegen mit dem Element 5 oder dem Element 7 beginnen, so erhalten wir abwechselnd die Werte 5 und 7, und wenn wir mit dem Element 3 oder dem Element 6 beginnen, so bleibt der jeweilige Wert nach Anwendung von π erhalten, also auch nach iterierter Anwendung von π.



Wir wollen nun die Tatsache, dass 1, 2, 4 bei iterierter Anwendung von π (und π^{-1}) ineinander übergehen, für eine alternative Notation von π ausnutzen.

(14.4) Bemerkung. Es seien eine Menge X und $\pi \in S_X$ gegeben. Für $x, y \in X$ gelte genau dann $x \sim_\pi y$, wenn es ein $k \in \mathbb{Z}$ mit $y = \pi^k(x)$ gibt. Dann ist $\sim_\pi$ eine Äquivalenzrelation auf X.

Beweis. Es seien $x, y, z \in X$ mit $x \sim_\pi y$ und $y \sim_\pi z$ gegeben, so dass es $k, l \in \mathbb{Z}$ mit $y = \pi^k(x)$ und $z = \pi^l(y)$ gibt. Dann folgt

$$z = \pi^l(y) = \pi^l(\pi^k(x)) = \pi^{k+l}(x)$$

und damit $x \sim_\pi z$. Folglich ist $\sim_\pi$ transitiv.
Für $x \in X$ gilt $\pi^0(x) = \mathrm{id}_X(x) = x$, also $x \sim_\pi x$. Folglich ist $\sim_\pi$ reflexiv.
Es seien $x, y \in X$ mit $x \sim_\pi y$ gegeben, so dass es ein $k \in \mathbb{Z}$ mit $y = \pi^k(x)$ gibt. Dann folgt $x = \pi^{-k}(y)$ und damit $y \sim_\pi x$. Folglich ist $\sim_\pi$ symmetrisch.
Insgesamt ist $\sim_\pi$ eine Äquivalenzrelation auf X. □

(14.5) Definition (Bahn)**.** Es seien eine Menge X und $\pi \in \mathrm{S}_X$ gegeben. Die Äquivalenzrelation $\sim_\pi$ auf X aus Bemerkung (14.4) heißt *Bahnengleichheit* unter π. Die Quotientenmenge $X/\pi := X/\sim_\pi$ heißt *Menge der Bahnen* unter π. Ein Element von X/π heißt *Bahn* in X unter π. Für $x \in X$ heißt $[x]_\pi := [x]_{\sim_\pi}$ die *Bahn* von x unter π. Für eine Bahn O in X unter π heißt $|O|$ die *Länge* von O. Eine Transversale von $X/\sim_\pi$ heißt *Transversale der Bahnen* unter π.

Nach dem Hauptsatz über Äquivalenzrelationen (5.20) ist die Menge der Bahnen einer Permutation einer Menge X eine Partition von X.

(14.6) Beispiel. Es sei $\pi \in \mathrm{S}_7$ gegeben durch $\pi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 3 & 1 & 7 & 6 & 5 \end{smallmatrix}\right)$. Dann ist

$$\begin{aligned} &[1] = [2] = [4] = \{1, 2, 4\}, \\ &[3] = \{3\}, \\ &[5] = [7] = \{5, 7\}, \\ &[6] = \{6\} \end{aligned}$$

und

$$[1, 7]/\pi = \{[1], [3], [5], [6]\} = \{\{1, 2, 4\}, \{3\}, \{5, 7\}, \{6\}\}.$$

Beweis. Für $k \in \mathbb{Z}$ erhalten wir induktiv

$$\begin{aligned} \pi^k(1) &= \begin{cases} 1, & \text{falls } k \equiv_3 0, \\ 2, & \text{falls } k \equiv_3 1, \\ 4, & \text{falls } k \equiv_3 2, \end{cases} \\ \pi^k(3) &= 3, \\ \pi^k(5) &= \begin{cases} 5, & \text{falls } k \equiv_2 0, \\ 7, & \text{falls } k \equiv_2 1, \end{cases} \\ \pi^k(6) &= 6. \end{aligned}$$

Folglich gilt $[1] = [2] = [4] = \{1, 2, 4\}$, $[3] = \{3\}$, $[5] = [7] = \{5, 7\}$, $[6] = \{6\}$ und damit

$$[1, 7]/\pi = \{[1], [2], [3], [4], [5], [6], [7]\} = \{[1], [3], [5], [6]\} = \{\{1, 2, 4\}, \{3\}, \{5, 7\}, \{6\}\}.$$ □

(14.7) Bemerkung. Es seien eine Menge X, $\pi \in \mathrm{S}_X$, $x \in X$ und $k \in \mathbb{Z} \setminus \{0\}$ mit $\pi^k(x) = x$ gegeben. Für $l \in \mathbb{Z}$ gilt

$$\pi^l(x) = \pi^{l \bmod k}(x).$$

Beweis. Für $l \in \mathbb{Z}$ gilt $l = (l \operatorname{div} k)k + l \bmod k$ und $\pi^{(l \operatorname{div} k)k}(x) = x$, also

$$\pi^l(x) = \pi^{(l \operatorname{div} k)k + l \bmod k}(x) = \pi^{l \bmod k}(\pi^{(l \operatorname{div} k)k}(x)) = \pi^{l \bmod k}(x).$$ □

(14.8) Bemerkung. Es seien eine Menge X, $\pi \in \mathrm{S}_X$ und $x \in X$ gegeben. Genau dann ist $[x]_\pi$ endlich, wenn es ein $k \in \mathbb{N}$ mit $\pi^k(x) = x$ gibt.

Beweis. Wenn $[x]_\pi$ endlich ist, dann gibt es $k, l \in \mathbb{Z}$ mit $k > l$ und $\pi^k(x) = \pi^l(x)$ und folglich mit

$$\pi^{k-l}(x) = \pi^{-l}(\pi^k(x)) = x$$

in X. Gibt es umgekehrt ein $k \in \mathbb{N}$ mit $\pi^k(x) = x$, so gilt

$$[x]_\pi = \{\pi^l(x) \mid l \in \mathbb{Z}\} = \{\pi^{l \bmod k}(x) \mid l \in \mathbb{Z}\} = \{\pi^r(x) \mid r \in [0, k-1]\}$$

nach Bemerkung (14.7), und insbesondere ist $[x]_\pi$ endlich. □

(14.9) Proposition. Es seien eine Menge X, $\pi \in \mathrm{S}_X$ und $x \in X$ so gegeben, dass die Bahn $[x]_\pi$ von x unter π endlich ist. Ferner sei $m := \min\{k \in \mathbb{N} \mid \pi^k(x) = x\}$. Dann ist

$$\mathbb{Z}/m \to [x]_\pi,\ [k]_m \mapsto \pi^k(x)$$

eine wohldefinierte Bijektion. Insbesondere gilt $|[x]_\pi| = m$ und

$$[x]_\pi = \{\pi^k(x) \mid k \in [0, m-1]\}.$$

Beweis. Wir betrachten die Abbildung $f\colon \mathbb{Z} \to X$, $k \mapsto \pi^k(x)$. Nach dem Homomorphiesatz für Mengen (5.15) gibt es eine wohldefinierte Injektion $\bar{f}\colon \mathbb{Z}/{=_f} \to X$ mit $f = \bar{f} \circ \mathrm{quo}$, gegeben durch $\bar{f}([k]) = f(k) = \pi^k(x)$ für $k \in \mathbb{Z}$, und es ist $\operatorname{Im} \bar{f} = \operatorname{Im} f$.
Um zu zeigen, dass $=_f = \equiv_m$ ist, seien $k, l \in \mathbb{Z}$ gegeben. Genau dann gilt $k =_f l$ in $\mathbb{Z}$, wenn $\pi^k(x) = \pi^l(x)$ in X ist. Dies ist äquivalent zu $\pi^{k-l}(x) = x$. Nach Bemerkung (14.7) gilt $\pi^{k-l}(x) = \pi^{(k-l) \bmod m}(x)$. Folglich gilt genau dann $k =_f l$, wenn $\pi^{(k-l) \bmod m}(x) = x$ ist. Wegen $(k-l) \bmod m \in [0, m-1]$ und der Minimalität von m ist dies äquivalent zu $(k-l) \bmod m = 0$, nach Proposition (13.15)(b) also zu $k \equiv_m l$. Somit gilt in der Tat $=_f = \equiv_m$ und damit $\mathbb{Z}/{=_f} = \mathbb{Z}/{\equiv_m} = \mathbb{Z}/m$.
Ferner gilt

$$\operatorname{Im} \bar{f} = \operatorname{Im} f = \{f(k) \mid k \in \mathbb{Z}\} = \{\pi^k(x) \mid k \in \mathbb{Z}\} = [x]_\pi.$$

Folglich ist $\bar{f}|^{\operatorname{Im} f}\colon \mathbb{Z}/m \to [x]_\pi$ eine Bijektion. Da $[0, m-1]$ nach Korollar (13.16)(a) eine Transversale von $\mathbb{Z}/m$ ist, folgt insbesondere $|[x]_\pi| = |\mathbb{Z}/m| = m$ und

$$[x]_\pi = \operatorname{Im} \bar{f} = \{\bar{f}([k]_m) \mid k \in [0, m-1]\} = \{\pi^k(x) \mid k \in [0, m-1]\}. \qquad \square$$

Um eine Permutation gemäß ihrer Bahnen zu zerlegen, betrachten wir nun solche Permutationen, die höchstens eine nicht-einelementige Bahn haben. Neben der Bahn müssen wir uns dann nur noch die Reihenfolge des Auftretens der Elemente in der Bahn bei der Anwendung von π merken, weswegen wir eine Tupelnotation wählen.

(14.10) Definition (Zykel)**.** Es sei eine Menge X gegeben.

(a) Eine Permutation ζ von X heißt *zyklisch* (oder *Zykel* von X), falls jede Bahn unter ζ endlich ist und höchstens eine Bahn mehr als 1 Element hat.

(b) Es sei ein Zykel ζ von X gegeben. Die *Länge* von ζ ist 0, wenn $X = \emptyset$ ist, und das Maximum der Längen aller Bahnen unter ζ, wenn $X \neq \emptyset$ ist.

Für $m \in \mathbb{N}_0$ sagen wir, dass ζ ein *m-Zykel* ist, wenn ζ die Länge m hat.

(c) Es seien $m \in \mathbb{N}_0$, ein m-Zykel ζ von X und $x \in X$ mit $|[x]_\zeta| = m$ gegeben. Wir schreiben

$$(x, \zeta(x), \ldots, \zeta^{m-1}(x)) := \zeta.$$

(14.11) Beispiel. In S_3 ist

$\left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right) = (1,2)$,
$\left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right) = (1,3)$,
$\left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right) = (1,2,3)$.

Wir betonen, dass die Bildung von Komposita weiterhin von rechts nach links gelesen wird:

(14.12) Beispiel.

(a) In S_3 gilt

$$(1,3)(1,2) = (1,2,3).$$

(b) Die Permutation $\left(\begin{smallmatrix}1&2&3&4&5\\2&3&1&5&4\end{smallmatrix}\right)$ in S_5 ist kein Zykel. Es gilt

$$\left(\begin{smallmatrix}1&2&3&4&5\\2&3&1&5&4\end{smallmatrix}\right) = (4,5)(1,2,3) = (1,2,3)(4,5).$$

Beweis.

(a) Es seien $\zeta, \eta \in \mathrm{S}_3$ gegeben durch $\zeta = (1,2)$, $\eta = (1,3)$. Dann gilt

$$\begin{aligned}\eta(\zeta(1)) &= \eta(2) = 2,\\ \eta(\zeta(2)) &= \eta(1) = 3,\\ \eta(\zeta(3)) &= \eta(3) = 1,\end{aligned}$$

also

$$\eta\zeta = (1,3)(1,2) = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right) = (1,2,3).$$

(b) Es seien $\zeta, \eta \in \mathrm{S}_5$ gegeben durch $\zeta = (1,2,3)$, $\eta = (4,5)$. Dann gilt

$$\begin{aligned}\eta(\zeta(1)) &= \eta(2) = 2,\\ \eta(\zeta(2)) &= \eta(3) = 3,\\ \eta(\zeta(3)) &= \eta(1) = 1,\\ \eta(\zeta(4)) &= \eta(4) = 5,\\ \eta(\zeta(5)) &= \eta(5) = 4,\end{aligned}$$

und

$$\begin{aligned}\zeta(\eta(1)) &= \zeta(1) = 2,\\ \zeta(\eta(2)) &= \zeta(2) = 3,\\ \zeta(\eta(3)) &= \zeta(3) = 1,\\ \zeta(\eta(4)) &= \zeta(5) = 5,\\ \zeta(\eta(5)) &= \zeta(4) = 4,\end{aligned}$$

also

$$(4,5)(1,2,3) = \eta\zeta = \left(\begin{smallmatrix}1&2&3&4&5\\2&3&1&5&4\end{smallmatrix}\right) = \zeta\eta = (1,2,3)(4,5).$$ □

Die Schreibweise eines Zykels ist nicht eindeutig, sondern hängt von der Wahl eines Vertreters der zugehörigen Bahn (der erste Eintrag in einem Zykel) ab:

(14.13) Beispiel. In S_4 gilt

$$(1,3,4,2) = (3,4,2,1) = (4,2,1,3) = (2,1,3,4).$$

(14.14) Proposition. Es seien eine endliche Menge X, $\pi \in \mathrm{S}_X$ und eine Transversale T der Bahnen unter π gegeben. Für $x \in T$ sei ferner $m_x := \min\{k \in \mathbb{N} \mid \pi^k(x) = x\}$. Dann ist

$$\pi = \prod_{x \in T} (x, \pi(x), \ldots, \pi^{m_x - 1}(x)) = \prod_{\substack{x \in T \\ \pi(x) \neq x}} (x, \pi(x), \ldots, \pi^{m_x - 1}(x)).$$

Beweis. Für $x \in T$ sei $m_x := \min\{k \in \mathbb{N} \mid \pi^k(x) = x\}$ und $\zeta_x := (x, \pi(x), \ldots, \pi^{m_x - 1}(x))$. Für $y \in X$ gilt dann

$$\zeta_x(y) = \begin{cases}\pi(y), & \text{falls } y \in [x]_\pi,\\ y, & \text{falls } y \notin [x]_\pi.\end{cases}$$

Zunächst seien $x, x' \in T$ mit $x \neq x'$ gegeben. Dann sind $[x]_\pi$ und $[x']_\pi$ disjunkt, d.h. für $y \in X$ gilt entweder $y \in [x]_\pi$ oder $y \in [x']_\pi$ oder $y \notin [x]_\pi \,\dot\cup\, [x']_\pi$ und somit

$$\zeta_{x'}(\zeta_x(y)) = \left.\begin{cases}\zeta_{x'}(\pi(y)), & \text{falls } y \in [x]_\pi,\\ \zeta_{x'}(y), & \text{falls } y \notin [x]_\pi\end{cases}\right\} = \left\{\begin{cases}\pi(y), & \text{falls } y \in [x]_\pi,\\ \pi(y), & \text{falls } y \in [x']_\pi,\\ y, & \text{falls } y \notin [x]_\pi \,\dot\cup\, [x']_\pi\end{cases}\right\}$$

$$= \left.\begin{cases} \zeta_x(\pi(y)), & \text{falls } y \in [x']_\pi, \\ \zeta_x(y), & \text{falls } y \notin [x']_\pi \end{cases}\right\} = \zeta_x(\zeta_{x'}(y)).$$

Folglich gilt $\zeta_{x'}\zeta_x = \zeta_x\zeta_{x'}$ in S_X.
Um $\pi = \prod_{x\in T} \zeta_x$ zu zeigen, sei $y \in X$ gegeben. Da T eine Transversale der Bahnen unter π ist, gibt es genau ein $x' \in T$ mit $y \in [x']_\pi$. Es gilt $\zeta_{x'}(y) = \pi(y)$ und damit

$$(\prod_{x\in T} \zeta_x)(y) = (\prod_{x\in T\setminus\{x'\}} \zeta_x)(\zeta_{x'}(y)) = (\prod_{x\in T\setminus\{x'\}} \zeta_x)(\pi(y)) = \pi(y).$$

Folglich ist in der Tat $\pi = \prod_{x\in T} \zeta_x$.
Da $\zeta_x = \mathrm{id}_X$ für alle $x \in T$ mit $\pi(x) = x$ ist, folgt

$$\pi = \prod_{x\in T} \zeta_x = \prod_{\substack{x\in T \\ \pi(x)\neq x}} \zeta_x. \qquad \square$$

Die in Proposition (14.14) verwendete Darstellung wird Zykelschreibweise genannt. Es lässt sich zeigen, dass sich jede Permutation einer endlichen Menge (bis auf Reihenfolge) eindeutig als Kompositum von paarweise disjunkten nicht-trivialen Zykeln schreiben lässt. Dabei heißt ein Zykel *nicht-trivial*, falls er mindestens Länge 2 hat, und zwei nicht-triviale Zykel heißen *disjunkt*, falls die zugehörigen eindeutigen nicht-einelementigen Bahnen disjunkt sind.

(14.15) Beispiel. In S_7 ist

$$\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 3 & 1 & 7 & 6 & 5 \end{smallmatrix}\right) = (1,2,4)(5,7).$$

Transpositionen

Die Zykel der Länge 2 bilden die „Grundbausteine“ in der symmetrischen Gruppe S_n für $n \in \mathbb{N}_0$, wie wir im Folgenden sehen werden.

(14.16) Definition (Transposition, Nachbartransposition)**.**

(a) Es sei $n \in \mathbb{N}_0$ gegeben. Eine *Transposition* (oder *Vertauschung*) von $[1,n]$ ist ein Zykel von $[1,n]$ der Länge 2.

(b) Es sei $n \in \mathbb{N}$ gegeben. Eine *Nachbartransposition* von $[1,n]$ ist eine Transposition von $[1,n]$ der Form $(j, j+1)$ für ein $j \in [1, n-1]$.

(14.17) Bemerkung. Es sei $n \in \mathbb{N}_0$ gegeben. Für verschiedene $i, j, k \in [1,n]$ gilt

$$(i,j) = (j,k)(i,k)(k,j)$$

in S_n.

(14.18) Bemerkung. Es sei $n \in \mathbb{N}_0$ gegeben.

(a) Es sei $l \in \mathbb{N}_0$ gegeben. Für verschiedene $j_1, \ldots, j_l \in [1,n]$ gilt

$$(j_1, \ldots, j_l) = (j_1, j_l)(j_1, j_{l-1}) \ldots (j_1, j_2) = (j_1, j_2)(j_2, j_3) \ldots (j_{l-1}, j_l)$$

in S_n.

(b) Für $i, j \in [1,n]$ mit $i < j$ gilt

$$(i,j) = (j, j-1) \ldots (i+2, i+1)(i, i+1)(i+1, i+2) \ldots (j-1, j).$$

Beweis.

(b) Es sei $i \in [1,n]$ gegeben. Wir führen Induktion nach $j \in [i+1,n]$, wobei für $j = i+1$ nichts zu tun ist. Es sei also $j \in [i+2,n]$ mit

$$(i,j-1) = (j-1,j-2)\dots(i+2,i+1)(i,i+1)(i+1,i+2)\dots(j-2,j-1)$$

gegeben. Dann ist nach Bemerkung (14.17) aber auch

$$\begin{aligned}(i,j) &= (j,j-1)(i,j-1)(j-1,j)\\ &= (j,j-1)(j-1,j-2)\dots(i+2,i+1)(i,i+1)(i+1,i+2)\dots(j-2,j-1)(j-1,j).\end{aligned}$$

Nach dem Induktionsprinzip gilt

$$(i,j) = (j,j-1)\dots(i+2,i+1)(i,i+1)(i+1,i+2)\dots(j-1,j)$$

für alle $j \in [i+1,n]$. □

(14.19) Beispiel.

(a) In S_9 ist

$$(1,4,7,3,5)(2,8,6,9) = (1,4)(4,7)(7,3)(3,5)(2,8)(8,6)(6,9).$$

(b) In S_9 ist

$$(1,4) = (4,3)(3,2)(1,2)(2,3)(3,4).$$

(14.20) Proposition. Es sei $n \in \mathbb{N}_0$ gegeben. Jede Permutation von $[1,n]$ ist ein Kompositum von Nachbartranspositionen von $[1,n]$.

Beweis. Dies folgt aus Proposition (14.14) und Bemerkung (14.18). □

Signum

Die Darstellung einer Permutation als Kompositum von Transpositionen ist nicht eindeutig, wie man bereits an Bemerkung (14.18) erkennt. Wir werden jedoch zeigen, dass zumindest die Parität der Anzahl der Transpositionen festgelegt ist: Lässt sich eine Permutation als ein Kompositum einer geraden Anzahl an Permutationen schreiben, dann nicht als ein Kompositum einer ungeraden Anzahl an Permutationen (und umgekehrt).
Um dies zu zeigen, zählen wir diejenigen Paare, bei welchen unter einer Permutation die Ordnungsbeziehung vertauscht wird.

(14.21) Definition (Fehlstand)**.** Es seien $n \in \mathbb{N}_0$ und $\pi \in S_n$ gegeben. Die *Menge der Fehlstände* von π ist definiert als

$$\mathrm{Inv}(\pi) := \{(i,j) \in [1,n] \times [1,n] \mid i < j,\ \pi(i) > \pi(j)\}.$$

Ein Element von $\mathrm{Inv}(\pi)$ wird *Fehlstand* (oder *Inversionspaar*) von π genannt.

(14.22) Beispiel. Es ist

$$\mathrm{Inv}(\left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right)) = \{(1,3),(1,4),(2,3),(2,4)\}.$$

(14.23) Bemerkung. Es seien $n \in \mathbb{N}$ und $j \in [1,n-1]$ gegeben.

(a) Es ist

$$\mathrm{Inv}((j,j+1)) = \{(j,j+1)\}.$$

(b) Für $\pi \in \mathrm{S}_n$ ist

$$\begin{aligned}\mathrm{Inv}(\pi \circ (j, j+1)) = \{(i, i') \mid i, i' \in [1, n] \setminus \{j, j+1\} \text{ mit } (i, i') \in \mathrm{Inv}(\pi)\} \\ \dot\cup \{(i, j+1) \mid i \in [1, j-1] \text{ mit } (i, j) \in \mathrm{Inv}(\pi)\} \\ \dot\cup \{(j+1, i) \mid i \in [j+2, n] \text{ mit } (j, i) \in \mathrm{Inv}(\pi)\} \\ \dot\cup \{(i, j) \mid i \in [1, j-1] \text{ mit } (i, j+1) \in \mathrm{Inv}(\pi)\} \\ \dot\cup \{(j, i) \mid i \in [j+2, n] \text{ mit } (j+1, i) \in \mathrm{Inv}(\pi)\} \dot\cup S,\end{aligned}$$

wobei

$$S = \begin{cases}\{(j, j+1)\}, & \text{falls } (j, j+1) \notin \mathrm{Inv}(\pi), \\ \emptyset, & \text{falls } (j, j+1) \in \mathrm{Inv}(\pi).\end{cases}$$

Beweis.

(b) Es sei $\pi \in \mathrm{S}_n$ gegeben und es sei $\sigma := \pi \circ (j, j+1)$. Für $i \in [1, n]$ ist

$$\sigma(i) = \begin{cases}\pi(j+1), & \text{falls } i = j, \\ \pi(j), & \text{falls } i = j+1, \\ \pi(i), & \text{falls } i \notin \{j, j+1\}.\end{cases}$$

Folglich gilt: Für $i, i' \in [1, n] \setminus \{j, j+1\}$ ist genau dann $(i, i') \in \mathrm{Inv}(\sigma)$, wenn $(i, i') \in \mathrm{Inv}(\pi)$. Für $i \in [1, j-1]$ ist genau dann $(i, j+1) \in \mathrm{Inv}(\sigma)$, wenn $(i, j) \in \mathrm{Inv}(\pi)$. Für $i \in [j+2, n]$ ist genau dann $(j+1, i) \in \mathrm{Inv}(\sigma)$, wenn $(j, i) \in \mathrm{Inv}(\pi)$. Für $i \in [1, j-1]$ ist genau dann $(i, j) \in \mathrm{Inv}(\sigma)$, wenn $(i, j+1) \in \mathrm{Inv}(\pi)$. Für $i \in [j+2, n]$ ist genau dann $(j, i) \in \mathrm{Inv}(\sigma)$, wenn $(j+1, i) \in \mathrm{Inv}(\pi)$. Genau dann ist $(j, j+1) \in \mathrm{Inv}(\sigma)$, wenn $(j, j+1) \notin \mathrm{Inv}(\pi)$. □

(14.24) Definition (Signum)**.** Es seien $n \in \mathbb{N}_0$ und $\pi \in \mathrm{S}_n$ gegeben. Das *Signum* (oder *Vorzeichen*) von π ist definiert als

$$\operatorname{sgn} \pi := (-1)^{|\mathrm{Inv}(\pi)|}.$$

Das Signum von Permutationen wird in der Linearen Algebra zur Definition der Determinante benutzt.

(14.25) Beispiel. Es ist

$$\operatorname{sgn} \left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right) = 1.$$

Beweis. Nach Beispiel (14.22) ist

$$\mathrm{Inv}\left(\left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right)\right) = \{(1,3), (1,4), (2,3), (2,4)\},$$

also

$$\operatorname{sgn} \left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right) = (-1)^4 = 1.$$ □

(14.26) Bemerkung. Es sei $n \in \mathbb{N}_0$ gegeben. Für $j \in [1, n-1]$ ist

$$\operatorname{sgn} (j, j+1) = -1.$$

Beweis. Nach Bemerkung (14.23)(a) ist $\mathrm{Inv}((j, j+1)) = \{(j, j+1)\}$ und damit

$$\operatorname{sgn} (j, j+1) = (-1)^{|\mathrm{Inv}((j, j+1))|} = (-1)^1 = -1.$$

für $j \in [1, n-1]$. □

(14.27) Proposition (Produktsatz)**.** Es sei $n \in \mathbb{N}_0$ gegeben. Für $\pi, \sigma \in \mathrm{S}_n$ gilt

$$\operatorname{sgn}(\pi \circ \sigma) = (\operatorname{sgn} \pi)(\operatorname{sgn} \sigma).$$

Beweis. Wir zeigen durch Induktion nach $l \in \mathbb{N}_0$: Für $\pi, \sigma \in \mathrm{S}_n$ so, dass σ ein Kompositum von l Nachbartranspositionen ist, gilt $\operatorname{sgn}(\pi \circ \sigma) = (\operatorname{sgn}\pi)(\operatorname{sgn}\sigma)$.
Für $l = 0$, $\pi, \sigma \in \mathrm{S}_n$ so, dass σ ein Kompositum von l Nachbartranspositionen ist, gilt $\sigma = \mathrm{id}_{[1,n]}$, also

$$\operatorname{sgn}(\pi \circ \sigma) = \operatorname{sgn}(\pi \circ \mathrm{id}_{[1,n]}) = \operatorname{sgn}\pi = \operatorname{sgn}\pi \cdot 1 = (\operatorname{sgn}\pi)(\operatorname{sgn}\mathrm{id}_{[1,n]}) = (\operatorname{sgn}\pi)(\operatorname{sgn}\sigma).$$

Es sei also $l \in \mathbb{N}$ so gegeben, dass $\operatorname{sgn}(\pi \circ \sigma') = (\operatorname{sgn}\pi)(\operatorname{sgn}\sigma')$ für $\pi, \sigma' \in \mathrm{S}_n$ derart, dass σ' ein Kompositum von $l-1$ Nachbartransposition ist. Ferner seien $\pi, \sigma \in \mathrm{S}_n$ so gegeben, dass σ ein Kompositum von l Nachbartranspositionen ist. Dann ist $\sigma = \sigma' \circ (j, j+1)$ für ein $\sigma' \in \mathrm{S}_n$, welches ein Kompositum von $l-1$ Nachbartranspositionen ist, und ein $j \in [1, n-1]$. Für $\rho \in \mathrm{S}_n$ gilt

$$|\operatorname{Inv}(\rho \circ (j, j+1))| = \begin{cases} |\operatorname{Inv}(\rho)| + 1, & \text{falls } (j, j+1) \notin \operatorname{Inv}(\rho), \\ |\operatorname{Inv}(\rho)| - 1, & \text{falls } (j, j+1) \in \operatorname{Inv}(\rho), \end{cases}$$

nach Bemerkung (14.23)(b) und damit

$$\begin{aligned} \operatorname{sgn}(\rho \circ (j, j+1)) = (-1)^{|\operatorname{Inv}(\rho \circ (j,j+1))|} &= \left.\begin{cases} (-1)^{|\operatorname{Inv}(\rho)|+1}, & \text{falls } (j, j+1) \notin \operatorname{Inv}(\rho), \\ (-1)^{|\operatorname{Inv}(\rho)|-1}, & \text{falls } (j, j+1) \in \operatorname{Inv}(\rho) \end{cases}\right\} = (-1)^{|\operatorname{Inv}(\rho)|} \cdot (-1) \\ &= (\operatorname{sgn}\rho)(\operatorname{sgn}(j, j+1)) \end{aligned}$$

nach Bemerkung (14.26). Mit der Induktionsvoraussetzung ergibt sich

$$\begin{aligned} \operatorname{sgn}(\pi \circ \sigma) &= \operatorname{sgn}(\pi \circ \sigma' \circ (j, j+1)) = (\operatorname{sgn}(\pi \circ \sigma'))(\operatorname{sgn}(j, j+1)) = (\operatorname{sgn}\pi)(\operatorname{sgn}\sigma')(\operatorname{sgn}(j, j+1)) \\ &= (\operatorname{sgn}\pi)(\operatorname{sgn}(\sigma' \circ (j, j+1))) = (\operatorname{sgn}\pi)(\operatorname{sgn}\sigma). \end{aligned}$$

Nach dem Induktionsprinzip und Proposition (14.20) gilt $\operatorname{sgn}(\pi \circ \sigma) = (\operatorname{sgn}\pi)(\operatorname{sgn}\sigma)$ für alle $\pi, \sigma \in \mathrm{S}_n$. □

(14.28) Korollar. Es sei $n \in \mathbb{N}_0$ gegeben. Für $\pi \in \mathrm{S}_n$ ist

$$\operatorname{sgn}\pi^{-1} = \operatorname{sgn}\pi.$$

Beweis. Es sei $\pi \in \mathrm{S}_n$ gegeben. Nach Proposition (14.27) gilt dann

$$(\operatorname{sgn}\pi^{-1})(\operatorname{sgn}\pi) = \operatorname{sgn}(\pi^{-1} \circ \pi) = \operatorname{sgn}\mathrm{id}_{[1,n]} = 1$$

und damit

$$\operatorname{sgn}\pi^{-1} = (\operatorname{sgn}\pi)^{-1} = \left.\begin{cases} 1^{-1}, & \text{falls } \operatorname{sgn}\pi = 1, \\ (-1)^{-1}, & \text{falls } \operatorname{sgn}\pi = -1 \end{cases}\right\} = \left.\begin{cases} 1, & \text{falls } \operatorname{sgn}\pi = 1, \\ -1, & \text{falls } \operatorname{sgn}\pi = -1 \end{cases}\right\} = \operatorname{sgn}\pi.$$ □

(14.29) Satz. Es seien $n \in \mathbb{N}_0$ und $\pi \in \mathrm{S}_n$ gegeben und es sei $\mathcal{O} := [1, n]/\pi$. Dann ist

$$\operatorname{sgn}\pi = (-1)^{\sum_{O \in \mathcal{O}}(|O|-1)} = (-1)^{\sum_{O \in \mathcal{O}, |O|>1}(|O|-1)} = (-1)^{n-|\mathcal{O}|} = (-1)^{|\{O \in \mathcal{O} \mid |O| \text{ ist gerade}\}|}.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(14.30) Beispiel. Für $(1,4,6)(3,8,5)(7,9) \in \mathrm{S}_9$ gilt

$$\operatorname{sgn}((1,4,6)(3,8,5)(7,9)) = -1.$$

Beweis. Es ist $\{O \in [1,9]/\pi \mid |O| > 1\} = \{\{1,4,6\}, \{3,8,5\}, \{7,9\}\}$. Nach Satz (14.29) folgt

$$\operatorname{sgn}((1,4,6)(3,8,5)(7,9)) = (-1)^{(3-1)+(3-1)+(2-1)} = (-1)^{2+2+1} = (-1)^5 = -1.$$ □

Alternativer Beweis von Beispiel (14.30). Es ist $[1,9]/\pi = \{\{1,4,6\}, \{2\}, \{3,8,5\}, \{7,9\}\}$. Nach Satz (14.29) folgt

$$\operatorname{sgn}((1,4,6)(3,8,5)(7,9)) = (-1)^{9-4} = (-1)^5 = -1.$$ □

Alternativer Beweis von Beispiel (14.30). Es ist $\{O \in [1,9]/\pi \mid |O| \text{ ist gerade}\} = \{\{7,9\}\}$. Nach Satz (14.29) folgt

$$\operatorname{sgn}((1,4,6)(3,8,5)(7,9)) = (-1)^1 = -1.$$ □

Zusätzliche Konzepte

Im Folgenden geben wir einige zusätzliche Definitionen, deren Studium dem Leser zur Übung überlassen sei.

(14.31) Definition (Ordnung)**.** Es seien eine Menge X und eine Permutation π von X gegeben. Die *Ordnung* von π ist definiert als

$$\operatorname{ord}\pi := \min\{k \in \mathbb{N} \mid \pi^k = \mathrm{id}_X\}.$$

(14.32) Definition (Fixpunkte, Träger)**.** Es seien eine Menge X und eine Permutation π von X gegeben.

(a) Die *Menge der Fixpunkte* unter π ist definiert als

$$\mathrm{Fix}(\pi) := \{x \in X \mid \pi(x) = x\}.$$

Ein Element von $\mathrm{Fix}(\pi)$ wird *Fixpunkt* unter π genannt.

(b) Der *Träger* von π ist definiert als

$$\mathrm{Supp}(\pi) := \{x \in X \mid \pi(x) \neq x\}.$$

Für $x \in \mathrm{Supp}(\pi)$ sagen wir, dass x unter π *bewegt* wird.

15 Matrixarithmetik

Bereits in Definition (2.52) wurde der Begriff einer Matrix als Spezialisierung des Begriffs einer Familie eingeführt. In diesem Abschnitt betrachten wir Matrizen mit Einträgen in einem gegebenen kommutativen Ring und führen für solche diverse Matrixoperationen ein.
Im Folgenden, bis zum Ende des Abschnitts und unter Ausnahme der Beispiele, sei stets ein kommutativer Ring R gegeben.

Matrixaddition

Falls nicht anders erwähnt, fassen wir ohne weiteren Kommentar für $m, n \in \mathbb{N}_0$ die Menge der $(m \times n)$-Matrizen über R als abelsche Gruppe im folgenden Sinne auf.

(15.1) Proposition. Es seien $m, n \in \mathbb{N}_0$ gegeben. Die Menge $R^{m\times n}$ wird eine abelsche Gruppe mit Addition gegeben durch

$$A +^{R^{m\times n}} B = (A_{i,j} +^R B_{i,j})_{i\in[1,m],j\in[1,n]}$$

für $A, B \in R^{m\times n}$. Die Null von $R^{m\times n}$ ist gegeben durch

$$0^{R^{m\times n}} = (0^R)_{i\in[1,m],j\in[1,n]}.$$

Für $A \in R^{m\times n}$ ist das Negative von A in $R^{m\times n}$ gegeben durch

$$(-A)^{R^{m\times n}} = ((-A_{i,j})^R)_{i\in[1,m],j\in[1,n]}.$$

Beweis. Wir verifizieren die Axiome einer abelschen Gruppe.

- *Assoziativität der Addition.* Für $A, B, C \in R^{m\times n}$ gilt

$$\begin{aligned} A + (B + C) &= A + (B_{i,j} + C_{i,j})_{i\in[1,m],j\in[1,n]} = (A_{i,j} + (B_{i,j} + C_{i,j}))_{i\in[1,m],j\in[1,n]} \\ &= ((A_{i,j} + B_{i,j}) + C_{i,j})_{i\in[1,m],j\in[1,n]} = (A_{i,j} + B_{i,j})_{i\in[1,m],j\in[1,n]} + C \\ &= (A + B) + C. \end{aligned}$$

  Folglich ist $+$ assoziativ.

- *Kommutativität der Addition.* Für $A, B \in R^{m\times n}$ gilt

$$A + B = (A_{i,j} + B_{i,j})_{i\in[1,m],j\in[1,n]} = (B_{i,j} + A_{i,j})_{i\in[1,m],j\in[1,n]} = B + A.$$

  Folglich ist + kommutativ.

- *Existenz der Null.* Für $A \in R^{m\times n}$ gilt

$$(0)_{i\in[1,m],j\in[1,n]} + A = (0 + A_{i,j})_{i\in[1,m],j\in[1,n]} = (A_{i,j})_{i\in[1,m],j\in[1,n]} = A.$$

  Wegen der Kommutativität von + ist $(0)_{i\in[1,m],j\in[1,n]}$ ein neutrales Element in $R^{m\times n}$ bzgl. +.

- *Existenz der Negativen.* Für $A \in R^{m\times n}$ gilt

$$(-A_{i,j})_{i\in[1,m],j\in[1,n]} + A = (-A_{i,j} + A_{i,j})_{i\in[1,m],j\in[1,n]} = (0)_{i\in[1,m],j\in[1,n]}.$$

  Wegen der Kommutativität von + ist $(-A_{i,j})_{i\in[1,m],j\in[1,n]}$ ein zu A inverses Element in $R^{m\times n}$ bzgl. +.

Insgesamt wird $R^{m\times n}$ eine abelsche Gruppe mit Addition gegeben durch $A + B = (A_{i,j} + B_{i,j})_{i\in[1,m],j\in[1,n]}$ für $A, B \in R^{m\times n}$, Null $0 = (0)_{i\in[1,m],j\in[1,n]}$ und Negativen $-A = (-A_{i,j})_{i\in[1,m],j\in[1,n]}$ für $A \in R^{m\times n}$. □

(15.2) Definition (Matrixaddition)**.** Es seien $m, n \in \mathbb{N}_0$ gegeben. Für $A, B \in R^{m\times n}$ wird $A + B$ gegeben wie in Proposition (15.1) die *Summe* (oder *Matrixsumme*) von A und B genannt. Die Null von $R^{m\times n}$ wird auch *Nullmatrix* (genauer $(m \times n)$*-Nullmatrix*) über R genannt. Für $A \in R^{m\times n}$ wird das Negative von A auch die *negative Matrix* von A genannt.

Bei den in Definition (15.2) eingeführten Begriffen handelt es sich um *komponentenweise* definierte Konzepte; wir sprechen von einer *komponentenweisen Addition*, einer *komponentenweisen Null* und *komponentenweisen Negativen.*

(15.3) Beispiel.

(a) In $\mathbb{Z}^{2\times 3}$ ist

$$\begin{pmatrix} 1 & 0 & -2 \\ 2 & -1 & 3 \end{pmatrix} + \begin{pmatrix} -2 & 2 & 4 \\ 1 & 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 2 & 2 \\ 3 & 0 & 2 \end{pmatrix}.$$

(b) In $\mathbb{Z}^{2\times 3}$ ist

$$0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

(c) In $\mathbb{Z}^{2\times 3}$ ist

$$-\begin{pmatrix} 1 & 0 & -2 \\ 2 & -1 & 3 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 2 \\ -2 & 1 & -3 \end{pmatrix}.$$

Beweis.

(a) In $\mathbb{Z}^{2\times 3}$ ist

$$\begin{pmatrix} 1 & 0 & -2 \\ 2 & -1 & 3 \end{pmatrix} + \begin{pmatrix} -2 & 2 & 4 \\ 1 & 1 & -1 \end{pmatrix} = \begin{pmatrix} 1-2 & 0+2 & -2+4 \\ 2+1 & -1+1 & 3-1 \end{pmatrix} = \begin{pmatrix} -1 & 2 & 2 \\ 3 & 0 & 2 \end{pmatrix}.$$

(c) In $\mathbb{Z}^{2\times 3}$ ist

$$-\begin{pmatrix} 1 & 0 & -2 \\ 2 & -1 & 3 \end{pmatrix} = \begin{pmatrix} -1 & -0 & -(-2) \\ -2 & -(-1) & -3 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 2 \\ -2 & 1 & -3 \end{pmatrix}.$$ □

Skalarmultiplikation von Matrizen

Matrizen lassen sich nicht nur addieren, sondern auch mit Elementen aus R multiplizieren. Diese sogenannte Skalarmultiplikation geschieht wieder komponentenweise:

(15.4) Definition (Skalarmultiplikation von Matrizen)**.** Es seien $m, n \in \mathbb{N}_0$ gegeben. Für $c \in R$, $A \in R^{m\times n}$ wird $cA = c \cdot A \in R^{m\times n}$ gegeben durch

$$cA = (cA_{i,j})_{i\in[1,m],j\in[1,n]}$$

das *c-fache* von A genannt.

(15.5) Beispiel. In $\mathbb{Z}^{2\times 3}$ ist

$$(-3)\begin{pmatrix}1 & 0 & -2\\ 2 & -1 & 3\end{pmatrix} = \begin{pmatrix}-3 & 0 & 6\\ -6 & 3 & -9\end{pmatrix}.$$

Beweis. In $\mathbb{Z}^{2\times 3}$ ist

$$(-3)\begin{pmatrix}1 & 0 & -2\\ 2 & -1 & 3\end{pmatrix} = \begin{pmatrix}(-3)\cdot 1 & (-3)\cdot 0 & (-3)\cdot(-2)\\ (-3)\cdot 2 & (-3)\cdot(-1) & (-3)\cdot 3\end{pmatrix} = \begin{pmatrix}-3 & 0 & 6\\ -6 & 3 & -9\end{pmatrix}. \qquad \square$$

(15.6) Konvention. Meistens lassen wir die Klammern um Produkte aus Skalaren und Matrizen weg, d.h. es gelte *Punkt- vor Strichrechnung.*

(15.7) Proposition. Es seien $m, n \in \mathbb{N}_0$ gegeben.

(a) *Assoziativität der Skalarmultiplikation.* Für $c, d \in R$, $A \in R^{m\times n}$ gilt

$$c(dA) = (cd)A.$$

(b) *Neutralität der Eins bzgl. der Skalarmultiplikation.* Für $A \in R^{m\times n}$ gilt

$$1A = A.$$

(c) *Distributivität von Matrixaddition und Skalarmultiplikation.* Für $c, d \in R$, $A \in R^{m\times n}$ gilt

$$(c + d)A = cA + dA.$$

Für $c \in R$, $A, B \in R^{m\times n}$ gilt

$$c(A + B) = cA + cB.$$

Beweis.

(a) Für $c, d \in R$, $A \in R^{m\times n}$ gilt

$$c(dA) = c\,(dA_{i,j})_{i\in[1,m],j\in[1,n]} = (c(dA_{i,j}))_{i\in[1,m],j\in[1,n]} = ((cd)A_{i,j})_{i\in[1,m],j\in[1,n]} = (cd)A.$$

(b) Für $A \in R^{m\times n}$ gilt

$$1A = (1A_{i,j})_{i\in[1,m],j\in[1,n]} = (A_{i,j})_{i\in[1,m],j\in[1,n]} = A.$$

(c) Für $c, d \in R$, $A \in R^{m\times n}$ gilt

$$\begin{aligned}(c + d)A &= ((c + d)A_{i,j})_{i\in[1,m],j\in[1,n]} = (cA_{i,j} + dA_{i,j})_{i\in[1,m],j\in[1,n]}\\ &= (cA_{i,j})_{i\in[1,m],j\in[1,n]} + (dA_{i,j})_{i\in[1,m],j\in[1,n]} = cA + dA.\end{aligned}$$

Für $c \in R$, $A, B \in R^{m\times n}$ gilt

$$\begin{aligned}c(A + B) &= c(A_{i,j} + B_{i,j})_{i\in[1,m],j\in[1,n]} = (c(A_{i,j} + B_{i,j}))_{i\in[1,m],j\in[1,n]} = (cA_{i,j} + cB_{i,j})_{i\in[1,m],j\in[1,n]}\\ &= (cA_{i,j})_{i\in[1,m],j\in[1,n]} + (cB_{i,j})_{i\in[1,m],j\in[1,n]} = cA + cB.\end{aligned} \qquad \square$$

(15.8) Konvention. Es seien $m, n \in \mathbb{N}_0$ gegeben. Da für $c, d \in R$, $A \in R^{m\times n}$ stets $c(dA) = (cd)A$ gilt, schreiben wir im Folgenden meist kurz $cdA := c(dA) = (cd)A$.

Matrixmultiplikation

Schließlich werden wir auch noch eine Multiplikation von Matrizen definieren. Im Gegensatz zur Addition und Skalarmultiplikation von Matrizen wird diese nicht komponentenweise definiert sein, sondern etwas komplizierter. Es werden nicht alle Matrizen miteinander multipliziert werden können, im Allgemeinen auch nicht alle solche vom selben Format. Eine komponentenweise Multiplikation (von Matrizen vom selben Format) könnten wir natürlich auch definieren und studieren, allerdings würde eine solche Multiplikation weniger nützliche Ergebnisse liefern als die im Folgenden definierte Matrixmultiplikation.

(15.9) Definition (Matrixmultiplikation)**.**

(a) Es seien $m, n, p \in \mathbb{N}_0$ gegeben. Für $A \in R^{m\times n}$, $B \in R^{n\times p}$ wird $AB = A \cdot B \in R^{m\times p}$ gegeben durch

$$AB = \Big(\sum_{j\in[1,n]} A_{i,j}B_{j,k}\Big)_{i\in[1,m],k\in[1,p]}$$

das *Matrixprodukt* von A und B genannt.

(b) Es sei $n \in \mathbb{N}_0$ gegeben. Die Matrix $\mathrm{E}_n \in R^{n\times n}$ gegeben durch

$$\mathrm{E}_n = (\delta_{i,j})_{i,j\in[1,n]}$$

wird *Einheitsmatrix* (genauer *n-te Einheitsmatrix* oder *n-te Identitätsmatrix*) über R genannt.

Das Matrixprodukt AB von Matrizen A und B über R ist somit nur definiert, falls die Anzahl der Spalten von A gleich der Anzahl der Zeilen von B ist. Um den Eintrag an einer Stelle (i, k) von AB zu berechnen, müssen wir die i-te Zeile $A_{i,-}$ von A und die k-te Spalte $B_{-,k}$ von B betrachten. Dann bilden wir die Produkte $A_{i,j}B_{j,k}$ für alle j, d.h. wir gehen $A_{i,-}$ von links nach rechts und $B_{-,k}$ von oben nach unten durch und bilden $A_{i,1}B_{1,k}$, $A_{i,2}B_{2,k}$, usw. Die Summe all dieser Produkte ist dann gerade der Eintrag von AB an der Stelle (i, k).

(15.10) Beispiel.

(a) Über $\mathbb{Z}$ ist

$$\begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & 0 \\ 2 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & -1 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} -2 & 4 \\ 1 & 2 \\ 0 & 7 \\ -1 & -3 \end{pmatrix}.$$

(b) In $\mathbb{Z}^{3\times 3}$ ist

$$\mathrm{E}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Beweis.

(a) Es ist

$$\begin{aligned} \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & 0 \\ 2 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & -1 \\ -2 & 3 \end{pmatrix} &= \begin{pmatrix} 0\cdot 1 + (-1)\cdot 0 + 1\cdot(-2) & 0\cdot 2 + (-1)\cdot(-1) + 1\cdot 3 \\ 1\cdot 1 + 0\cdot 0 + 0\cdot(-2) & 1\cdot 2 + 0\cdot(-1) + 0\cdot 3 \\ 2\cdot 1 + 0\cdot 0 + 1\cdot(-2) & 2\cdot 2 + 0\cdot(-1) + 1\cdot 3 \\ (-1)\cdot 1 + 1\cdot 0 + 0\cdot(-2) & (-1)\cdot 2 + 1\cdot(-1) + 0\cdot 3 \end{pmatrix} \\ &= \begin{pmatrix} -2 & 4 \\ 1 & 2 \\ 0 & 7 \\ -1 & -3 \end{pmatrix}. \end{aligned}$$

□

(15.11) Konvention. Wir lassen die Klammern um Matrixprodukte meistens weg, d.h. es gelte *Punkt- vor Strichrechnung.*

(15.12) Proposition.

(a) *Assoziativität der Matrixmultiplikation.* Es seien $m, n, p, q \in \mathbb{N}_0$ gegeben. Für $A \in R^{m\times n}$, $B \in R^{n\times p}$, $C \in R^{p\times q}$ gilt

$$A(BC) = (AB)C.$$

(b) *Einselemente der Matrixmultiplikation.* Es seien $m, n \in \mathbb{N}_0$ gegeben. Für $A \in R^{m\times n}$ gilt

$$\mathrm{E}_m A = A\mathrm{E}_n = A.$$

(c) *Distributivität von Matrixaddition und Matrixmultiplikation.* Es seien $m, n, p \in \mathbb{N}_0$ gegeben. Für $A, A' \in R^{m\times n}$, $B \in R^{n\times p}$ gilt

$$(A + A')B = AB + A'B.$$

Für $A \in R^{m\times n}$, $B, B' \in R^{n\times p}$ gilt

$$A(B + B') = AB + AB'.$$

(d) *Distributivität von Skalarmultiplikation und Matrixmultiplikation.* Es seien $m, n, p \in \mathbb{N}_0$ gegeben. Für $c \in R$, $A \in R^{m\times n}$, $B \in R^{n\times p}$ gilt

$$(cA)B = A(cB) = c(AB).$$

Beweis.

(a) Für $A \in R^{m\times n}$, $B \in R^{n\times p}$, $C \in R^{p\times q}$ gilt

$$\begin{aligned}(A(BC))_{i,l} &= \sum_{j\in[1,n]} A_{i,j}(BC)_{j,l} = \sum_{j\in[1,n]} A_{i,j} \sum_{k\in[1,p]} B_{j,k}C_{k,l} = \sum_{j\in[1,n]} \sum_{k\in[1,p]} A_{i,j}B_{j,k}C_{k,l} \\ &= \sum_{k\in[1,p]} \Big(\sum_{j\in[1,n]} A_{i,j}B_{j,k}\Big)C_{k,l} = \sum_{k\in[1,p]} (AB)_{i,k}C_{k,l} = ((AB)C)_{i,l}\end{aligned}$$

für $i \in [1, m]$, $l \in [1, q]$ und damit $A(BC) = (AB)C$.

(b) Für $A \in R^{m\times n}$ gilt

$$\begin{aligned}(\mathrm{E}_m A)_{i,k} &= \sum_{j\in[1,n]} (\mathrm{E}_m)_{i,j}A_{j,k} = \sum_{j\in[1,n]} \delta_{i,j}A_{j,k} = A_{i,k}, \\ (A\mathrm{E}_n)_{i,k} &= \sum_{j\in[1,n]} A_{i,j}(\mathrm{E}_n)_{j,k} = \sum_{j\in[1,n]} A_{i,j}\delta_{j,k} = A_{i,k}\end{aligned}$$

für $i \in [1, m]$, $k \in [1, n]$ und damit $\mathrm{E}_m A = A\mathrm{E}_n = A$.

(c) Für $A, A' \in R^{m\times n}$, $B \in R^{n\times p}$ gilt

$$\begin{aligned}((A + A')B)_{i,k} &= \sum_{j\in[1,n]} (A + A')_{i,j}B_{j,k} = \sum_{j\in[1,n]} (A_{i,j} + A'_{i,j})B_{j,k} = \sum_{j\in[1,n]} A_{i,j}B_{j,k} + \sum_{j\in[1,n]} A'_{i,j}B_{j,k} \\ &= (AB)_{i,k} + (A'B)_{i,k} = (AB + A'B)_{i,k}\end{aligned}$$

für $i \in [1, m]$, $k \in [1, p]$ und damit $(A + A')B = AB + A'B$.

Für $A \in R^{m\times n}$, $B, B' \in R^{n\times p}$ gilt

$$\begin{aligned}(A(B + B'))_{i,k} &= \sum_{j\in[1,n]} A_{i,j}(B + B')_{j,k} = \sum_{j\in[1,n]} A_{i,j}(B_{j,k} + B'_{j,k}) = \sum_{j\in[1,n]} A_{i,j}B_{j,k} + \sum_{j\in[1,n]} A_{i,j}B'_{j,k} \\ &= (AB)_{i,k} + (AB')_{i,k} = (AB + AB')_{i,k}\end{aligned}$$

für $i \in [1, m]$, $k \in [1, p]$ und damit $A(B + B') = AB + AB'$.

(d) Für $c \in R$, $A \in R^{m\times n}$, $B \in R^{n\times p}$ gilt

$$((cA)B)_{i,k} = \sum_{j\in[1,n]} (cA)_{i,j}B_{j,k} = \sum_{j\in[1,n]} cA_{i,j}B_{j,k} = c\sum_{j\in[1,n]} A_{i,j}B_{j,k} = c\,(AB)_{i,k} = (c(AB))_{i,k},$$
$$(A(cB))_{i,k} = \sum_{j\in[1,n]} A_{i,j}(cB)_{j,k} = \sum_{j\in[1,n]} A_{i,j}\,cB_{j,k} = c\sum_{j\in[1,n]} A_{i,j}B_{j,k} = c\,(AB)_{i,k} = (c(AB))_{i,k}$$

für $i \in [1,m]$, $k \in [1,p]$ und damit $(cA)B = A(cB) = c(AB)$. □

(15.13) Korollar. Es sei $n \in \mathbb{N}_0$ gegeben. Die abelsche Gruppe $R^{n\times n}$ wird ein Ring mit Multiplikation gegeben durch die Matrixmultiplikation. Die Eins von $R^{n\times n}$ ist gegeben durch

$$1^{R^{n\times n}} = \mathrm{E}_n.$$

Beweis. Dies folgt aus Proposition (15.12)(a), (b), (c). □

Es sei $n \in \mathbb{N}_0$ gegeben. Wie in jedem Ring gibt es auch im Ring $R^{n\times n}$ den Begriff des invertierbaren Elements, vgl. Definition (6.25)(a): Ein $A \in R^{n\times n}$ ist invertierbar, falls ein $B \in R^{n\times n}$ mit $AB = BA = \mathrm{E}_n$ existiert. In diesem Fall ist das Inverse zu A eindeutig bestimmt und wird mit A^{-1} bezeichnet, vgl. Korollar (6.16) und Definition (6.25)(a). Die Gruppe der invertierbaren Elemente in $R^{n\times n}$ ist unter folgender Terminologie bekannt:

(15.14) Definition (allgemeine lineare Gruppe)**.** Es sei $n \in \mathbb{N}_0$ gegeben. Die Gruppe

$$\mathrm{GL}_n(R) := (R^{n\times n})^\times$$

heißt *allgemeine lineare Gruppe* (oder *volle lineare Gruppe*) vom Grad n über R. Ein Element von $\mathrm{GL}_n(R)$ wird *invertierbare* $(n \times n)$*-Matrix* über R genannt.

(15.15) Beispiel. Es sei $A \in \mathbb{Z}^{2\times 2}$ gegeben durch

$$A = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}.$$

Dann ist $A \in \mathrm{GL}_2(\mathbb{Z})$ mit

$$A^{-1} = \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}.$$

Beweis. Es ist

$$\begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$
$$\begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$ □

Mit dem Invertierbarkeitskriterium (16.28) werden wir im folgenden Abschnitt ein Verfahren kennenlernen, mit welchem wir eine gegebene Matrix auf Invertierbarkeit testen und ggf. ihr Inverses bestimmen können.

Transposition von Matrizen

Eine weitere häufig auftretende Operation auf Matrizen mit Einträgen in R ist die sogenannte Transposition:

(15.16) Definition (Transponierte)**.** Es seien $m, n \in \mathbb{N}_0$ und $A \in R^{m\times n}$ gegeben. Die Matrix $A^{\mathrm{tr}} \in R^{n\times m}$ gegeben durch

$$A^{\mathrm{tr}} = (A_{i,j})_{j\in[1,n],i\in[1,m]}$$

wird *Transponierte* von A (oder die *zu* A *transponierte Matrix*) genannt.

(15.17) Beispiel. Über $\mathbb{Z}$ ist

$$\begin{pmatrix} 1 & 0 & -2 \\ 2 & -1 & 3 \end{pmatrix}^{\mathrm{tr}} = \begin{pmatrix} 1 & 2 \\ 0 & -1 \\ -2 & 3 \end{pmatrix}.$$

(15.18) Proposition.

(a) Es seien $m, n, p \in \mathbb{N}_0$ gegeben. Für $A \in R^{m\times n}$, $B \in R^{n\times p}$ gilt

$$(AB)^{\mathrm{tr}} = B^{\mathrm{tr}} A^{\mathrm{tr}}.$$

(b) Es sei $n \in \mathbb{N}_0$ gegeben. Dann gilt

$$\mathrm{E}_n^{\mathrm{tr}} = \mathrm{E}_n.$$

(c) Es sei $n \in \mathbb{N}_0$ gegeben. Für $A \in \mathrm{GL}_n(R)$ ist auch $A^{\mathrm{tr}} \in \mathrm{GL}_n(R)$ mit

$$(A^{\mathrm{tr}})^{-1} = (A^{-1})^{\mathrm{tr}}.$$

(d) Es seien $m, n \in \mathbb{N}_0$ gegeben. Für $A, B \in R^{m\times n}$ gilt

$$(A + B)^{\mathrm{tr}} = A^{\mathrm{tr}} + B^{\mathrm{tr}}.$$

(e) Es seien $m, n \in \mathbb{N}_0$ gegeben. Für $c \in R$, $A \in R^{m\times n}$ gilt

$$(cA)^{\mathrm{tr}} = cA^{\mathrm{tr}}.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(15.19) Bemerkung. Es seien $m, n \in \mathbb{N}_0$ gegeben. Für $A \in R^{m\times n}$ gilt

$$(A^{\mathrm{tr}})^{\mathrm{tr}} = A.$$

Adjunktion von Matrizen

Eine leichte Modifikation der Transposition von Matrizen mit Einträgen in $\mathbb{C}$ ist die sogenannte Adjunktion.

(15.20) Definition (Adjungierte)**.** Es seien $m, n \in \mathbb{N}_0$ und $A \in \mathbb{C}^{m\times n}$ gegeben. Die Matrix $A^{\mathrm{ad}} \in \mathbb{C}^{n\times m}$ gegeben durch

$$A^{\mathrm{ad}} = (\overline{A_{i,j}})_{j\in[1,n],i\in[1,m]}$$

wird *Adjungierte* von A (oder die *zu A adjungierte Matrix*) genannt.

(15.21) Beispiel. Über $\mathbb{C}$ ist

$$\begin{pmatrix} 1+\mathrm{i} & -3\mathrm{i} & 2-2\mathrm{i} \\ 0 & -1+2\mathrm{i} & \mathrm{i} \end{pmatrix}^{\mathrm{ad}} = \begin{pmatrix} 1-\mathrm{i} & 0 \\ 3\mathrm{i} & -1-2\mathrm{i} \\ 2+2\mathrm{i} & -\mathrm{i} \end{pmatrix}.$$

(15.22) Proposition.

(a) Es seien $m, n, p \in \mathbb{N}_0$ gegeben. Für $A \in \mathbb{C}^{m\times n}$, $B \in \mathbb{C}^{n\times p}$ gilt

$$(AB)^{\mathrm{ad}} = B^{\mathrm{ad}} A^{\mathrm{ad}}.$$

(b) Es sei $n \in \mathbb{N}_0$ gegeben. Dann gilt

$$\mathrm{E}_n^{\mathrm{ad}} = \mathrm{E}_n.$$

(c) Es sei $n \in \mathbb{N}_0$ gegeben. Für $A \in \mathrm{GL}_n(\mathbb{C})$ ist auch $A^{\mathrm{ad}} \in \mathrm{GL}_n(\mathbb{C})$ mit
$$(A^{\mathrm{ad}})^{-1} = (A^{-1})^{\mathrm{ad}}.$$

(d) Es seien $m, n \in \mathbb{N}_0$ gegeben. Für $A, B \in \mathbb{C}^{m\times n}$ gilt
$$(A+B)^{\mathrm{ad}} = A^{\mathrm{ad}} + B^{\mathrm{ad}}.$$

(e) Es seien $m, n \in \mathbb{N}_0$ gegeben. Für $c \in \mathbb{C}$, $A \in \mathbb{C}^{m\times n}$ gilt
$$(cA)^{\mathrm{ad}} = \overline{c}A^{\mathrm{ad}}.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(15.23) Bemerkung. Es seien $m, n \in \mathbb{N}_0$ gegeben. Für $A \in \mathbb{C}^{m\times n}$ gilt
$$(A^{\mathrm{ad}})^{\mathrm{ad}} = A.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

Standardbasis

Zum Abschluss dieses Abschnitts führen wir noch eine Notation für Matrizen ein, welche an genau einer Stelle die Eins von R und sonst stets die Null von R als Einträge haben. Mit Hilfe dieser Matrizen lässt sich eine beliebige Matrix über R auf kanonische Art und Weise zerlegen, siehe Bemerkung (15.26).

(15.24) Notation.

(a) Es seien $m, n \in \mathbb{N}_0$ gegeben. Für $k \in [1, m]$, $l \in [1, n]$ sei $\mathrm{e}_{k,l} \in R^{m\times n}$ gegeben durch
$$\mathrm{e}_{k,l} = (\delta_{(i,j),(k,l)})_{i\in[1,m],j\in[1,n]}.$$

(b) Es sei $n \in \mathbb{N}_0$ gegeben. Für $k \in [1, n]$ schreiben wir auch
$$\mathrm{e}_k = \mathrm{e}_{k,1}.$$

(c) Es sei $n \in \mathbb{N}_0$ gegeben. Für $k \in [1, n]$ schreiben wir auch
$$\mathrm{e}_k = \mathrm{e}_{1,k}.$$

(15.25) Beispiel.

(a) In $\mathbb{Z}^{2\times 2}$ ist
$$\mathrm{e}_{1,1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \mathrm{e}_{1,2} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \mathrm{e}_{2,1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \mathrm{e}_{2,2} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

(b) In $\mathbb{Z}^{3\times 1}$ ist
$$\mathrm{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \mathrm{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \mathrm{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

(c) In $\mathbb{Z}^{1\times 2}$ ist
$$\mathrm{e}_1 = \begin{pmatrix} 1 & 0 \end{pmatrix}, \mathrm{e}_2 = \begin{pmatrix} 0 & 1 \end{pmatrix}.$$

(15.26) Bemerkung. Es seien $m, n \in \mathbb{N}_0$ und $A \in R^{m\times n}$ gegeben. Dann gilt
$$A = \sum_{i\in[1,m],j\in[1,n]} A_{i,j}\mathrm{e}_{i,j}.$$

Beweis. Es ist
$$\begin{aligned}\sum_{k\in[1,m],l\in[1,n]} A_{k,l}\mathrm{e}_{k,l} &= \sum_{k\in[1,m],l\in[1,n]} A_{k,l}(\delta_{(i,j),(k,l)})_{i\in[1,m],j\in[1,n]} \\ &= (\sum_{k\in[1,m],l\in[1,n]} A_{k,l}\delta_{(i,j),(k,l)})_{i\in[1,m],j\in[1,n]} = (A_{i,j})_{i\in[1,m],j\in[1,n]} = A.\end{aligned}$$
□

16 Lineare Gleichungssysteme

Es seien $m, n \in \mathbb{N}_0$ und ein kommutativer Ring R gegeben. Ein *lineares Gleichungssystem* aus m Gleichungen und n Unbekannten x_j für $j \in [1, n]$ über R ist durch

$$\begin{array}{ccccccccc} A_{1,1}x_1 & + & A_{1,2}x_2 & + & \dots & + & A_{1,n}x_n & = & b_1, \\ A_{2,1}x_1 & + & A_{2,2}x_2 & + & \dots & + & A_{2,n}x_n & = & b_2, \\ & & & & & & & \vdots & \\ A_{m,1}x_1 & + & A_{m,2}x_2 & + & \dots & + & A_{m,n}x_n & = & b_m \end{array}$$

für gegebene $A_{i,j}, b_i \in R$ für $i \in [1, m]$, $j \in [1, n]$, gegeben. Kurz können wir hierfür auch

$$\sum_{j \in [1,n]} A_{i,j}x_j = b_i$$

für $i \in [1, m]$ schreiben. Wir nennen das lineare Gleichungssystem *homogen*, falls $b_i = 0$ für $i \in [1, m]$, und ansonsten *inhomogen*.
Wir beginnen mit einem Beispiel:

(16.1) Beispiel. Es seien $x_1, x_2, x_3, x_4 \in \mathbb{R}$ gegeben. Genau dann gilt

$$\begin{array}{rcrcrcrcr} -2x_1 & + & 2x_2 & - & 6x_3 & - & 10x_4 & = & -24, \\ 2x_1 & + & 3x_2 & - & 9x_3 & - & 7x_4 & = & -15, \\ x_1 & + & x_2 & - & 3x_3 & - & 2x_4 & = & -4, \end{array}$$

wenn es ein $a \in \mathbb{R}$ mit

$$x_1 = 1,\ x_2 = -1 + 3a,\ x_3 = a,\ x_4 = 2$$

gibt.

Beweis. Zunächst gelte

$$\begin{aligned} -2x_1 + 2x_2 - 6x_3 - 10x_4 &= -24, \\ 2x_1 + 3x_2 - 9x_3 - 7x_4 &= -15, \\ x_1 + x_2 - 3x_3 - 2x_4 &= -4. \end{aligned}$$

Aus $-2x_1 + 2x_2 - 6x_3 - 10x_4 = -24$ und $2x_1 + 3x_2 - 9x_3 - 7x_4 = -15$ folgt

$$5x_2 - 15x_3 - 17x_4 = (-2x_1 + 2x_2 - 6x_3 - 10x_4) + (2x_1 + 3x_2 - 9x_3 - 7x_4) = -24 - 15 = -39.$$

Aus $2x_1 + 3x_2 - 9x_3 - 7x_4 = -15$ und $x_1 + x_2 - 3x_3 - 2x_4 = -4$ folgt

$$x_2 - 3x_3 - 3x_4 = (2x_1 + 3x_2 - 9x_3 - 7x_4) - 2(x_1 + x_2 - 3x_3 - 2x_4) = -15 - 2(-4) = -7.$$

Aus $5x_2 - 15x_3 - 17x_4 = -39$ und $x_2 - 3x_3 - 3x_4 = -7$ folgt

$$-2x_4 = (5x_2 - 15x_3 - 17x_4) - 5(x_2 - 3x_3 - 3x_4) = -39 - 5(-7) = -4$$

und damit

$$x_4 = 2.$$

Dies liefert

$$\begin{aligned} -2x_1 + 2x_2 - 6x_3 &= -24 + 10x_4 = -24 + 10 \cdot 2 = -4, \\ 2x_1 + 3x_2 - 9x_3 &= -15 + 7x_4 = -15 + 7 \cdot 2 = -1, \\ x_1 + x_2 - 3x_3 &= -4 + 2x_4 = -4 + 2 \cdot 2 = 0, \\ x_2 - 3x_3 &= -7 + 3x_4 = -7 + 3 \cdot 2 = -1. \end{aligned}$$

Aus $x_1 + x_2 - 3x_3 = 0$ und $x_2 - 3x_3 = -1$ folgt

$$x_1 = (x_1 + x_2 - 3x_3) - (x_2 - 3x_3) = 0 - (-1) = 1.$$

Wenn wir also $a := x_3$ setzen, so haben wir

$$x_3 = a,$$
$$x_2 = -1 + 3x_3 = -1 + 3a.$$

Gibt es umgekehrt ein $a \in \mathbb{R}$ mit $x_1 = 1$, $x_2 = -1 + 3a$, $x_3 = a$, $x_4 = 2$, so gilt auch

$$-2x_1 + 2x_2 - 6x_3 - 10x_4 = -2 \cdot 1 + 2(-1 + 3a) - 6a - 10 \cdot 2 = -24,$$
$$2x_1 + 3x_2 - 9x_3 - 7x_4 = 2 \cdot 1 + 3(-1 + 3a) - 9a - 7 \cdot 2 = -15,$$
$$x_1 + x_2 - 3x_3 - 2x_4 = 1 + (-1 + 3a) - 3a - 2 \cdot 2 = -4.$$ □

Man kann sich vorstellen, dass ein naives Vorgehen wie im Beweis von Beispiel (16.1) bei „großen“ linearen Gleichungssystemen (in Anwendungen können durchaus auch mal mehrere Hunderttausend Gleichungen und Unbekannte auftreten) sehr schnell zu Unübersichtlichkeiten führen kann.
In diesem Abschnitt werden wir ein systematisches Verfahren zum Lösen linearer Gleichungssysteme über *Körpern* erarbeiten. Die Kernidee des Verfahrens ist wie folgt: Aus den gegebenen Gleichungen gewinnen wir fortlaufend neue Gleichungen. Hierbei ersetzen wir für jede neue Gleichung eine der vorherigen Gleichungen, ohne hierbei die Gesamtheit der Lösungen zu verändern. Wir erhalten also stets neue lineare Gleichungssysteme mit der gleichen Anzahl an Gleichungen und mit den gleichen Lösungen. Dies machen wir so lange, bis wir am Ende ein lineares Gleichungssystem haben, welches eine so einfache Gestalt hat, dass wir die Lösungen direkt bestimmen oder sogar ablesen können.
Da wir einige spezielle lineare Gleichungen über *speziellen kommutativen Ringen* schon gesehen haben, vgl. Bemerkung (16.32) und Bemerkung (16.33), arbeiten wir wie in Abschnitt 15 über einem kommutativen Ring so lange es uns ohne Schwierigkeiten möglich ist. Die relevantesten Ergebnisse dieses Abschnittes sind jedoch lediglich für Körper gültig, an diesen Stellen werden wir unser Setup also spezialisieren.

Lösungsmenge eines linearen Gleichungssystems

Zur effizienten Darstellung linearer Gleichungssysteme können Matrizen und die in Definition (15.9)(a) eingeführte Matrixmultiplikation verwandt werden: Ein lineares Gleichungssystem aus m Gleichungen und n Unbekannten wie oben hängt nur von den gegebenen Koeffizienten $A_{i,j}$ und den Werten b_i für $i \in [1, m]$, $j \in [1, n]$ ab. Mit Hilfe von Matrizen lässt es sich durch eine einzige Gleichung umschreiben:

$$\begin{pmatrix} A_{1,1} & A_{1,2} & \dots & A_{1,n} \\ \vdots & \vdots & & \vdots \\ A_{m,1} & A_{m,2} & \dots & A_{m,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

Die gegebenen Daten des linearen Gleichungssystems lassen sich außerdem in der Matrix

$$\left(\begin{array}{cccc|c} A_{1,1} & A_{1,2} & \dots & A_{1,n} & b_1 \\ \vdots & \vdots & & \vdots & \vdots \\ A_{m,1} & A_{m,2} & \dots & A_{m,n} & b_m \end{array}\right)$$

zusammenfassen, die *erweiterte Koeffizientenmatrix* des linearen Gleichungssystems. Der präzise Zusammenhang zwischen Matrizen und linearen Gleichungssystemen wird in der nachfolgenden Definition festgehalten:

(16.2) Definition (Lösung eines linearen Gleichungssystems)**.** Es seien ein kommutativer Ring R und $m, n \in \mathbb{N}_0$ gegeben.

(a) Es seien $A \in R^{m \times n}$ und $b \in R^{m \times 1}$ gegeben. Die *Lösungsmenge des linearen Gleichungssystems* zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$ ist definiert als

$$\mathrm{Sol}(A, b) := \{x \in R^{n \times 1} \mid Ax = b\}.$$

Ein Element von $\mathrm{Sol}(A, b)$ wird *Lösung des linearen Gleichungssystems* zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$ genannt.

(b) Es sei $A \in R^{m\times n}$ gegeben. Die Lösungsmenge $\mathrm{Sol}(A,0)$ des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid 0\right)$ wird auch *Lösungsmenge des homogenen linearen Gleichungssystems* (oder *Lösungsraum des homogenen linearen Gleichungssystems*) zur Koeffizientenmatrix A genannt. Ein Element von $\mathrm{Sol}(A,0)$ wird auch *Lösung des homogenen linearen Gleichungssystems* zur Koeffizientenmatrix A genannt.

(16.3) Beispiel. Es seien $A \in \mathbb{R}^{3\times 4}$ und $b \in \mathbb{R}^{3\times 1}$ gegeben durch

$$A = \begin{pmatrix} -2 & 2 & -6 & -10 \\ 2 & 3 & -9 & -7 \\ 1 & 1 & -3 & -2 \end{pmatrix},\ b = \begin{pmatrix} -24 \\ -15 \\ -4 \end{pmatrix}.$$

Die Lösungsmenge des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$ ist gegeben durch

$$\mathrm{Sol}(A,b) = \begin{pmatrix} 1 \\ -1 \\ 0 \\ 2 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 0 \\ 3 \\ 1 \\ 0 \end{pmatrix}.$$

Beweis. Nach Beispiel (16.1) ist

$$\begin{aligned} \mathrm{Sol}(A,b) &= \{x \in \mathbb{R}^{4\times 1} \mid \text{es gibt ein } a \in \mathbb{R} \text{ mit } x = \begin{pmatrix} 1 \\ -1+3a \\ a \\ 2 \end{pmatrix}\} = \{\begin{pmatrix} 1 \\ -1+3a \\ a \\ 2 \end{pmatrix} \mid a \in \mathbb{R}\} \\ &= \{\begin{pmatrix} 1 \\ -1 \\ 0 \\ 2 \end{pmatrix} + a \begin{pmatrix} 0 \\ 3 \\ 1 \\ 0 \end{pmatrix} \mid a \in \mathbb{R}\} = \begin{pmatrix} 1 \\ -1 \\ 0 \\ 2 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 0 \\ 3 \\ 1 \\ 0 \end{pmatrix}. \end{aligned}$$

□

(16.4) Proposition. Es seien ein kommutativer Ring R, $m,n \in \mathbb{N}_0$, $A \in R^{m\times n}$, $b \in R^{m\times 1}$ und $x \in \mathrm{Sol}(A,b)$ gegeben. Dann ist

$$\mathrm{Sol}(A,0) \to \mathrm{Sol}(A,b),\ x_0 \mapsto x + x_0$$

eine wohldefinierte Bijektion. Insbesondere ist

$$\mathrm{Sol}(A,b) = x + \mathrm{Sol}(A,0).$$

Beweis. Auf Grund der Negierbarkeit von x ist $f\colon R^{n\times 1} \to R^{n\times 1}$, $x_0 \mapsto x + x_0$ eine Bijektion. Ferner ist

$$\begin{aligned} f(\mathrm{Sol}(A,0)) &= \{x' \in R^{n\times 1} \mid \text{es gibt ein } x_0 \in \mathrm{Sol}(A,0) \text{ mit } x' = f(x_0)\} \\ &= \{x' \in R^{n\times 1} \mid \text{es gibt ein } x_0 \in \mathrm{Sol}(A,0) \text{ mit } x' = x + x_0\} \\ &= \{x' \in R^{n\times 1} \mid \text{es gibt ein } x_0 \in \mathrm{Sol}(A,0) \text{ mit } x' - x = x_0\} \\ &= \{x' \in R^{n\times 1} \mid x' - x \in \mathrm{Sol}(A,0)\} = \{x' \in R^{n\times 1} \mid A(x'-x) = 0\} \\ &= \{x' \in R^{n\times 1} \mid Ax' - Ax = 0\} = \{x' \in R^{n\times 1} \mid Ax' = Ax\} = \mathrm{Sol}(A,Ax) = \mathrm{Sol}(A,b), \end{aligned}$$

so dass f zu einer surjektiven Abbildung $f|^{\mathrm{Sol}(A,b)}_{\mathrm{Sol}(A,0)}\colon \mathrm{Sol}(A,0) \to \mathrm{Sol}(A,b)$ einschränkt. Die Injektivität von f impliziert ferner die Injektivität von $f|^{\mathrm{Sol}(A,b)}_{\mathrm{Sol}(A,0)}$. Insgesamt ist $f|^{\mathrm{Sol}(A,b)}_{\mathrm{Sol}(A,0)}$ eine Bijektion. Insbesondere ist

$$\mathrm{Sol}(A,b) = \mathrm{Im}\, f|^{\mathrm{Sol}(A,b)}_{\mathrm{Sol}(A,0)} = f(\mathrm{Sol}(A,0)) = x + \mathrm{Sol}(A,0).$$

□

Für ein gegebenes inhomogenes lineares Gleichungssystem genügt es also, eine spezielle Lösung zu finden, sofern man die Lösungsmenge des zugehörigen homogenen linearen Gleichungssystems kennt. Aus theoretischer Sicht bietet ein homogenes lineares Gleichungssystem einige Vorteile, da die Lösungsmenge eines solchen einiges an Struktur aufweist:

(16.5) Proposition. Es seien ein kommutativer Ring R, $m, n \in \mathbb{N}_0$ und $A \in R^{m\times n}$ gegeben.

(a) Für $x, x' \in \mathrm{Sol}(A, 0)$ ist auch $x + x' \in \mathrm{Sol}(A, 0)$.

(b) Es ist $0 \in \mathrm{Sol}(A, 0)$.

(c) Für $a \in R$, $x \in \mathrm{Sol}(A, 0)$ ist auch $ax \in \mathrm{Sol}(A, 0)$.

Beweis.

(a) Für $x, x' \in \mathrm{Sol}(A, 0)$ gilt $Ax = 0$ und $Ax' = 0$, also auch

$$A(x + x') = Ax + Ax' = 0 + 0 = 0$$

und damit $x + x' \in \mathrm{Sol}(A, 0)$.

(b) Wegen $A0 = 0$ ist $0 \in \mathrm{Sol}(A, 0)$.

(c) Für $x \in \mathrm{Sol}(A, 0)$ gilt $Ax = 0$, also für $a \in R$ auch

$$A(ax) = a(Ax) = a\,0 = 0$$

und damit $ax \in \mathrm{Sol}(A, 0)$. □

Proposition (16.5) besagt, dass wir nicht nur in der Menge der Spaltenmatrizen $R^{n\times 1}$ rechnen (Spaltenmatrizen addieren und mit Skalaren multiplizieren) können, sondern bereits in der Teilmenge $\mathrm{Sol}(A, 0)$: Die Summe von Spaltenmatrizen in $\mathrm{Sol}(A, 0)$ liegt wieder in $\mathrm{Sol}(A, 0)$ (und nicht erst in der größeren Menge $R^{n\times 1}$), so dass wir $\mathrm{Sol}(A, 0)$ selbst mit dieser Addition betrachten können. Ähnlich für die Skalarmultiplikation. Die Lösungsmenge $\mathrm{Sol}(A, 0)$ bekommt durch diese Addition und Skalarmultiplikation selbst eine Struktur. ([49])

Zeilenstufenform

Zunächst studieren wir Matrizen, bei denen sich die Lösungen der zugehörigen linearen Gleichungssysteme sofort rekursiv ermitteln lassen.

(16.6) Definition (Zeilenstufenindizes, Zeilenstufenanzahl)**.** Es seien ein kommutativer Ring R, $m, n \in \mathbb{N}_0$ und $A \in R^{m\times n}$ gegeben.

(a) Für $i \in [1, m]$ heißt

$$\mathrm{ech}_i = \mathrm{ech}_i(A) := \begin{cases} \min\{j \in [1, n] \mid A_{i,j} \neq 0\}, & \text{falls } A_{i,-} \neq 0, \\ n + i, & \text{falls } A_{i,-} = 0, \end{cases}$$

der *i-te Zeilenstufenindex* von A.

(b) Es heißt

$$|\{i \in [1, m] \mid A_{i,-} \neq 0\}|$$

die *Zeilenstufenanzahl* von A.

(16.7) Beispiel. Es sei $A \in \mathbb{R}^{3\times 4}$ gegeben durch

$$A = \begin{pmatrix} 0 & 3 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

[49] In der *Linearen Algebra* werden Strukturen dieser Art, sogenannte (*Unter-*)*Moduln* (bzw. (*Unter-*)*Vektorräume*, falls R ein Körper ist), studiert; an der RWTH Aachen bspw. im Kurs Lineare Algebra für Informatiker (etwa 2. Semester im Studiengang B.Sc. Informatik).

(a) Die Zeilenstufenindizes von A sind gegeben durch

$$\begin{aligned}\mathrm{ech}_1 &= 2,\\ \mathrm{ech}_2 &= 6,\\ \mathrm{ech}_3 &= 1.\end{aligned}$$

(b) Die Zeilenstufenanzahl von A ist gleich 2.

Beweis.

(a) Es ist $A_{1,-} = \begin{pmatrix}0 & 3 & 0 & -1\end{pmatrix} \neq 0$ und $\{j \in [1,4] \mid A_{1,j} \neq 0\} = \{2,4\}$, also

$$\mathrm{ech}_1 = \min\{j \in [1,4] \mid A_{1,j} \neq 0\} = \min\{2,4\} = 2.$$

Es ist $A_{2,-} = \begin{pmatrix}0 & 0 & 0 & 0\end{pmatrix} = 0$, also

$$\mathrm{ech}_2 = 4 + 2 = 6.$$

Es ist $A_{3,-} = \begin{pmatrix}1 & 0 & 0 & 0\end{pmatrix} \neq 0$ und $\{j \in [1,4] \mid A_{3,j} \neq 0\} = \{1\}$, also

$$\mathrm{ech}_3 = \min\{j \in [1,4] \mid A_{3,j} \neq 0\} = \min\{1\} = 1.$$

(b) Es ist $\{i \in [1,m] \mid A_{i,-} \neq 0\} = \{1,3\}$, also

$$|\{i \in [1,m] \mid A_{i,-} \neq 0\}| = |\{1,3\}| = 2.$$ □

(16.8) Definition ((reduzierte) Zeilenstufenform)**.** Es seien ein kommutativer Ring R, $m,n \in \mathbb{N}_0$ und $A \in R^{m\times n}$ gegeben.

(a) Wir sagen, dass A in *Zeilenstufenform* ist, falls

$$\mathrm{ech}_i < \mathrm{ech}_{i+1}$$

für alle $i \in [1, m-1]$ gilt.

(b) Es sei r die Zeilenstufenanzahl von A. Wir sagen, dass A in *reduzierter Zeilenstufenform* ist, falls A in Zeilenstufenform ist und

$$A_{-,\mathrm{ech}_i} = \mathrm{e}_i$$

für alle $i \in [1,r]$ gilt.

Eine Matrix A in Zeilenstufenform ist von folgender Gestalt, wobei die mit $*$ markierten Einträge beliebig sind und $A_{i,\mathrm{ech}_i} \neq 0$ für $i \in [1,r]$ und für ein $r \in [0,m]$:

$$A = \left(\begin{array}{ccc|ccccccccccc}
0 & \dots & 0 & A_{1,\mathrm{ech}_1} & * & \dots & * & * & * & \dots & * & * & * & \dots & * \\
0 & \dots & 0 & 0 & 0 & \dots & 0 & A_{2,\mathrm{ech}_2} & * & \dots & * & * & * & \dots & * \\
\vdots & & \vdots & \vdots & \vdots & & \vdots & & \ddots & \ddots & \ddots & \vdots & \vdots & & \vdots \\
0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & A_{r,\mathrm{ech}_r} & * & \dots & * \\
\hline
0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\
\vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & & \vdots & \vdots & \vdots & & \vdots \\
0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 0 & 0 & \dots & 0
\end{array}\right)$$

Eine Matrix A in reduzierter Zeilenstufenform ist von folgender Gestalt:

$$A = \left(\begin{array}{ccc|ccccccccccc}
0 & \dots & 0 & 1 & * & \dots & * & 0 & * & \dots & * & 0 & * & \dots & * \\
0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & * & \dots & * & 0 & * & \dots & * \\
\vdots & & \vdots & \vdots & \vdots & & \vdots & & \ddots & \ddots & \ddots & \vdots & \vdots & & \vdots \\
0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 1 & * & \dots & * \\
\hline
0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\
\vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & & \vdots & \vdots & \vdots & & \vdots \\
0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 0 & 0 & \dots & 0
\end{array}\right)$$

(16.9) Beispiel.

(a) Über $\mathbb{R}$ ist die Matrix

$$\begin{pmatrix} 1 & 1 & -1 & -3 \\ 0 & 0 & 2 & 4 \\ 2 & 2 & 0 & -2 \end{pmatrix}$$

nicht in Zeilenstufenform.

(b) Über $\mathbb{R}$ ist die Matrix

$$\begin{pmatrix} 1 & 1 & -1 & -3 \\ 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

in Zeilenstufenform, aber nicht in reduzierter Zeilenstufenform.

(c) Über $\mathbb{R}$ ist die Matrix

$$\begin{pmatrix} 1 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

in reduzierter Zeilenstufenform.

In folgender Proposition geben wir eine rekursive Formel für die Lösungmenge eines linearen Gleichungssystems zu einer Matrix über einem Körper in Zeilenstufenform an.

(16.10) Proposition (Lösbarkeitskriterium und Lösungsbestimmung für lineare Gleichungssysteme über Körpern in Zeilenstufenform)**.** Es seien ein Körper K, $m, n \in \mathbb{N}_0$, $A \in K^{m\times n}$ in Zeilenstufenform und $b \in K^{m\times 1}$ gegeben. Ferner sei r die Zeilenstufenanzahl von A.

(a) Genau dann gibt es eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\big(A \mid b\big)$, wenn die Zeilenstufenanzahl von $\big(A \mid b\big)$ auch gleich r ist.

(b) Es sei r auch die Zeilenstufenanzahl von $\big(A \mid b\big)$. Dann ist die Lösungsmenge des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\big(A \mid b\big)$ gegeben durch

$$\mathrm{Sol}(A,b) = \{x \in K^{n\times 1} \mid \text{für } i \in [1,r] \text{ ist } x_{\mathrm{ech}_i} = A^{-1}_{i,\mathrm{ech}_i}(b_i - \sum_{j\in[\mathrm{ech}_i+1,n]} A_{i,j}x_j)\}.$$

Beweis. Zunächst sei die Zeilenstufenanzahl von $\big(A \mid b\big)$ ungleich r, so dass es ein $i \in [r+1, m]$ mit $A_{i,-} = 0$ und $b_i \neq 0$ gibt.

$$\big(A \mid b\big) = \left(\begin{array}{ccccccccccc|c} 0 & \dots & 0 & A_{1,\mathrm{ech}_1} & A_{1,\mathrm{ech}_1+1} & \dots & A_{1,\mathrm{ech}_r-1} & A_{1,\mathrm{ech}_r} & \dots & A_{1,n} & b_1 \\ \vdots & & \vdots & & \ddots & \ddots & \ddots & \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & A_{r,\mathrm{ech}_r} & \dots & A_{r,n} & b_r \\ \hline 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & b_{r+1} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & b_m \end{array}\right)$$

Für $x \in K^{n\times 1}$ ist dann aber

$$(Ax)_i = \sum_{j\in[1,n]} A_{i,j}x_j = \sum_{j\in[1,n]} 0x_j = 0 \neq b_i,$$

also $Ax \neq b$ und damit $\mathrm{Sol}(A,b) = \emptyset$.

Nun sei umgekehrt die Zeilenstufenanzahl von $\left(A \mid b\right)$ gleich r, so dass $A_{i,-} = 0$ und $b_i = 0$ für alle $i \in [r+1, m]$ gilt.

$$\left(A \mid b\right) = \left(\begin{array}{cccccccccc|c} 0 & \dots & 0 & A_{1,\mathrm{ech}_1} & A_{1,\mathrm{ech}_1+1} & \dots & A_{1,\mathrm{ech}_r-1} & A_{1,\mathrm{ech}_r} & \dots & A_{1,n} & b_1 \\ \vdots & & \vdots & & \ddots & \ddots & \ddots & \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & A_{r,\mathrm{ech}_r} & \dots & A_{r,n} & b_r \\ \hline 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \end{array}\right)$$

Dann ist $\left(A \mid b\right)$ in Zeilenstufenform und für $i \in [1, r]$ gilt

$$\mathrm{ech}_i(\left(A \mid b\right)) = \mathrm{ech}_i(A).$$

Nun sei $x \in K^{n \times 1}$ gegeben. Genau dann ist x eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$, wenn $Ax = b$ gilt, d.h. wenn für $i \in [1, m]$ stets

$$\sum_{j \in [1,n]} A_{i,j} x_j = b_i$$

gilt. Da A in Zeilenstufenform ist, gilt für $i \in [1, r]$ stets $A_{i,j} = 0$ für $j \in [1, \mathrm{ech}_i - 1]$ und damit

$$\sum_{j \in [1,n]} A_{i,j} x_j = \sum_{j \in [\mathrm{ech}_i, n]} A_{i,j} x_j = A_{i,\mathrm{ech}_i} x_{\mathrm{ech}_i} + \sum_{j \in [\mathrm{ech}_i + 1, n]} A_{i,j} x_j.$$

Ferner gilt für $i \in [r+1, m]$ ohnehin stets

$$\sum_{j \in [1,n]} A_{i,j} x_j = \sum_{j \in [1,n]} 0 x_j = 0 = b_i.$$

Somit ist x genau dann eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$, wenn

$$A_{i,\mathrm{ech}_i} x_{\mathrm{ech}_i} + \sum_{j \in [\mathrm{ech}_i + 1, n]} A_{i,j} x_j = b_i$$

für $i \in [1, r]$ gilt. Diese Bedingung ist jedoch äquivalent dazu, dass

$$x_{\mathrm{ech}_i} = A^{-1}_{i,\mathrm{ech}_i} (b_i - \sum_{j \in [\mathrm{ech}_i + 1, n]} A_{i,j} x_j)$$

für $i \in [1, r]$ gilt. Nun ist dies aber eine rekursive Beschreibung von x, folglich also $\mathrm{Sol}(A, b) \neq \emptyset$. □

Der konstruktive Beweis von Proposition (16.10) liefert folgenden Algorithmus zur Bestimmung der Lösungsmenge eines linearen Gleichungssystems zu einer erweiterten Koeffizientenmatrix in Zeilenstufenform.

$$\left(\begin{array}{cccccccccccccc|c} 0 & \dots & 0 & \blacksquare & * & \dots & * & * & * & \dots & * & * & * & \dots & * & * \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & \blacksquare & * & \dots & * & * & * & \dots & * & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & & \ddots & \ddots & \ddots & \vdots & \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & \blacksquare & * & \dots & * & * \\ \hline 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \end{array}\right)$$

Die mit $*$ markierten Einträge sind beliebig und die mit ■ markierten Einträge sind ungleich 0. Die r Unbekannten an den ■-Spalten nennen wir *abhängige Variablen*, die anderen $n - r$ Unbekannten nennen wir *freie Variablen*. Zunächst bringen wir die freien Variablen auf die rechte Seite des linearen Gleichungssystems und ersetzen sie der Reihe nach durch „Parameter“ $a_1, \dots, a_{n-r} \in K$. Danach lösen wir, von unten nach oben, nach den abhängigen Variablen auf; nach jedem dieser Schritte steht in der jeweils nächsten zu lösenden Gleichung genau eine abhängige Variable.

(16.11) Algorithmus.

- Eingabe: $A \in K^{m\times n}$ in Zeilenstufenform, $b \in K^{m\times 1}$ für einen Körper K und gewisse $m, n \in \mathbb{N}_0$
- Ausgabe: $\mathrm{Sol}(A, b)$
- Verfahren:

```
function solref(A, b)
    ermittle die Zeilenstufenanzahl r von A;

    if b_i ≠ 0 für ein i ∈ [r+1, m] then
        return ∅;
    end if;

    l := 1;
    for j from 1 to n do
        if j ≠ ech_i für alle i ∈ [1, r] then
            x_j := a_l;                          // a_l ist ein Symbol
            l := l + 1;
        end if;
    end for;

    for i from r to 1 do
        x_{ech_i} := A^{-1}_{i,ech_i}(b_i - Σ_{j∈[ech_i+1,n]} A_{i,j} x_j);
    end for;

    return {x | a_l ∈ K für l ∈ [1, n-r]};
end function;
```

(16.12) Beispiel. Es seien $A \in \mathbb{R}^{3\times 4}$ und $b \in \mathbb{R}^{3\times 1}$ gegeben durch

$$A = \begin{pmatrix} 2 & 2 & -2 & -6 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \; b = \begin{pmatrix} 4 \\ 1 \\ 0 \end{pmatrix}.$$

Die Lösungsmenge des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$ ist gegeben durch

$$\mathrm{Sol}(A, b) = \begin{pmatrix} 3 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \mathbb{R} \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 1 \\ 0 \\ -2 \\ 1 \end{pmatrix}.$$

Beweis. Es ist

$$\left(A \mid b\right) = \left(\begin{array}{cccc|c} 2 & 2 & -2 & -6 & 4 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Für $x \in \mathbb{R}^{4\times 1}$ gilt genau dann $x \in \mathrm{Sol}(A, b)$, wenn es $a_1, a_2 \in \mathbb{R}$ gibt mit

$$\begin{aligned} x_2 &= a_1, \\ x_4 &= a_2, \\ x_3 &= 1 - 2x_4 = 1 - 2a_2, \\ x_1 &= 2^{-1}(4 - 2x_2 + 2x_3 + 6x_4) = 2 - x_2 + x_3 + 3x_4 = 2 - a_1 + (1 - 2a_2) + 3a_2 = 3 - a_1 + a_2. \end{aligned}$$

Folglich ist

$$\mathrm{Sol}(A, b) = \left\{ \begin{pmatrix} 3 - a_1 + a_2 \\ a_1 \\ 1 - 2a_2 \\ a_2 \end{pmatrix} \mid a_1, a_2 \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} 3 \\ 0 \\ 1 \\ 0 \end{pmatrix} + a_1 \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 1 \\ 0 \\ -2 \\ 1 \end{pmatrix} \mid a_1, a_2 \in \mathbb{R} \right\}$$

$$= \begin{pmatrix} 3 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \mathbb{R} \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 1 \\ 0 \\ -2 \\ 1 \end{pmatrix}. \qquad \square$$

Elementare Zeilenoperationen

Da eine beliebige Matrix nicht in Zeilenstufenform ist, benötigen wir zum Lösen allgemeiner linearer Gleichungssysteme eine Methode, um eine gegebene Matrix in eine geeignete Matrix in (reduzierter) Zeilenstufenform zu überführen. Hierbei bedeutet „geeignet“, dass die Lösungsmenge des linearen Gleichungssystems zur ursprünglichen Matrix gleich der Lösungsmenge des linearen Gleichungssystems zur Matrix in Zeilenstufenform sein sollte.
Um den Prozess des Überführens von Matrizen zu formalisieren, führen wir Operationen auf den Zeilen von Matrizen ein. Betrachten wir diese Zeilenoperationen simultan für alle $(m \times n)$-Matrizen über einem kommutativen Ring R für gegebene $m, n \in \mathbb{N}_0$, so erhalten wir also eine Abbildung $R^{m\times n} \to R^{m\times n}$. Wir werden in Proposition (16.17) sehen, dass diese Operatoren die Lösungsmengen von linearen Gleichungssystemen invariant lassen.

(16.13) Definition ((elementare) Zeilenoperatoren)**.** Es seien ein kommutativer Ring R und $m, n \in \mathbb{N}_0$ gegeben.

(a) Für $k, l \in [1, m]$ ist der *Vertauschungsoperator* der k-ten und l-ten Zeile definiert als Abbildung $\mathrm{sw}_{k,l} \colon R^{m\times n} \to R^{m\times n}$ gegeben durch

$$\mathrm{sw}_{k,l}(A)_{i,-} = \begin{cases} A_{l,-} & \text{für } i = k, \\ A_{k,-} & \text{für } i = l, \\ A_{i,-} & \text{für } i \in [1, m] \setminus \{k, l\} \end{cases}$$

für $A \in R^{m\times n}$.

(b) Für $k, l \in [1, m]$ mit $k \neq l$ und $c \in R$ ist der *Additionsoperator* des c-fachen der l-ten zur k-ten Zeile definiert als Abbildung $\mathrm{add}_{k,l,c} \colon R^{m\times n} \to R^{m\times n}$ gegeben durch

$$\mathrm{add}_{k,l,c}(A)_{i,-} = \begin{cases} A_{k,-} + cA_{l,-} & \text{für } i = k, \\ A_{i,-} & \text{für } i \in [1, m] \setminus \{k\} \end{cases}$$

für $A \in R^{m\times n}$.

(c) Für $k \in [1, m]$ und $c \in R^\times$ ist der *Multiplikationsoperator* der k-ten Zeile um das c-fache definiert als Abbildung $\mathrm{mul}_{k,c} \colon R^{m\times n} \to R^{m\times n}$ gegeben durch

$$\mathrm{mul}_{k,c}(A)_{i,-} = \begin{cases} cA_{k,-} & \text{für } i = k, \\ A_{i,-} & \text{für } i \in [1, m] \setminus \{k\} \end{cases}$$

für $A \in R^{m\times n}$.

(d) Ein *elementarer Zeilenoperator* auf $R^{m\times n}$ ist eine Abbildung $\rho \colon R^{m\times n} \to R^{m\times n}$ von der Form $\rho = \mathrm{sw}_{k,l}$ für gewisse $k, l \in [1, m]$ oder $\rho = \mathrm{add}_{k,l,c}$ für gewisse $k, l \in [1, m]$ mit $k \neq l$ und $c \in R$ oder $\rho = \mathrm{mul}_{k,c}$ für gewisse $k \in [1, m]$, $c \in R^\times$.

(e) Ein *Zeilenoperator* auf $K^{m\times n}$ ist eine Abbildung $\rho \colon K^{m\times n} \to K^{m\times n}$, welche ein (endliches) Kompositum von elementaren Zeilenoperatoren ist.

Wir betonen, dass wir für die Definition des Additionsoperators in (16.13)(b) stets $k \neq l$ fordern, während dies für den Vertauschungsoperator in (16.13)(a) nicht zwingend vorgeschrieben wird: Im Fall $k = l$ gilt mit der dort verwendeten Notation $\mathrm{sw}_{k,l} = \mathrm{id}_{K^{m\times n}}$. Ebenso haben wir $\mathrm{add}_{k,l,c} = \mathrm{id}_{K^{m\times n}}$ im Fall $c = 0$ in Definition (16.13)(b) sowie $\mathrm{mul}_{k,c} = \mathrm{id}_{K^{m\times n}}$ im Fall $c = 1$ in Definition (16.13)(c).

Wenden wir den Vertauschungsoperator $\mathrm{sw}_{k,l}$ für $k,l \in [1,m]$ auf eine Matrix $A \in R^{m\times n}$ an, so bewirkt dies, dass die k-te und die l-te Zeile von A vertauscht werden. Steht die Matrix für ein lineares Gleichungssystem, so entspricht dies also gerade der Vertauschung der k-ten und l-ten Gleichung.
Wenden wir den Additionsoperator $\mathrm{add}_{k,l,c}$ für $k,l \in [1,m]$, $k \neq l$, $c \in R$ auf eine Matrix $A \in R^{m\times n}$ an, so bewirkt dies, dass das c-fache der l-ten Zeile von A zur k-ten Zeile von A addiert wird. Steht die Matrix für ein lineares Gleichungssystem, so entspricht dies also gerade der Addition des c-fachen der l-ten Gleichung zur k-ten Gleichung.
Wenden wir den Multiplikationsoperator $\mathrm{mul}_{k,c}$ für $k \in [1,m]$, $c \in R^\times$ auf eine Matrix $A \in R^{m\times n}$ an, so bewirkt dies, dass die k-te Zeile von A mit c multipliziert wird. Steht die Matrix für ein lineares Gleichungssystem, so entspricht dies also gerade der Multiplikation der k-ten Gleichung mit c.
Wirkt ein (elementarer) Zeilenoperator auf einer Matrix, so sprechen wir von einer (elementaren) Zeilenoperation.

(16.14) Beispiel. Über $\mathbb{Q}$ gilt

$$\begin{pmatrix} 0 & 2 & 1 & -3 \\ 2 & 0 & -2 & 6 \\ 0 & 4 & 2 & -7 \end{pmatrix} \overset{\mathrm{sw}_{1,2}}{\longmapsto} \begin{pmatrix} 2 & 0 & -2 & 6 \\ 0 & 2 & 1 & -3 \\ 0 & 4 & 2 & -7 \end{pmatrix} \overset{\mathrm{add}_{3,2,-2}}{\longmapsto} \begin{pmatrix} 2 & 0 & -2 & 6 \\ 0 & 2 & 1 & -3 \\ 0 & 0 & 0 & -1 \end{pmatrix} \overset{\mathrm{mul}_{1,\frac{1}{2}}}{\longmapsto} \begin{pmatrix} 1 & 0 & -1 & 3 \\ 0 & 2 & 1 & -3 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Die wichtigste Eigenschaft einer elementaren Zeilenoperation ist ihre Fähigkeit, rückgängig gemacht zu werden:

(16.15) Bemerkung. Es seien ein kommutativer Ring R und $m,n \in \mathbb{N}_0$ gegeben.

(a) Für $k,l \in [1,m]$ ist $\mathrm{sw}_{k,l}\colon R^{m\times n} \to R^{m\times n}$ eine invertierbare Abbildung mit

$$\mathrm{sw}_{k,l}^{-1} = \mathrm{sw}_{l,k} = \mathrm{sw}_{k,l}.$$

(b) Für $k,l \in [1,m]$ mit $k \neq l$ und $c \in R$ ist $\mathrm{add}_{k,l,c}\colon R^{m\times n} \to R^{m\times n}$ eine invertierbare Abbildung mit

$$\mathrm{add}_{k,l,c}^{-1} = \mathrm{add}_{k,l,-c}.$$

(c) Für $k \in [1,m]$, $c \in R^\times$ ist $\mathrm{mul}_{k,c}\colon R^{m\times n} \to R^{m\times n}$ eine invertierbare Abbildung mit

$$\mathrm{mul}_{k,c}^{-1} = \mathrm{mul}_{k,c^{-1}}.$$

Beweis.

(a) Für $k,l \in [1,m]$ gilt

$$\mathrm{sw}_{l,k}(A)_{i,-} = \begin{cases} A_{k,-}, & \text{falls } i = l, \\ A_{l,-}, & \text{falls } i = k, \\ A_{i,-}, & \text{falls } i \in [1,m] \setminus \{k,l\} \end{cases} = \begin{cases} A_{l,-}, & \text{falls } i = k, \\ A_{k,-}, & \text{falls } i = l, \\ A_{i,-}, & \text{falls } i \in [1,m] \setminus \{k,l\} \end{cases} = \mathrm{sw}_{k,l}(A)_{i,-}$$

und

$$\mathrm{sw}_{k,l}(\mathrm{sw}_{k,l}(A))_{i,-} = \begin{cases} \mathrm{sw}_{k,l}(A)_{l,-}, & \text{falls } i = k, \\ \mathrm{sw}_{k,l}(A)_{k,-}, & \text{falls } i = l, \\ \mathrm{sw}_{k,l}(A)_{i,-}, & \text{falls } i \in [1,m] \setminus \{k,l\} \end{cases} = A_{i,-}$$

für $i \in [1,m]$, $A \in R^{m\times n}$, also $\mathrm{sw}_{l,k} = \mathrm{sw}_{k,l}$ und $\mathrm{sw}_{k,l} \circ \mathrm{sw}_{k,l} = \mathrm{id}_{R^{m\times n}}$. Folglich ist $\mathrm{sw}_{k,l}$ eine invertierbare Abbildung mit

$$\mathrm{sw}_{k,l}^{-1} = \mathrm{sw}_{l,k} = \mathrm{sw}_{k,l}.$$

(b) Es seien $k,l \in [1,m]$ mit $k \neq l$ gegeben. Für $c \in R$ gilt dann

$$\mathrm{add}_{k,l,-c}(\mathrm{add}_{k,l,c}(A))_{i,-} = \begin{cases} \mathrm{add}_{k,l,c}(A)_{k,-} + (-c)\,\mathrm{add}_{k,l,c}(A)_{l,-}, & \text{falls } i = k, \\ \mathrm{add}_{k,l,c}(A)_{i,-}, & \text{falls } i \in [1,m] \setminus \{k\} \end{cases}$$

$$= \left.\begin{cases} A_{k,-} + cA_{l,-} + (-c)A_{l,-}, & \text{falls } i = k, \\ A_{i,-}, & \text{falls } i \in [1,m] \setminus \{k\} \end{cases}\right\} = A_{i,-}$$

für $i \in [1,m]$, $A \in R^{m\times n}$, also $\mathrm{add}_{k,l,-c} \circ \mathrm{add}_{k,l,c} = \mathrm{id}_{R^{m\times n}}$. Damit gilt für $c \in R$ jedoch auch $\mathrm{add}_{k,l,c} \circ \mathrm{add}_{k,l,-c} = \mathrm{add}_{k,l,-(-c)} \circ \mathrm{add}_{k,l,-c} = \mathrm{id}_{R^{m\times n}}$. Folglich ist $\mathrm{add}_{k,l,c}$ für $c \in R$ eine invertierbare Abbildung mit

$$\mathrm{add}_{k,l,c}^{-1} = \mathrm{add}_{k,l,-c}.$$

(c) Es sei $k \in [1,m]$ gegeben. Für $c \in R^\times$ gilt dann

$$\mathrm{mul}_{k,c^{-1}}(\mathrm{mul}_{k,c}(A))_{i,-} = \left.\begin{cases} c^{-1}\,\mathrm{mul}_{k,c}(A)_{k,-}, & \text{falls } i = k, \\ \mathrm{mul}_{k,c}(A)_{i,-}, & \text{falls } i \in [1,m] \setminus \{k\} \end{cases}\right\}$$
$$= \left.\begin{cases} c^{-1}cA_{k,-}, & \text{falls } i = k, \\ A_{i,-}, & \text{falls } i \in [1,m] \setminus \{k\} \end{cases}\right\} = A_{i,-}$$

für $i \in [1,m]$, $A \in R^{m\times n}$, also $\mathrm{mul}_{k,c^{-1}} \circ \mathrm{mul}_{k,c} = \mathrm{id}_{R^{m\times n}}$. Damit gilt für $c \in R^\times$ jedoch auch $\mathrm{mul}_{k,c} \circ \mathrm{mul}_{k,c^{-1}} = \mathrm{mul}_{k,(c^{-1})^{-1}} \circ \mathrm{mul}_{k,c^{-1}} = \mathrm{id}_{R^{m\times n}}$. Folglich ist $\mathrm{mul}_{k,c^{-1}}$ für $c \in R^\times$ eine invertierbare Abbildung mit

$$\mathrm{mul}_{k,c}^{-1} = \mathrm{mul}_{k,c^{-1}}.$$ □

(16.16) Korollar. Es seien ein kommutativer Ring R und $m,n \in \mathbb{N}_0$ und ein Zeilenoperator ρ auf $R^{m\times n}$ gegeben. Dann ist ρ invertierbar und ρ^{-1} ist ebenfalls ein Zeilenoperator auf $R^{m\times n}$.

Beweis. Dies folgt aus Bemerkung (16.15) und Proposition (3.21)(a). □

(16.17) Proposition. Es seien ein kommutativer Ring R und $m,n \in \mathbb{N}_0$, $A, A' \in R^{m\times n}$, $b, b' \in R^{m\times 1}$ und ein Zeilenoperator ρ auf $R^{m\times(n+1)}$ mit $\left(A' \mid b'\right) = \rho(\left(A \mid b\right))$ gegeben. Dann ist

$$\mathrm{Sol}(A', b') = \mathrm{Sol}(A, b).$$

Beweis. Zunächst sei ρ ein elementarer Zeilenoperator auf $R^{m\times(n+1)}$, d.h. $\rho = \mathrm{sw}_{k,l}$ für gewisse $k,l \in [1,m]$ oder $\rho = \mathrm{add}_{k,l,c}$ für gewisse $k,l \in [1,m]$ mit $k \neq l$ und $c \in R$ oder $\rho = \mathrm{mul}_{k,c}$ für gewisse $k \in [1,m]$, $c \in R^\times$. Ferner sei eine Lösung x des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$ gegeben, d.h. es gelte

$$\sum_{j\in[1,n]} A_{i,j}x_j = b_i$$

für $i \in [1,m]$.
Wenn $\rho = \mathrm{sw}_{k,l}$ für gewisse $k,l \in [1,m]$ ist, dann gilt

$$\sum_{j\in[1,n]} \mathrm{sw}_{k,l}(A)_{i,j}x_j = \left.\begin{cases} \sum_{j\in[1,n]} A_{l,j}x_j, & \text{falls } i = k, \\ \sum_{j\in[1,n]} A_{k,j}x_j, & \text{falls } i = l, \\ \sum_{j\in[1,n]} A_{i,j}x_j, & \text{falls } i \in [1,m] \setminus \{k,l\} \end{cases}\right\} = \left\{\begin{cases} b_l, & \text{falls } i = k, \\ b_k, & \text{falls } i = l, \\ b_i, & \text{falls } i \in [1,m] \setminus \{k,l\} \end{cases}\right\}$$
$$= \mathrm{sw}_{k,l}(b)_i,$$

für $i \in [1,m]$, d.h. x ist eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix

$$\left(\mathrm{sw}_{k,l}(A) \mid \mathrm{sw}_{k,l}(b)\right) = \mathrm{sw}_{k,l}(\left(A \mid b\right)) = \rho(\left(A \mid b\right)).$$

Wenn $\rho = \mathrm{add}_{k,l,c}$ für gewisse $k,l \in [1,m]$ mit $k \neq l$ und $c \in R$ ist, dann gilt

$$\sum_{j\in[1,n]} \mathrm{add}_{k,l,c}(A)_{i,j}x_j = \left.\begin{cases} \sum_{j\in[1,n]} (A_{k,j} + cA_{l,j})x_j, & \text{falls } i = k, \\ \sum_{j\in[1,n]} A_{i,j}x_j, & \text{falls } i \in [1,m] \setminus \{k\} \end{cases}\right\}$$

$$= \begin{Bmatrix} \sum_{j\in[1,n]} A_{k,j}x_j + c\sum_{j\in[1,n]} A_{l,j}x_j, & \text{falls } i = k, \\ \sum_{j\in[1,n]} A_{i,j}x_j, & \text{falls } i \in [1,m] \setminus \{k\} \end{Bmatrix}$$
$$= \begin{Bmatrix} b_k + cb_l, & \text{falls } i = k, \\ b_i, & \text{falls } i \in [1,m] \setminus \{k\} \end{Bmatrix} = \mathrm{add}_{k,l,c}(b)_i,$$

für $i \in [1,m]$, d.h. x ist eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix

$$\big(\mathrm{add}_{k,l,c}(A) \mid \mathrm{add}_{k,l,c}(b)\big) = \mathrm{add}_{k,l,c}\big((A \mid b)\big) = \rho\big((A \mid b)\big).$$

Wenn $\rho = \mathrm{mul}_{k,c}$ für gewisse $k \in [1,m]$ und $c \in R^\times$ ist, dann gilt

$$\sum_{j\in[1,n]} \mathrm{mul}_{k,c}(A)_{i,j}x_j = \begin{Bmatrix} \sum_{j\in[1,n]}(cA_{k,j})x_j, & \text{falls } i = k, \\ \sum_{j\in[1,n]} A_{i,j}x_j, & \text{falls } i \in [1,m] \setminus \{k\} \end{Bmatrix}$$
$$= \begin{Bmatrix} c\sum_{j\in[1,n]} A_{k,j}x_j, & \text{falls } i = k, \\ \sum_{j\in[1,n]} A_{i,j}x_j, & \text{falls } i \in [1,m] \setminus \{k\} \end{Bmatrix} = \begin{Bmatrix} cb_k, & \text{falls } i = k, \\ b_i, & \text{falls } i \in [1,m] \setminus \{k\} \end{Bmatrix}$$
$$= \mathrm{mul}_{k,c}(b)_i,$$

für $i \in [1,m]$, d.h. x ist eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix

$$\big(\mathrm{mul}_{k,c}(A) \mid \mathrm{mul}_{k,c}(b)\big) = \mathrm{mul}_{k,c}\big((A \mid b)\big) = \rho\big((A \mid b)\big).$$

Folglich ist in jedem Fall x auch eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\rho\big((A \mid b)\big) = \big(A' \mid b'\big)$, d.h. es gilt $\mathrm{Sol}(A,b) \subseteq \mathrm{Sol}(A',b')$.
Nach Bemerkung (16.15) ist ρ invertierbar und ρ^{-1} ist ebenfalls ein elementarer Zeilenoperator auf $R^{m\times n}$. Somit ist jede Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\big(A' \mid b'\big) = \rho\big((A \mid b)\big)$ auch eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\rho^{-1}(\rho\big((A \mid b)\big)) = \big(A' \mid b'\big)$, d.h. es gilt auch $\mathrm{Sol}(A',b') \subseteq \mathrm{Sol}(A,b)$.
Insgesamt gilt $\mathrm{Sol}(A,b) = \mathrm{Sol}(A',b')$.
Jeder beliebige Zeilenoperator ρ ist ein Kompositum von elementaren Zeilenoperatoren. Der allgemeine Fall folgt daher aus dem Spezialfall für elementare Zeilenoperatoren durch Induktion. □

Gauß-Eliminierung

Wir stellen nun ein Verfahren vor, das sogenannte Gaußsche Eliminationsverfahren, welches mittels Zeilenoperationen eine gegebene Matrix über einem Körper in eine Matrix in (reduzierter) Zeilenstufenform überführt.

(16.18) Satz (Gauß-Eliminierung)**.** Es seien ein Körper K, $m,n \in \mathbb{N}_0$ und $A \in K^{m\times n}$ gegeben.

(a) Es seien Tupel $(l_1,\dots,l_m)$, $(k_1,\dots,k_m)$, $(A'_1,\dots,A'_m)$, $(A_0,\dots,A_m)$ wie folgt rekursiv gegeben.
Für $i \in [1,m]$ sei

$$l_i := \min\{\mathrm{ech}_h(A_{i-1}) \mid h \in [i,m]\}.$$

Für $i \in [1,m]$ sei $k_i \in [i,m]$ gegeben mit

$$l_i = \mathrm{ech}_{k_i}(A_{i-1}),$$

sofern $l_i \le n$ ist, und durch $k_i := i$, falls $l_i > n$ ist.
Für $i \in [1,m]$ sei

$$A'_i := \mathrm{sw}_{i,k_i}(A_{i-1}).$$

Es sei

$$A_i := \begin{cases} A & \text{für } i = 0, \\ (\prod_{h\in[i+1,m]} \mathrm{add}_{h,i,-(A'_i)_{h,l_i}(A'_i)^{-1}_{i,l_i}})(A'_i) & \text{für } i \in [1,m], \text{ falls } l_i \le n, \\ A_{i-1} & \text{für } i \in [1,m], \text{ falls } l_i > n. \end{cases}$$

Dann gilt:

(i) Für $i \in [1,m]$, $h \in [i+1,m]$ ist

$$\mathrm{ech}_h(A_i) > \mathrm{ech}_i(A_i).$$

(ii) Für $i \in [1,m]$, $h \in [1,i-1]$ ist

$$\mathrm{ech}_h(A_i) < \mathrm{ech}_{h+1}(A_i).$$

(iii) Es ist A_m in Zeilenstufenform.

(b) Es sei A in Zeilenstufenform und es sei r die Zeilenstufenanzahl von A. Ferner seien Tupel $(l_1,\dots,l_r)$, $(A'_1,\dots,A'_r)$, $(A_1,\dots,A_{r+1})$ wie folgt rekursiv gegeben.
Für $i \in [1,r]$ sei

$$\begin{aligned} l_i &:= \mathrm{ech}_i(A_{i+1}), \\ A'_i &:= \mathrm{mul}_{i,(A_{i+1})_{i,l_i}^{-1}}(A_{i+1}). \end{aligned}$$

Es sei

$$A_i := \begin{cases} A & \text{für } i = r+1, \\ (\prod_{h\in[1,i-1]} \mathrm{add}_{h,i,-(A'_i)_{h,l_i}})(A'_i) & \text{für } i \in [1,r]. \end{cases}$$

Dann gilt:

(i) Für $i \in [1,r]$, $h \in [1,m]$ ist

$$\mathrm{ech}_h(A_i) = \mathrm{ech}_h(A).$$

Für $i \in [1,r]$, $h \in [i,r]$, $k \in [1,m]$ ist

$$A_{k,\mathrm{ech}_h} = \delta_{k,h}.$$

(ii) Es ist A_1 in reduzierter Zeilenstufenform.

(16.19) Algorithmus (Gauß-Eliminierung)**.**

(a) Algorithmus zur Berechnung einer Zeilenstufenform:

- Eingabe: $A \in K^{m\times n}$ für einen Körper K und gewisse $m,n \in \mathbb{N}_0$
- Ausgabe: $\rho(A) \in K^{m\times n}$ in Zeilenstufenform für einen Zeilenoperator ρ auf $K^{m\times n}$
- Verfahren:

```
function rowechelonform(A)
    for i from 1 to m do
        l := min {ech_h(A) | h ∈ [i,m]};
        if l ∈ [1,n] then
            wähle k ∈ [1,m] mit l = ech_k(A);
        else
            return A;
        end if;
        A := sw_{i,k}(A);
        for h ∈ [i+1,m] do
            A := add_{h,i,-A_{h,l} A_{i,l}^{-1}}(A);
        end for;
    end for;

    return A;
end function;
```

(b) Algorithmus zur Berechnung einer reduzierten Zeilenstufenform:

- Eingabe: $A \in K^{m\times n}$ für einen Körper K und gewisse $m, n \in \mathbb{N}_0$
- Ausgabe: $\rho(A) \in K^{m\times n}$ in reduzierter Zeilenstufenform für einen Zeilenoperator ρ auf $K^{m\times n}$
- Verfahren:

```
function reducedrowechelonform(A)
    A := rowechelonform(A);
    r := max {h ∈ [1,m] | ech_h(A) ∈ [1,n]};

    for i from r to 1 do
        l := ech_i(A);
        A := mul_{i,A_{i,l}^{-1}}(A);
        for h ∈ [1,i−1] do
            A := add_{h,i,−A_{h,l}}(A);
        end for;
    end for;

    return A;
end function;
```

(16.20) Korollar. Es seien ein Körper K, $m, n \in \mathbb{N}_0$ und $A \in K^{m\times n}$ gegeben.

(a) Es existiert ein Zeilenoperator ρ auf $K^{m\times n}$, welcher sich als Kompositum von Vertauschungs- und Additionsoperatoren schreiben lässt, so, dass $\rho(A)$ in Zeilenstufenform ist.

(b) Wenn A in Zeilenstufenform ist, dann existiert ein Zeilenoperator ρ auf $K^{m\times n}$, welcher sich als Kompositum von Multiplikations- und Additionsoperatoren schreiben lässt, so, dass $\rho(A)$ in reduzierter Zeilenstufenform und $\mathrm{ech}_i(\rho(A)) = \mathrm{ech}_i(A)$ für alle $i \in [1, m]$ ist.

(c) Es existiert ein Zeilenoperator ρ auf $K^{m\times n}$ so, dass $\rho(A)$ in reduzierter Zeilenstufenform ist.

(16.21) Beispiel. Es seien $B, B', B'' \in \mathbb{R}^{3\times 5}$ gegeben durch

$$B = \begin{pmatrix} 2 & 3 & -9 & -7 & -15 \\ -2 & 2 & -6 & -10 & -24 \\ 1 & 1 & -3 & -2 & -4 \end{pmatrix}, B' = \begin{pmatrix} 1 & 1 & -3 & -2 & -4 \\ 0 & 1 & -3 & -3 & -7 \\ 0 & 0 & 0 & -2 & -4 \end{pmatrix}, B'' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & -3 & 0 & -1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}.$$

Dann lässt sich B durch eine Folge elementarer Zeilenoperationen in die Matrix B' und in die Matrix B'' überführen.

Beweis. Wir benutzen das Gaußsche Eliminationsverfahren:

$$\begin{pmatrix} 2 & 3 & -9 & -7 & -15 \\ -2 & 2 & -6 & -10 & -24 \\ 1 & 1 & -3 & -2 & -4 \end{pmatrix} \overset{\mathrm{sw}_{1,3}}{\longmapsto} \begin{pmatrix} 1 & 1 & -3 & -2 & -4 \\ -2 & 2 & -6 & -10 & -24 \\ 2 & 3 & -9 & -7 & -15 \end{pmatrix}$$
$$\overset{\mathrm{add}_{3,1,-2}\circ\mathrm{add}_{2,1,2}}{\longmapsto} \begin{pmatrix} 1 & 1 & -3 & -2 & -4 \\ 0 & 4 & -12 & -14 & -32 \\ 0 & 1 & -3 & -3 & -7 \end{pmatrix} \overset{\mathrm{sw}_{2,3}}{\longmapsto} \begin{pmatrix} 1 & 1 & -3 & -2 & -4 \\ 0 & 1 & -3 & -3 & -7 \\ 0 & 4 & -12 & -14 & -32 \end{pmatrix}$$
$$\overset{\mathrm{add}_{3,2,-4}}{\longmapsto} \begin{pmatrix} 1 & 1 & -3 & -2 & -4 \\ 0 & 1 & -3 & -3 & -7 \\ 0 & 0 & 0 & -2 & -4 \end{pmatrix} \overset{\mathrm{mul}_{3,-\frac{1}{2}}}{\longmapsto} \begin{pmatrix} 1 & 1 & -3 & -2 & -4 \\ 0 & 1 & -3 & -3 & -7 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$
$$\overset{\mathrm{add}_{2,3,3}\circ\mathrm{add}_{1,3,2}}{\longmapsto} \begin{pmatrix} 1 & 1 & -3 & 0 & 0 \\ 0 & 1 & -3 & 0 & -1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix} \overset{\mathrm{add}_{1,2,-1}}{\longmapsto} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & -3 & 0 & -1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

□

Alternativer Beweis von Beispiel (16.3). Nach Beispiel (16.21), Proposition (16.17) und Proposition (16.10) ist

$$\mathrm{Sol}(\begin{pmatrix} -2 & 2 & -6 & -10 \\ 2 & 3 & -9 & -7 \\ 1 & 1 & -3 & -2 \end{pmatrix}, \begin{pmatrix} -24 \\ -15 \\ -4 \end{pmatrix}) = \mathrm{Sol}(\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix}) = \{\begin{pmatrix} 1 \\ -1 \\ 0 \\ 2 \end{pmatrix} + a \begin{pmatrix} 0 \\ 3 \\ 1 \\ 0 \end{pmatrix} \mid a \in \mathbb{R}\}$$

$$= \begin{pmatrix} 1 \\ -1 \\ 0 \\ 2 \end{pmatrix} + \mathbb{R} \begin{pmatrix} 0 \\ 3 \\ 1 \\ 0 \end{pmatrix}. \qquad \square$$

Elementarmatrizen

Als nächstes werden wir sehen, dass sich elementare Zeilenoperationen als Matrixmultiplikationen mit sogenannten Elementarmatrizen schreiben lassen.

(16.22) Definition (Elementarmatrizen)**.** Es sei ein kommutativer Ring R und $n \in \mathbb{N}_0$ gegeben.

(a) Für $k, l \in [1, n]$ heißt

$$\mathrm{Sw}_{k,l} := \mathrm{sw}_{k,l}(\mathrm{E}_n)$$

die *Vertauschungsmatrix* (oder die *Elementarmatrix* zum Vertauschungsoperator) der k-ten und l-ten Zeile.

(b) Für $k, l \in [1, n]$ mit $k \neq l$ und $c \in R$ heißt

$$\mathrm{Add}_{k,l,c} := \mathrm{add}_{k,l,c}(\mathrm{E}_n)$$

die *Additionsmatrix* (oder die *Elementarmatrix* zum Additionsoperator) des c-fachen der l-ten zur k-ten Zeile.

(c) Für $k \in [1, n]$, $c \in R^\times$ heißt

$$\mathrm{Mul}_{k,c} := \mathrm{mul}_{k,c}(\mathrm{E}_n)$$

die *Multiplikationsmatrix* (oder die *Elementarmatrix* zum Multiplikationsoperator) der k-ten Zeile um das c-fache.

(d) Eine *Elementarmatrix* in $R^{n\times n}$ ist ein $P \in R^{n\times n}$ von der Form $P = \mathrm{Sw}_{k,l}$ für gewisse $k, l \in [1, n]$ oder $P = \mathrm{Add}_{k,l,c}$ für gewisse $k, l \in [1, n]$ mit $k \neq l$ und $c \in R$ oder $P = \mathrm{Mul}_{k,c}$ für gewisse $k \in [1, n]$, $c \in R^\times$.

(16.23) Beispiel.

(a) In $\mathbb{Q}^{3\times 3}$ ist

$$\mathrm{Sw}_{2,3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

(b) In $\mathbb{Q}^{3\times 3}$ ist

$$\mathrm{Add}_{3,1,2} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}.$$

(c) In $\mathbb{Q}^{3\times 3}$ ist

$$\mathrm{Mul}_{2,-3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

(16.24) Bemerkung. Es seien ein kommutativer Ring R und $n \in \mathbb{N}_0$ gegeben.

(a) Für $k, l \in [1, n]$ gilt

$$(\mathrm{Sw}_{k,l})_{i,-} = \begin{cases} \mathrm{e}_l & \text{für } i = k, \\ \mathrm{e}_k & \text{für } i = l, \\ \mathrm{e}_i & \text{für } i \in [1, n] \setminus \{k, l\}. \end{cases}$$

(b) Für $k, l \in [1, n]$ mit $k \neq l$ und $c \in R$ gilt

$$(\mathrm{Add}_{k,l,c})_{i,-} = \begin{cases} \mathrm{e}_k + c\,\mathrm{e}_l & \text{für } i = k, \\ \mathrm{e}_i & \text{für } i \in [1, n] \setminus \{k\}. \end{cases}$$

(c) Für $k \in [1, n]$, $c \in R^\times$ gilt

$$(\mathrm{Mul}_{k,c})_{i,-} = \begin{cases} c\,\mathrm{e}_k & \text{für } i = k, \\ \mathrm{e}_i & \text{für } i \in [1, n] \setminus \{k\}. \end{cases}$$

Beweis.

(a) Für $k, l \in [1, n]$ gilt

$$(\mathrm{Sw}_{k,l})_{i,-} = (\mathrm{sw}_{k,l}(\mathrm{E}_n))_{i,-} = \left.\begin{cases} (\mathrm{E}_n)_{l,-}, & \text{falls } i = k, \\ (\mathrm{E}_n)_{k,-}, & \text{falls } i = l, \\ (\mathrm{E}_n)_{i,-}, & \text{falls } i \in [1, n] \setminus \{k, l\} \end{cases}\right\} = \begin{cases} \mathrm{e}_l, & \text{falls } i = k, \\ \mathrm{e}_k, & \text{falls } i = l, \\ \mathrm{e}_i, & \text{falls } i \in [1, n] \setminus \{k, l\}, \end{cases}$$

für $i \in [1, n]$.

(b) Für $k, l \in [1, n]$ mit $k \neq l$ und $c \in R$ gilt

$$\begin{aligned}(\mathrm{Add}_{k,l,c})_{i,-} = (\mathrm{add}_{k,l,c}(\mathrm{E}_n))_{i,-} &= \left.\begin{cases} (\mathrm{E}_n)_{k,-} + c\,(\mathrm{E}_n)_{l,-}, & \text{falls } i = k, \\ (\mathrm{E}_n)_{i,-}, & \text{falls } i \in [1, n] \setminus \{k\} \end{cases}\right\} \\ &= \begin{cases} \mathrm{e}_k + c\,\mathrm{e}_l, & \text{falls } i = k, \\ \mathrm{e}_i, & \text{falls } i \in [1, n] \setminus \{k\}, \end{cases}\end{aligned}$$

für $i \in [1, n]$.

(c) Für $k \in [1, n]$, $c \in R^\times$ gilt

$$(\mathrm{Mul}_{k,c})_{i,-} = (\mathrm{mul}_{k,c}(\mathrm{E}_n))_{i,-} = \left.\begin{cases} c\,(\mathrm{E}_n)_{k,-}, & \text{falls } i = k, \\ (\mathrm{E}_n)_{i,-}, & \text{falls } i \in [1, n] \setminus \{k\} \end{cases}\right\} = \begin{cases} c\,\mathrm{e}_k, & \text{falls } i = k, \\ \mathrm{e}_i, & \text{falls } i \in [1, n] \setminus \{k\}, \end{cases}$$

für $i \in [1, n]$. □

(16.25) Proposition. Es seien ein kommutativer Ring R, $m, n \in \mathbb{N}_0$ und $A \in R^{m \times n}$ gegeben.

(a) Für $k, l \in [1, m]$ gilt

$$\mathrm{sw}_{k,l}(A) = \mathrm{Sw}_{k,l}\, A.$$

(b) Für $k, l \in [1, m]$ mit $k \neq l$ und $c \in R$ gilt

$$\mathrm{add}_{k,l,c}(A) = \mathrm{Add}_{k,l,c}\, A.$$

(c) Für $k \in [1, m]$, $c \in R^\times$ gilt

$$\mathrm{mul}_{k,c}(A) = \mathrm{Mul}_{k,c}\, A.$$

Beweis.

(a) Für $k, l \in [1, m]$ gilt

$$(\mathrm{Sw}_{k,l}\, A)_{i,-} = \sum_{j \in [1,m]} (\mathrm{Sw}_{k,l})_{i,j} A_{j,-} = \left.\begin{cases} \sum_{j \in [1,m]} (\mathrm{e}_l)_j A_{j,-}, & \text{falls } i = k, \\ \sum_{j \in [1,m]} (\mathrm{e}_k)_j A_{j,-}, & \text{falls } i = l, \\ \sum_{j \in [1,m]} (\mathrm{e}_i)_j A_{j,-}, & \text{falls } i \in [1, m] \setminus \{k, l\} \end{cases}\right\}$$

$$= \begin{Bmatrix} \sum_{j\in[1,m]} \delta_{l,j} A_{j,-}, & \text{falls } i = k, \\ \sum_{j\in[1,m]} \delta_{k,j} A_{j,-}, & \text{falls } i = l, \\ \sum_{j\in[1,m]} \delta_{i,j} A_{j,-}, & \text{falls } i \in [1,m] \setminus \{k,l\} \end{Bmatrix} = \begin{Bmatrix} A_{l,-}, & \text{falls } i = k, \\ A_{k,-}, & \text{falls } i = l, \\ A_{i,-}, & \text{falls } i \in [1,m] \setminus \{k,l\} \end{Bmatrix}$$
$$= \mathrm{sw}_{k,l}(A)_{i,-}$$

für $i \in [1,m]$ und damit $\mathrm{Sw}_{k,l} A = \mathrm{sw}_{k,l}(A)$.

(b) Für $k,l \in [1,m]$ mit $k \neq l$ und $c \in R$ gilt

$$(\mathrm{Add}_{k,l,c} A)_{i,-} = \sum_{j\in[1,m]} (\mathrm{Add}_{k,l,c})_{i,j} A_{j,-} = \begin{Bmatrix} \sum_{j\in[1,m]} (\mathrm{e}_k + c\,\mathrm{e}_l)_j A_{j,-}, & \text{falls } i = k, \\ \sum_{j\in[1,m]} (\mathrm{e}_i)_j A_{j,-}, & \text{falls } i \in [1,m] \setminus \{k\} \end{Bmatrix}$$
$$= \begin{Bmatrix} \sum_{j\in[1,m]} (\delta_{k,j} + c\,\delta_{l,j}) A_{j,-}, & \text{falls } i = k, \\ \sum_{j\in[1,m]} \delta_{i,j} A_{j,-}, & \text{falls } i \in [1,m] \setminus \{k\} \end{Bmatrix}$$
$$= \begin{Bmatrix} A_{k,-} + cA_{l,-}, & \text{falls } i = k, \\ A_{i,-}, & \text{falls } i \in [1,m] \setminus \{k\} \end{Bmatrix} = \mathrm{add}_{k,l,c}(A)_{i,-}$$

für $i \in [1,m]$ und damit $\mathrm{Add}_{k,l,c} A = \mathrm{add}_{k,l,c}(A)$.

(c) Für $k \in [1,m]$, $c \in R^\times$ gilt

$$(\mathrm{Mul}_{k,c} A)_{i,-} = \sum_{j\in[1,m]} (\mathrm{Mul}_{k,c})_{i,j} A_{j,-} = \begin{Bmatrix} \sum_{j\in[1,m]} (c\,\mathrm{e}_k)_j A_{j,-}, & \text{falls } i = k, \\ \sum_{j\in[1,m]} (\mathrm{e}_i)_j A_{j,-}, & \text{falls } i \in [1,m] \setminus \{k\} \end{Bmatrix}$$
$$= \begin{Bmatrix} \sum_{j\in[1,m]} c\,\delta_{k,j} A_{j,-}, & \text{falls } i = k, \\ \sum_{j\in[1,m]} \delta_{i,j} A_{j,-}, & \text{falls } i \in [1,m] \setminus \{k\} \end{Bmatrix} = \begin{Bmatrix} cA_{k,-}, & \text{falls } i = k, \\ A_{i,-}, & \text{falls } i \in [1,m] \setminus \{k\} \end{Bmatrix}$$
$$= \mathrm{mul}_{k,c}(A)_{i,-}$$

für $i \in [1,m]$ und damit $\mathrm{Mul}_{k,c} A = \mathrm{mul}_{k,c}(A)$. □

(16.26) Korollar. Es seien ein kommutativer Ring R und ein $n \in \mathbb{N}_0$ gegeben.

(a) Für $k,l \in [1,n]$ ist $\mathrm{Sw}_{k,l} \in \mathrm{GL}_n(R)$ mit

$$\mathrm{Sw}_{k,l}^{-1} = \mathrm{Sw}_{l,k} = \mathrm{Sw}_{k,l}.$$

(b) Für $k,l \in [1,n]$ mit $k \neq l$ und $c \in R$ ist $\mathrm{Add}_{k,l,c} \in \mathrm{GL}_n(R)$ mit

$$\mathrm{Add}_{k,l,c}^{-1} = \mathrm{Add}_{k,l,-c}.$$

(c) Für $k \in [1,n]$, $c \in R^\times$ ist $\mathrm{Mul}_{k,c} \in \mathrm{GL}_n(R)$ mit

$$\mathrm{Mul}_{k,c}^{-1} = \mathrm{Mul}_{k,c^{-1}}.$$

Beweis.

(a) Für $k,l \in [1,n]$ gilt

$$\mathrm{Sw}_{k,l}\,\mathrm{Sw}_{k,l} = \mathrm{sw}_{k,l}(\mathrm{sw}_{k,l}(\mathrm{E}_n)) = \mathrm{E}_n$$

nach Proposition (16.25)(a) und Bemerkung (16.15)(a), d.h. $\mathrm{Sw}_{k,l} \in \mathrm{GL}_n(R)$ mit $\mathrm{Sw}_{k,l}^{-1} = \mathrm{Sw}_{k,l} = \mathrm{sw}_{k,l}(\mathrm{E}_n) = \mathrm{sw}_{l,k}(\mathrm{E}_n) = \mathrm{Sw}_{l,k}$.

(b) Für $k,l \in [1,n]$ mit $k \neq l$ und $c \in R$ gilt

$$\mathrm{Add}_{k,l,-c}\,\mathrm{Add}_{k,l,c} = \mathrm{add}_{k,l,-c}(\mathrm{add}_{k,l,c}(\mathrm{E}_n)) = \mathrm{E}_n,$$
$$\mathrm{Add}_{k,l,c}\,\mathrm{Add}_{k,l,-c} = \mathrm{add}_{k,l,c}(\mathrm{add}_{k,l,-c}(\mathrm{E}_n)) = \mathrm{E}_n$$

nach Proposition (16.25)(b) und Bemerkung (16.15)(b), d.h. $\mathrm{Add}_{k,l,c} \in \mathrm{GL}_n(R)$ mit $\mathrm{Add}_{k,l,c}^{-1} = \mathrm{Add}_{k,l,-c}$.

(c) Für $k \in [1,n]$, $c \in R^\times$ gilt

$$\begin{aligned}\mathrm{Mul}_{k,c^{-1}} \mathrm{Mul}_{k,c} &= \mathrm{mul}_{k,c^{-1}}(\mathrm{mul}_{k,c}(\mathrm{E}_n)) = \mathrm{E}_n,\\ \mathrm{Mul}_{k,c} \mathrm{Mul}_{k,c^{-1}} &= \mathrm{mul}_{k,c}(\mathrm{mul}_{k,c^{-1}}(\mathrm{E}_n)) = \mathrm{E}_n\end{aligned}$$

nach Proposition (16.25)(c) und Bemerkung (16.15)(c), d.h. $\mathrm{Mul}_{k,c} \in \mathrm{GL}_n(R)$ mit $\mathrm{Mul}_{k,c}^{-1} = \mathrm{Mul}_{k,c^{-1}}$. □

(16.27) Korollar. Es seien ein kommutativer Ring R, $m,n \in \mathbb{N}_0$ und ein Zeilenoperator ρ auf $R^{m\times n}$ gegeben. Ferner sei ρ' der entsprechende Zeilenoperator auf $R^{m\times m}$. Dann ist $\rho'(\mathrm{E}_m) \in \mathrm{GL}_m(R)$ und für $A \in R^{m\times n}$ gilt

$$\rho(A) = \rho'(\mathrm{E}_m)\, A.$$

Beweis. Es seien $k \in \mathbb{N}_0$, elementare Zeilenoperatoren ρ_i auf $R^{m\times n}$ für $i \in [1,k]$ mit $\rho = \rho_k \circ \ldots \circ \rho_1$ gegeben. Ferner sei ρ_i' für $i \in [1,k]$ der zu ρ_i entsprechende elementare Zeilenoperator auf $R^{m\times m}$, so dass $\rho' = \rho_k' \circ \ldots \circ \rho_1'$ gilt. Nach Proposition (16.25) gilt

$$\rho'(\mathrm{E}_m) = \rho_k'(\ldots(\rho_1'(\mathrm{E}_m))) = \rho_k'(\mathrm{E}_m)\ldots\rho_1'(\mathrm{E}_m),$$

d.h. $\rho'(\mathrm{E}_m)$ ist ein Produkt von Elementarmatrizen. Jede Elementarmatrix ist nach Korollar (16.26) invertierbar, also auch $\rho'(\mathrm{E}_m)$ nach Proposition (6.27)(a). Für $A \in K^{m\times n}$ gilt ferner

$$\rho(A) = \rho_k(\ldots(\rho_1(A))) = \rho_k'(\mathrm{E}_m)\ldots\rho_1'(\mathrm{E}_m)\, A = \rho'(\mathrm{E}_m)\, A$$

nach Proposition (16.25). □

Inversion von Matrizen

Unsere Erkenntnisse über Zeilenoperationen und Elementarmatrizen erlauben uns, einen Algorithmus anzugeben, welcher von einer quadratischen Matrix über einem Körper entscheidet, ob diese invertierbar ist, und gegebenfalls die Inverse zu berechnen:

(16.28) Satz (Invertierbarkeitskriterium und Inversenbestimmung)**.** Es seien ein Körper K, $n \in \mathbb{N}_0$ und $A \in K^{n\times n}$ gegeben.

(a) Die folgenden Bedingungen sind äquivalent.

(i) Es ist $A \in \mathrm{GL}_n(K)$.

(ii) Für jeden Zeilenoperator ρ auf $K^{n\times n}$ gilt: Wenn $\rho(A)$ in reduzierter Zeilenstufenform ist, dann ist $\rho(A) = \mathrm{E}_n$.

(iii) Es gibt einen Zeilenoperator ρ auf $K^{n\times n}$ mit $\rho(A) = \mathrm{E}_n$.

(b) Es sei ein Zeilenoperator ρ auf $K^{n\times n}$ mit $\rho(A) = \mathrm{E}_n$ gegeben. Dann ist

$$A^{-1} = \rho(\mathrm{E}_n).$$

Beweis. Zunächst gelte Bedingung (a)(i), d.h. es sei $A \in \mathrm{GL}_n(K)$, und es sei ein Zeilenoperator ρ auf $K^{n\times n}$ so gegeben, dass $\rho(A)$ in reduzierter Zeilenstufenform ist. Nach Korollar (16.27) gibt es ein $R \in \mathrm{GL}_n(K)$ mit $\rho(A) = RA$. Mit A und R ist dann aber auch $\rho(A) = RA$ invertierbar. Insbesondere hat $\rho(A)$ keine Nullzeilen, d.h. die Zeilenstufenanzahl von $\rho(A)$ ist n. Da aber $\rho(A)$ in reduzierter Zeilenstufenform ist, impliziert dies bereits $\rho(A) = \mathrm{E}_n$, d.h. Bedingung (a)(ii) gilt.
Als nächstes gelte Bedingung (a)(ii), d.h. für jeden elementaren Zeilenoperator ρ auf $K^{n\times n}$ so, dass $\rho(A)$ in reduzierter Zeilenstufenform ist, gelte $\rho(A) = \mathrm{E}_n$. Da es nach Korollar (16.20)(c) stets einen solchen Zeilenoperator ρ auf $K^{n\times n}$ gibt, impliziert dies bereits die Gültigkeit von Bedingung (a)(iii).
Schließlich gelte Bedingung (a)(iii), d.h. es gebe einen Zeilenoperator ρ auf $K^{n\times n}$ mit $\rho(A) = \mathrm{E}_n$. Nach Korollar (16.27) ist $\rho(\mathrm{E}_n) \in \mathrm{GL}_n(K)$ und es gilt $\mathrm{E}_n = \rho(A) = \rho(\mathrm{E}_n)\, A$. Dies impliziert $\rho(\mathrm{E}_n)^{-1} = A$ nach Bemerkung (6.15). Nach Proposition (6.27)(c) ist dann aber auch $A = \rho(\mathrm{E}_n)^{-1}$ invertierbar mit

$$A^{-1} = (\rho(\mathrm{E}_n)^{-1})^{-1} = \rho(\mathrm{E}_n),$$

d.h. Bedingung (a)(i) gilt.
Insgesamt sind Bedingung (a)(i), Bedingung (a)(ii) und Bedingung (a)(iii) äquivalent. □

Das Gaußsche Eliminationsverfahren (16.18) liefert zu einer gegebenen Matrix $A \in K^{n\times n}$ für einen Körper K und ein $n \in \mathbb{N}_0$ einen Zeilenoperator ρ auf $K^{n\times n}$ so, dass $\rho(A)$ in reduzierter Zeilenstufenform ist. Das Invertierbarkeitskriterium (16.28) besagt nun, dass A genau dann invertierbar ist, wenn $\rho(A) = \mathrm{E}_n$ ist, und dass in diesem Fall $A^{-1} = \rho(\mathrm{E}_n)$ gilt. Wenn A invertierbar ist, so können wir also die zusammengesetzte Matrix $\left(A \mid \mathrm{E}_n\right)$ durch eine Zeilenoperation auf die Matrix $\left(\mathrm{E}_n \mid A^{-1}\right)$ in reduzierter Zeilenstufenform bringen.

(16.29) Beispiel. Es sei $A \in \mathbb{Q}^{3\times 3}$ gegeben durch

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Dann ist $A \in \mathrm{GL}_3(\mathbb{Q})$ mit

$$A^{-1} = \begin{pmatrix} -1 & 1 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix}.$$

Beweis. Wir wenden elementare Zeilenoperationen auf die Matrix $\left(A \mid \mathrm{E}_3\right)$ an:

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \xmapsto{\mathrm{add}_{1,2,-1}} \left(\begin{array}{ccc|ccc} 0 & 0 & 1 & 1 & -1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \xmapsto{\mathrm{add}_{3,1,-1}} \left(\begin{array}{ccc|ccc} 0 & 0 & 1 & 1 & -1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 & 1 & 1 \end{array}\right)$$

$$\xmapsto{\mathrm{add}_{2,3,-1}} \left(\begin{array}{ccc|ccc} 0 & 0 & 1 & 1 & -1 & 0 \\ 0 & 1 & 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & -1 & 1 & 1 \end{array}\right) \xmapsto{\mathrm{sw}_{1,3}} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 & -1 & 0 \end{array}\right)$$

Nach dem Invertierbarkeitskriterium (16.28) ist A invertierbar mit

$$A^{-1} = \begin{pmatrix} -1 & 1 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix}.$$

□

Lineare Gleichungen über kommutativen Ringen

Lineare Gleichungssysteme über kommutativen Ringen sind meist deutlich schwieriger zu lösen als über Körpern. Wir fassen hier lediglich die bereits studierten Ergebnisse über lineare Gleichungen aus den Abschnitten 12 und 13 noch einmal zusammen.

(16.30) Definition (Lösung einer linearen Gleichung)**.** Es seien ein kommutativer Ring R und $n \in \mathbb{N}_0$ gegeben.

(a) Es seien $a \in R^{1\times n}$ und $b \in R^{1\times 1}$ gegeben. Die Lösungsmenge $\mathrm{Sol}(a, b)$ des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(a \mid b\right)$ wird auch *Lösungsmenge der linearen Gleichung* zur erweiterten Koeffizientenmatrix $\left(a \mid b\right)$ genannt. Ein Element von $\mathrm{Sol}(a, b)$ wird auch *Lösung der linearen Gleichung* zur erweiterten Koeffizientenmatrix $\left(a \mid b\right)$ genannt.

(b) Es sei $a \in R^{1\times n}$ gegeben. Die Lösungsmenge $\mathrm{Sol}(a, 0)$ der linearen Gleichung zur erweiterten Koeffizientenmatrix $\left(a \mid 0\right)$ wird auch *Lösungsmenge der homogenen linearen Gleichung* zur Koeffizientenmatrix a genannt. Ein Element von $\mathrm{Sol}(a, 0)$ wird auch *Lösung der homogenen linearen Gleichung* zur Koeffizientenmatrix a genannt.

(16.31) Beispiel.

(a) Es ist

$$\mathrm{Sol}(\begin{pmatrix} 2238 & 168 \end{pmatrix}, \begin{pmatrix} -24 \end{pmatrix}) = \begin{pmatrix} 12 \\ -160 \end{pmatrix} + \mathbb{Z} \begin{pmatrix} 28 \\ -373 \end{pmatrix}.$$

(b) Es ist

$$\mathrm{Sol}(\begin{pmatrix} 2238 & 168 \end{pmatrix}, \begin{pmatrix} 4 \end{pmatrix}) = \emptyset.$$

Beweis. Dies folgt aus Beispiel (12.30). □

(16.32) Bemerkung (Lösbarkeitskriterium und Lösungsbestimmung für lineare Gleichungen in 2 Unbekannten über $\mathbb{Z}$ bzw. $K[X]$)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a \in R^{1\times 2}$ und $b \in R^{1\times 1}$ gegeben.

(a) Genau dann gibt es eine Lösung der linearen Gleichung zur erweiterten Koeffizientenmatrix $\left(a \mid b\right)$, wenn

$$\gcd(a_1, a_2) \mid b$$

gilt. ([50])

(b) Es seien $p_1, p_2, q \in R$ mit $a_1 = p_1 \gcd(a_1, a_2)$, $a_2 = p_2 \gcd(a_1, a_2)$ und $b = q \gcd(a_1, a_2)$ gegeben. Ferner sei $x' \in \mathrm{Sol}(a, \gcd(a_1, a_2))$ gegeben. Dann ist

$$\mathrm{Sol}(a, b) = \begin{cases} R^{2\times 1}, & \text{falls } a = 0, \\ qx' + R \begin{pmatrix} p_2 \\ -p_1 \end{pmatrix}, & \text{falls } a \neq 0. \end{cases}$$

Beweis. Dies folgt aus Satz (12.29). □

(16.33) Bemerkung (Lösbarkeitskriterium und Lösungsbestimmung für lineare Gleichungen in einer Unbekannten über $\mathbb{Z}/n$ bzw. $K[X]/f$)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $m \in R$ und $a, b \in R$ gegeben.

(a) Genau dann gibt es eine Lösung der linearen Gleichung zur erweiterten Koeffizientenmatrix $\left([a]_m \mid [b]_m\right)$, wenn

$$\gcd(m, a) \mid b$$

gilt.

(b) Es seien $p, q, r \in R$ mit $m = p \gcd(m, a)$, $a = q \gcd(m, a)$ und $b = r \gcd(m, a)$ gegeben. Ferner sei $x' \in R$ mit $[x'] = [q]^{-1}$ in R/p gegeben. Dann ist

$$\mathrm{Sol}([a]_m, [b]_m) = \begin{cases} R/m, & \text{falls } (m, a) = (0, 0), \\ [r]_m [x']_m + (R/m)\,[p]_m, & \text{falls } (m, a) \neq (0, 0). \end{cases}$$

Beweis. Dies folgt aus Satz (13.21). □

17 Kombinatorische Funktionen

Bevor wir im nächsten Abschnitt zu kombinatorischen Problemen und zugehörigen Lösungsansätzen kommen, führen wir nun einige Funktionen ein, welche uns dann im nächsten Abschnitt immer wieder begegnen werden.

Fakultäten

Wir beginnen mit der Fakultätsfunktion. Im nächsten Abschnitt wird diese bei der Bestimmung der Anzahl von Permutationen auftreten, siehe Korollar (18.31) und Korollar (18.32).

(17.1) Definition (Fakultät)**.** Für $n \in \mathbb{N}_0$ heißt

$$n! = \prod_{i \in [1,n]} i,$$

gelesen n *fakultät*, die *Fakultät* von n.

[50] Unter Missbrauch der Notation notieren wir hier den Eintrag $b_1 = b_{1,1}$ von $b \in R^{1\times 1}$ als b.

(17.2) Beispiel. Es gilt

$$0! = 1,$$
$$1! = 1,$$
$$2! = 2,$$
$$3! = 6,$$
$$4! = 24.$$

Beweis. Es gilt

$$0! = \prod_{i\in[1,0]} i = 1,$$
$$1! = \prod_{i\in[1,1]} i = 1,$$
$$2! = \prod_{i\in[1,2]} i = 1 \cdot 2 = 2,$$
$$3! = \prod_{i\in[1,3]} i = 1 \cdot 2 \cdot 3 = 6,$$
$$4! = \prod_{i\in[1,4]} i = 1 \cdot 2 \cdot 3 \cdot 4 = 24.$$ □

Die Fakultätsfunktion erfüllt folgende Rekursionsgleichung:

(17.3) Bemerkung. Es gilt

$$n! = \begin{cases} 1, & \text{für } n = 0, \\ (n-1)!\, n, & \text{für } n \in \mathbb{N}. \end{cases}$$

Beweis. Für $n = 0$ gilt

$$n! = \prod_{i\in[1,0]} i = 1,$$

und für $n \in \mathbb{N}$ gilt

$$n! = \prod_{i\in[1,n]} i = (\prod_{i\in[1,n-1]} i)\, n = (n-1)!\, n.$$ □

Binomialkoeffizienten

Als nächstes kommen wir zu den Binomialkoeffizienten, welche im nächsten Abschnitt bei der Bestimmung der Anzahl von Kombinationen und Multikombinationen auftreten werden, siehe Korollar (18.62) und Korollar (18.50).

(17.4) Definition (Binomialkoeffizient)**.** Für $n \in \mathbb{Z}$, $k \in \mathbb{N}_0$ heißt

$$\binom{n}{k} = \frac{\prod_{i\in[1,k]}(n-i+1)}{k!},$$

gelesen n *über* k, der *Binomialkoeffizient* von n über k.

Im Regelfall werden wir nur Binomialkoeffizienten $\binom{n}{k}$ für $n, k \in \mathbb{N}_0$ betrachten.

(17.5) Beispiel. Es gilt

$$\binom{5}{3} = 10.$$

Beweis. Es gilt

$$\binom{5}{3} = \frac{\prod_{i\in[1,3]}(5-i+1)}{3!} = \frac{5\cdot 4\cdot 3}{1\cdot 2\cdot 3} = 10. \qquad \square$$

(17.6) Bemerkung. Für $n, k \in \mathbb{N}_0$ mit $k > n$ gilt

$$\binom{n}{k} = 0.$$

Beweis. Für $n, k \in \mathbb{N}_0$ mit $k > n$ ist $n+1 \in [1,k]$, also

$$\prod_{i\in[1,k]} (n-i+1) = \prod_{i\in[1,k]\setminus\{n+1\}} (n-i+1)\cdot(n-(n+1)+1) = 0$$

und damit

$$\binom{n}{k} = \frac{\prod_{i\in[1,k]}(n-i+1)}{k!} = 0. \qquad \square$$

Die Binomialkoeffizienten erfüllen folgende Rekursionsgleichung:

(17.7) Proposition. Es gilt

$$\binom{n}{k} = \begin{cases} 1, & \text{für } n \in \mathbb{Z},\ k = 0, \\ 0, & \text{für } n = 0,\ k \in \mathbb{N}, \\ \binom{n-1}{k} + \binom{n-1}{k-1}, & \text{für } n \in \mathbb{Z},\ k \in \mathbb{N}. \end{cases}$$

Beweis. Für $n \in \mathbb{Z}$, $k = 0$ gilt

$$\binom{n}{k} = \binom{n}{0} = \frac{\prod_{i\in[1,0]}(n-i+1)}{0!} = \frac{1}{1} = 1.$$

Für $n = 0$, $k \in \mathbb{N}$ gilt

$$\binom{n}{k} = \binom{0}{k} = 0$$

nach Bemerkung (17.6). Für $n \in \mathbb{Z}$, $k \in \mathbb{N}$ gilt

$$\begin{aligned} \binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{\prod_{i\in[1,k]}(n-1-i+1)}{k!} + \frac{\prod_{i\in[1,k-1]}(n-1-i+1)}{(k-1)!} \\ &= \frac{\prod_{i\in[1,k-1]}(n-i)\cdot(n-k) + \prod_{i\in[1,k-1]}(n-i)\cdot k}{k!} \\ &= \frac{\prod_{i\in[1,k-1]}(n-i)\cdot(n-k+k)}{k!} = \frac{\prod_{i\in[0,k-1]}(n-i)}{k!} = \frac{\prod_{i\in[1,k]}(n-i+1)}{k!} \\ &= \binom{n}{k}. \end{aligned}$$ $\square$

(17.8) Korollar.

(a) Für $n \in \mathbb{Z}$, $k \in \mathbb{N}_0$ ist $\binom{n}{k} \in \mathbb{Z}$.

(b) Für $n, k \in \mathbb{N}_0$ ist $\binom{n}{k} \in \mathbb{N}_0$.

Beweis. Dies sei dem Leser zur Übung überlassen. $\square$

(17.9) Korollar. Für $n \in \mathbb{Z}$, $k \in \mathbb{N}_0$ gilt

$$\binom{k+n}{k} = \sum_{i\in[0,k]} \binom{i+n-1}{i}$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

Nach Proposition (17.7) lassen sich die Binomialkoeffizienten nicht-negativer ganzer Zahlen rekursiv im sogenannten *Pascalschen Dreieck* berechnen:

(17.10) Beispiel. Die Binomialkoeffizienten $\binom{n}{k}$ für $n, k \in [0,4]$ sind wie folgt gegeben.

$\binom{n}{k}$	0	1	2	3	4	k
0	1	0	0	0	0	
1	1	1	0	0	0	
2	1	2	1	0	0	
3	1	3	3	1	0	
4	1	4	6	4	1	
n						

(17.11) Proposition. Für $n \in \mathbb{N}_0$, $k \in [0,n]$ gilt

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

Beweis. Es seien $n \in \mathbb{N}_0$, $k \in [0,n]$ gegeben. Dann ist $[1,k] \to [n-k+1,n]$, $i \mapsto n-i+1$ eine wohldefinierte Bijektion mit Inverser $[n-k+1,n] \to [1,k]$, $j \mapsto n-j+1$. Folglich gilt

$$\binom{n}{k} = \frac{\prod_{i\in[1,k]}(n-i+1)}{k!} = \frac{\prod_{j\in[n-k+1,n]} j}{k!} = \frac{\prod_{j\in[1,n]} j}{k! \prod_{j\in[1,n-k]} j} = \frac{n!}{k!\,(n-k)!}.$$ □

(17.12) Korollar. Für alle $n \in \mathbb{N}_0$, $k \in [0,n]$ gilt

$$\binom{n}{n-k} = \binom{n}{k}.$$

Beweis. Nach Proposition (17.11) gilt

$$\binom{n}{n-k} = \frac{n!}{(n-k)!\,(n-(n-k))!} = \frac{n!}{(n-k)!\,k!} = \binom{n}{k}$$

für alle $n, k \in \mathbb{N}_0$. □

(17.13) Proposition (binomischer Lehrsatz)**.** Es seien ein Ring R und $x, y \in R$ mit $xy = yx$ gegeben. Für $n \in \mathbb{N}_0$ gilt

$$(x+y)^n = \sum_{k\in[0,n]} \binom{n}{k} x^k y^{n-k}.$$

Beweis. Wir führen Induktion nach n. Für $n = 0$ gilt

$$(x+y)^n = (x+y)^0 = 1 = \binom{0}{0} x^0 y^0 = \sum_{k\in[0,0]} \binom{0}{k} x^k y^{0-k} = \sum_{k\in[0,n]} \binom{n}{k} x^k y^{n-k}.$$

Es sei also $n \in \mathbb{N}$ mit

$$(x+y)^{n-1} = \sum_{k\in[0,n-1]} \binom{n-1}{k} x^k y^{n-1-k}$$

gegeben. Nach Proposition (17.7) gilt dann auch

$$\begin{aligned}(x+y)^n &= (x+y)^{n-1}(x+y) = \Big(\sum_{k\in[0,n-1]} \binom{n-1}{k} x^k y^{n-1-k}\Big)(x+y) \\ &= \sum_{k\in[0,n-1]} \binom{n-1}{k} x^k y^{n-1-k} x + \sum_{k\in[0,n-1]} \binom{n-1}{k} x^k y^{n-1-k} y\end{aligned}$$

$$
\begin{aligned}
&= \sum_{k\in[0,n-1]} \binom{n-1}{k} x^{k+1} y^{n-1-k} + \sum_{k\in[0,n-1]} \binom{n-1}{k} x^k y^{n-k} \\
&= \sum_{k\in[1,n]} \binom{n-1}{k-1} x^k y^{n-k} + \sum_{k\in[0,n-1]} \binom{n-1}{k} x^k y^{n-k} \\
&= \sum_{k\in[1,n-1]} \binom{n-1}{k-1} x^k y^{n-k} + \binom{n-1}{n-1} x^n y^{n-n} + \binom{n-1}{0} x^0 y^{n-0} + \sum_{k\in[1,n-1]} \binom{n-1}{k} x^k y^{n-k} \\
&= \binom{n-1}{0} x^0 y^{n-0} + \sum_{k\in[1,n-1]} (\binom{n-1}{k-1} + \binom{n-1}{k}) x^k y^{n-k} + \binom{n-1}{n-1} x^n y^{n-n} \\
&= \binom{n}{0} x^0 y^{n-0} + \sum_{k\in[1,n-1]} \binom{n}{k} x^k y^{n-k} + \binom{n}{n} x^n y^{n-n} = \sum_{k\in[0,n]} \binom{n}{k} x^k y^{n-k}.
\end{aligned}
$$

Nach dem Induktionsprinzip gilt

$$(x+y)^n = \sum_{k\in[0,n]} \binom{n}{k} x^k y^{n-k}$$

für alle $n \in \mathbb{N}_0$. □

(17.14) Korollar. Für $n \in \mathbb{N}_0$ gilt

$$\sum_{k\in\mathbb{N}_0} \binom{n}{k} = \sum_{k\in[0,n]} \binom{n}{k} = 2^n.$$

Beweis. Es sei $n \in \mathbb{N}_0$ gegeben. Für $k \in \mathbb{N}_0 \setminus [0,n]$ ist dann $\binom{n}{k} = 0$ nach (17.6). Nach dem binomischen Lehrsatz (17.13) folgt

$$\sum_{k\in\mathbb{N}_0} \binom{n}{k} = \sum_{k\in[0,n]} \binom{n}{k} = \sum_{k\in[0,n]} \binom{n}{k} \cdot 1^k \cdot 1^{n-k} = (1+1)^n = 2^n.$$ □

Multinomialkoeffizienten

Binomialkoeffizienten lassen sich zu sogenannten Multinomialkoeffizienten verallgemeinern, welche im nächsten Abschnitt bei der Bestimmung der Anzahl von Kombinationen über mehreren Indexmengen sowie der Anzahl der Repräsentanten von Multikombinationen auftreten werden, siehe Korollar (18.95) und Korollar (18.102).

(17.15) Definition (Multinomialkoeffizient)**.** Für $n \in \mathbb{Z}$, $r \in \mathbb{N}_0$, $k \in \mathbb{N}_0^r$ heißt

$$\binom{n}{k} = \binom{n}{k_1, \ldots, k_r} := \frac{\prod_{i\in[1,\sum_{j\in[1,r]} k_j]} (n-i+1)}{\prod_{j\in[1,r]} k_j!},$$

gelesen *n über k* (oder *n über $k_1, \ldots, k_r$*), der *Multinomialkoeffizient* von n über k.

(17.16) Beispiel. Es gilt

$$\binom{7}{3,2} = 210.$$

Beweis. Es gilt

$$\binom{7}{3,2} = \frac{\prod_{i\in[1,3+2]} (7-i+1)}{3!\cdot 2!} = \frac{7\cdot 6\cdot 5\cdot 4\cdot 3}{1\cdot 2\cdot 3\cdot 1\cdot 2} = 210.$$ □

Viele der obigen Aussagen über Binomialkoeffizienten lassen sich ebenfalls zu Aussagen über Multinomialkoeffizienten verallgemeinern. Wir überlassen die Beweise dem Leser.

(17.17) Bemerkung. Für $n, r \in \mathbb{N}_0$, $k \in \mathbb{N}_0^r$ mit $\sum_{j\in[1,r]} k_j > n$ gilt

$$\binom{n}{k} = 0.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(17.18) Proposition. Es gilt

$$\binom{n}{k} = \begin{cases} 1, & \text{für } n \in \mathbb{Z},\ r \in \mathbb{N}_0,\ k = 0, \\ 0, & \text{für } n = 0,\ r \in \mathbb{N},\ k \in \mathbb{N}_0^r \setminus \{0\}, \\ \binom{n}{k_1,\ldots,k_{l-1},k_{l+1},\ldots,k_r}, & \text{für } n \in \mathbb{Z},\ r \in \mathbb{N},\ l \in [1,r],\ k \in \mathbb{N}_0^r \text{ mit } k_l = 0, \\ \binom{n-1}{k} + \sum_{l\in[1,r]} \binom{n-1}{k_1,\ldots,k_{l-1},k_l-1,k_{l+1},\ldots,k_r}, & \text{für } n \in \mathbb{Z},\ r \in \mathbb{N},\ k \in \mathbb{N}^r. \end{cases}$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(17.19) Korollar.

(a) Für $n \in \mathbb{Z}$, $r \in \mathbb{N}_0$, $k \in \mathbb{N}_0^r$ ist $\binom{n}{k} \in \mathbb{Z}$.

(b) Für $n, r \in \mathbb{N}_0$, $k \in \mathbb{N}_0^r$ ist $\binom{n}{k} \in \mathbb{N}_0$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(17.20) Bemerkung. Für $n \in \mathbb{Z}$, $r \in \mathbb{N}$, $k \in \mathbb{N}_0^r$ gilt

$$\binom{n}{k} = \binom{n}{k_1,\ldots,k_{r-1}} \binom{n - \sum_{l\in[1,r-1]} k_l}{k_r}.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(17.21) Korollar. Für $n \in \mathbb{Z}$, $r \in \mathbb{N}$, $k \in \mathbb{N}_0^r$ gilt

$$\binom{n}{k} = \prod_{j\in[1,r]} \binom{n - \sum_{l\in[1,j-1]} k_l}{k_j}.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(17.22) Proposition. Es seien $n, r \in \mathbb{N}_0$ und $k \in \mathbb{N}_0^r$ gegeben.

(a) Wenn $\sum_{i\in[1,r]} k_i \leq n$ gilt, dann ist

$$\binom{n}{k_1,\ldots,k_r} = \frac{n!}{\prod_{j\in[1,r]} k_j! \cdot (n - \sum_{i\in[1,r]} k_i)!}.$$

(b) Wenn $\sum_{i\in[1,r]} k_i = n$ gilt, dann ist

$$\binom{n}{k_1,\ldots,k_r} = \frac{n!}{\prod_{j\in[1,r]} k_j!}.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(17.23) Korollar. Für $n, r \in \mathbb{N}_0$, $k \in \mathbb{N}_0^r$ mit $\sum_{i\in[1,r]} k_i \leq n$ gilt

$$\binom{n}{k_1,\ldots,k_r} = \binom{n}{k_1,\ldots,k_r, n - \sum_{i\in[1,r]} k_i}.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(17.24) Proposition (Multinomialsatz)**.** Es seien ein Ring R, $r \in \mathbb{N}_0$ und $x = (x_1, \ldots, x_r) \in R^r$ mit $x_i x_j = x_j x_i$ für $i, j \in [1, r]$ gegeben. Für $n \in \mathbb{N}_0$ gilt

$$(\sum_{j\in[1,r]} x_j)^n = \sum_{\substack{k\in\mathbb{N}_0^r \\ \sum_{j\in[1,r]} k_j = n}} \binom{n}{k} \prod_{j\in[1,r]} x_j^{k_j}.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(17.25) Korollar. Für $n, r \in \mathbb{N}_0$ ist

$$\sum_{\substack{k\in\mathbb{N}_0^r \\ \sum_{j\in[1,r]} k_j = n}} \binom{n}{k} = r^n.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

Stirlingzahlen

Schließlich führen wir die sogenannten Stirlingzahlen ein, welche analog zu den Binomialkoeffizienten eine Rekursionsgleichung erfüllen, vgl. Proposition (17.7), und über diese definiert werden können. Im Gegensatz zu den Binomialkoeffizienten werden wir die Stirlingzahlen in beiden Argumenten für ganze Zahlen definieren. Im nächsten Abschnitt werden die Stirlingzahlen bei der Bestimmung der Anzahlen von Partitionen und Permutationen auftreten, siehe Korollar (18.133) und Korollar (18.152).

(17.26) Proposition. Es gibt genau eine Abbildung $\left\{ {-} \atop {=} \right\} \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(n, k) \mapsto \left\{ {n} \atop {k} \right\}$ mit

$$\left\{ {n} \atop {k} \right\} = \begin{cases} 1, & \text{für } n = 0,\ k = 0, \\ 0, & \text{für } n \in \mathbb{Z} \setminus \{0\},\ k = 0 \text{ und für } n = 0,\ k \in \mathbb{Z} \setminus \{0\}, \end{cases}$$

und so, dass die folgenden drei äquivalenten Bedingungen erfüllt sind.

- Für $n, k \in \mathbb{Z}$ gilt $\left\{ {n} \atop {k} \right\} = k \left\{ {n-1} \atop {k} \right\} + \left\{ {n-1} \atop {k-1} \right\}$.
- Für $n, k \in \mathbb{Z}$ gilt $\left\{ {n} \atop {k} \right\} = \frac{1}{k}(\left\{ {n+1} \atop {k} \right\} - \left\{ {n} \atop {k-1} \right\})$.
- Für $n, k \in \mathbb{Z}$ gilt $\left\{ {n} \atop {k} \right\} = \left\{ {n+1} \atop {k+1} \right\} - (k+1)\left\{ {n} \atop {k+1} \right\}$.

Diese Abbildung erfüllt

$$\left\{ {n} \atop {k} \right\} = \begin{cases} 1, & \text{für } n, k \in \mathbb{Z} \text{ mit } n = k, \\ 0, & \text{für } n, k \in \mathbb{Z} \text{ mit } n < k \text{ und mit } n \geq 0,\ k < 0. \end{cases}$$

Beweis. Es gibt genau eine Abbildung $\left\{ {-} \atop {=} \right\} \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(n, k) \mapsto \left\{ {n} \atop {k} \right\}$ mit $\left\{ {n} \atop {k} \right\}$ für $n, k \in \mathbb{Z}$ gegeben durch

$$\left\{ {n} \atop {k} \right\} = \begin{cases} 1, & \text{falls } n = 0,\ k = 0, \\ 0, & \text{falls } n > 0,\ k = 0, \\ 0, & \text{falls } n < 0,\ k = 0, \\ 0, & \text{falls } n = 0,\ k > 0, \\ k \left\{ {n-1} \atop {k} \right\} + \left\{ {n-1} \atop {k-1} \right\}, & \text{falls } n > 0,\ k > 0, \\ \frac{1}{k}(\left\{ {n+1} \atop {k} \right\} - \left\{ {n} \atop {k-1} \right\}), & \text{falls } n < 0,\ k > 0, \\ \left\{ {n+1} \atop {k+1} \right\} - (k+1)\left\{ {n} \atop {k+1} \right\}, & \text{falls } k < 0. \end{cases}$$

Zunächst zeigen wir $\left\{ {n} \atop {k} \right\} = 0$ für $n, k \in \mathbb{Z}$ mit $n \geq 0$, $k < 0$ durch Induktion nach k. Für $k = -1$, $n \in \mathbb{Z}$ mit $n \geq 0$ gilt $n + 1 \geq 1 > 0$ und damit

$$\left\{ {n} \atop {k} \right\} = \left\{ {n} \atop {-1} \right\} = \left\{ {n+1} \atop {0} \right\} - 0 \cdot \left\{ {n} \atop {0} \right\} = \left\{ {n+1} \atop {0} \right\} = 0.$$

Es sei $k \in \mathbb{Z}$ mit $k < -1$ so gegeben, dass $\left\{ {n \atop k+1} \right\} = 0$ für $n \in \mathbb{Z}$ mit $n \geq 0$ ist. Dann gilt auch

$$\left\{ {n \atop k} \right\} = \left\{ {n+1 \atop k+1} \right\} - (k+1) \cdot \left\{ {n \atop k+1} \right\} = 0 - (k+1) \cdot 0 = 0$$

für $n \in \mathbb{Z}$ mit $n \geq 0$. Nach dem Induktionsprinzip gilt $\left\{ {n \atop k} \right\} = 0$ für $n, k \in \mathbb{Z}$ mit $n \geq 0$, $k < 0$.
Insbesondere gilt $\left\{ {0 \atop k} \right\} = 0$ für $k \in \mathbb{Z}$ mit $k < 0$ und damit

$$\left\{ {n \atop k} \right\} = \begin{cases} 1, & \text{für } n = 0,\ k = 0, \\ 0, & \text{für } n \in \mathbb{Z} \setminus \{0\},\ k = 0 \text{ und für } n = 0,\ k \in \mathbb{Z} \setminus \{0\}. \end{cases}$$

Als nächstes zeigen wir, dass $\left\{ {n \atop k} \right\} = k \left\{ {n-1 \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\}$ für alle $n, k \in \mathbb{Z}$ gilt. Für $n, k \in \mathbb{Z}$ mit $n > 0$, $k > 0$ gilt $\left\{ {n \atop k} \right\} = k \left\{ {n-1 \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\}$ nach Definition. Für $n, k \in \mathbb{Z}$ mit $n \leq 0$, $k > 0$ gilt $n - 1 < n \leq 0$, also $\left\{ {n-1 \atop k} \right\} = \frac{1}{k}(\left\{ {n \atop k} \right\} - \left\{ {n-1 \atop k-1} \right\})$ und damit $\left\{ {n \atop k} \right\} = k\left\{ {n-1 \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\}$. Für $n, k \in \mathbb{Z}$ mit $k \leq 0$ gilt $k - 1 < k \leq 0$, also $\left\{ {n-1 \atop k-1} \right\} = \left\{ {n \atop k} \right\} - k\left\{ {n-1 \atop k} \right\}$ und damit $\left\{ {n \atop k} \right\} = k\left\{ {n-1 \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\}$. Insgesamt gilt $\left\{ {n \atop k} \right\} = k \left\{ {n-1 \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\}$ für alle $n, k \in \mathbb{Z}$.
Die Äquivalenz der drei genannten Bedingungen lässt sich analog zeigen.
Schließlich zeigen wir $\left\{ {n \atop n} \right\} = 1$ für $n \in \mathbb{Z}$ und $\left\{ {n \atop k} \right\} = 0$ für $n, k \in \mathbb{Z}$ mit $n < k$ durch Induktion nach n. Für $n = 0$ gilt $\left\{ {n \atop k} \right\} = \left\{ {0 \atop 0} \right\} = 1$ für $k = 0 = n$ und $\left\{ {n \atop k} \right\} = \left\{ {0 \atop k} \right\} = 0$ für $k \in \mathbb{Z}$ mit $k > 0 = n$. Für $n \in \mathbb{Z}$ mit $n > 0$ so, dass $\left\{ {n-1 \atop n-1} \right\} = 1$ und $\left\{ {n-1 \atop k} \right\} = 0$ für $k \in \mathbb{Z}$ mit $k > n - 1$ gilt, gilt auch

$$\left\{ {n \atop k} \right\} = n\left\{ {n-1 \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\} = \left\{ \begin{cases} n \cdot 0 + 1, & \text{für } k = n, \\ n \cdot 0 + 0, & \text{für } k \in \mathbb{Z} \text{ mit } k > n \end{cases} \right\} = \begin{cases} 1, & \text{für } k = n, \\ 0, & \text{für } k \in \mathbb{Z} \text{ mit } k > n. \end{cases}$$

Es sei $n \in \mathbb{Z}$ mit $n < 0$ so gegeben, dass $\left\{ {n+1 \atop n+1} \right\} = 1$ und $\left\{ {n+1 \atop k} \right\} = 0$ für $k \in \mathbb{Z}$ mit $k > n + 1$ gilt. Um zu zeigen, dass $\left\{ {n \atop k} \right\} = 0$ für $k \in \mathbb{Z}$ mit $k > n$ gilt, führen wir Induktion nach k ([51]). Für $k = 0$ gilt $\left\{ {n \atop k} \right\} = \left\{ {n \atop 0} \right\} = 0$. Für $k \in \mathbb{Z}$ mit $k > 0$ und $\left\{ {n \atop k-1} \right\} = 0$ gilt auch

$$\left\{ {n \atop k} \right\} = \frac{1}{k}(\left\{ {n+1 \atop k} \right\} - \left\{ {n \atop k-1} \right\}) = \frac{1}{k}(0 - 0) = 0$$

nach (innerer und äußerer) Induktionsvoraussetzung. Für $k \in \mathbb{Z}$ mit $n < k < 0$ und $\left\{ {n \atop k+1} \right\} = 0$ gilt auch

$$\left\{ {n \atop k} \right\} = \left\{ {n+1 \atop k+1} \right\} - (k+1)\left\{ {n \atop k+1} \right\} = 0 - (k+1) \cdot 0 = 0$$

nach (innerer und äußerer) Induktionsvoraussetzung. Nach dem Induktionsprinzip gilt $\left\{ {n \atop k} \right\} = 0$ für $k \in \mathbb{Z}$ mit $k > n$. Nach (äußerer) Induktionsvoraussetzung folgt

$$\left\{ {n \atop n} \right\} = \left\{ {n+1 \atop n+1} \right\} - (n+1)\left\{ {n \atop n+1} \right\} = 1 - (n+1) \cdot 0 = 1.$$

Nach dem Induktionsprinzip gilt $\left\{ {n \atop n} \right\} = 1$ für $n \in \mathbb{Z}$ und $\left\{ {n \atop k} \right\} = 0$ für $n, k \in \mathbb{Z}$ mit $n < k$. □

(17.27) Definition (Stirlingzahl)**.** Es sei $\left\{ {- \atop =} \right\} \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(n, k) \mapsto \left\{ {n \atop k} \right\}$ die nach Proposition (17.26) eindeutige Abbildung mit

$$\left\{ {n \atop k} \right\} = \begin{cases} 1, & \text{für } n = 0,\ k = 0, \\ 0, & \text{für } n \in \mathbb{Z} \setminus \{0\},\ k = 0 \text{ und für } n = 0,\ k \in \mathbb{Z} \setminus \{0\}, \end{cases}$$

und mit

$$\left\{ {n \atop k} \right\} = k \left\{ {n-1 \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\}$$

für $n, k \in \mathbb{Z}$. Für $n, k \in \mathbb{Z}$ heißt $\left\{ {n \atop k} \right\}$ die *Stirlingzahl* von n über k.
Für $n, k \in \mathbb{Z}$ setzen wir ferner

$$\left[{n \atop k} \right] := \left\{ {-k \atop -n} \right\}.$$

[51] Wir führen also eine Induktion innerhalb des Induktionsschlusses.

Die doppelte Schreibweise der Stirlingzahlen hat Ihren Ursprung in der Tatsache, dass man historisch die Zahlen $\begin{bmatrix} n \\ k \end{bmatrix}$ für $n, k \in \mathbb{N}_0$ als *Stirlingzahlen erster Art* und die Zahlen $\left\{ {n \atop k} \right\}$ für $n, k \in \mathbb{N}_0$ als *Stirlingzahlen zweiter Art* bezeichnet.
Die Stirlingzahlen lassen sich rekursiv im sogenannten *Stirlingschen Tandem* berechnen:

(17.28) Beispiel. Die Stirlingzahlen $\left\{ {n \atop k} \right\}$ und $\begin{bmatrix} n \\ k \end{bmatrix}$ für $n, k \in [-4, 4]$ sind wie folgt gegeben.

$\left\{ {n \atop k} \right\}$	-4	-3	-2	-1	0	1	2	3	4	k
-4	1	0	0	0	0	0	0	0	0	
-3	6	1	0	0	0	0	0	0	0	
-2	11	3	1	0	0	0	0	0	0	
-1	6	2	1	1	0	0	0	0	0	
0	0	0	0	0	1	0	0	0	0	
1	0	0	0	0	0	1	0	0	0	
2	0	0	0	0	0	1	1	0	0	
3	0	0	0	0	0	1	3	1	0	
4	0	0	0	0	0	1	7	6	1	
n										

$\begin{bmatrix} n \\ k \end{bmatrix}$	-4	-3	-2	-1	0	1	2	3	4
-4	1	0	0	0	0	0	0	0	0
-3	6	1	0	0	0	0	0	0	0
-2	7	3	1	0	0	0	0	0	0
-1	1	1	1	1	0	0	0	0	0
0	0	0	0	0	1	0	0	0	0
1	0	0	0	0	0	1	0	0	0
2	0	0	0	0	0	1	1	0	0
3	0	0	0	0	0	2	3	1	0
4	0	0	0	0	0	6	11	6	1
n									

Die die Stirlingzahlen definierende Rekursionsgleichung lässt sich auch wie folgt ausdrücken.

(17.29) Bemerkung. Für $n, k \in \mathbb{Z}$ gilt

$$\begin{bmatrix} n \\ k \end{bmatrix} = (n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}.$$

Beweis. Für $n, k \in \mathbb{Z}$ gilt

$$\begin{bmatrix} n-1 \\ k-1 \end{bmatrix} = \left\{ {-(k-1) \atop -(n-1)} \right\} = \left\{ {-k+1 \atop -n+1} \right\} = (-n+1) \left\{ {-k \atop -n+1} \right\} + \left\{ {-k \atop -n} \right\} = (-n+1) \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n \\ k \end{bmatrix}$$

und damit

$$\begin{bmatrix} n \\ k \end{bmatrix} = (n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}.$$ □

18 Kombinatorik

Die mathematische Kombinatorik beschäftigt sich mit der Bestimmung von Kardinalitäten gewisser endlicher Mengen, sprich dem Zählen mathematischer Objekte. Durch Modellierung lassen sich so viele Zählprobleme des Alltags lösen.
Wir beginnen mit der Vorstellung einiger allgemeiner Methoden zur Berechnung von Kardinalitäten. Danach studieren wir die klassischen Modelle für Auswahlen: Variationen, Permutation (in Mengen), Multikombinationen und Kombinationen. Als Spezialfälle erhalten wir Formeln für Anzahlen bereits eingeführter mathematischer Objekte wie Teilmengen und Abbildungen. Den Abschluss bilden Modelle für Unterteilungen wie Partitionen mit vorgegebener Anzahl an Teilen, surjektive Abbildungen und Permutationen (von Mengen) mit vorgegebener Anzahl von Bahnen.

Kombinatorische Beweisprinzipien

Zunächst studieren wir einige allgemeine Strategien zur Bestimmung von Kardinalitäten endlicher Mengen.

(18.1) Bemerkung (Gleichheitsregel)**.** Es seien endliche Mengen X und Y gegeben. Genau dann gilt $|X| = |Y|$, wenn es eine Bijektion $X \to Y$ gibt.

(18.2) Beispiel. Es ist

$$|\{n \in [1, 100] \mid \text{es gibt ein } k \in \mathbb{N} \text{ mit } n = k^2\}| = 10.$$

Beweis. Es sei $f\colon \mathbb{N} \to \mathbb{N},\ k \mapsto k^2$. Da für $k, l \in [1,10]$ aus $k^2 = l^2$ bereits $k = l$ folgt, ist f injektiv. Wegen $f([1,10]) \subseteq [1,100]$ und $f(\mathbb{N} \setminus [1,10]) \subseteq \mathbb{N} \setminus [1,100]$ gilt ferner

$$\begin{aligned} f([1,10]) &= f([1,10]) \cap [1,100] = \{n \in \mathbb{N} \mid \text{es gibt ein } k \in [1,10] \text{ mit } n = f(k)\} \cap [1,100] \\ &= \{n \in [1,100] \mid \text{es gibt ein } k \in [1,10] \text{ mit } n = f(k)\} \\ &= \{n \in [1,100] \mid \text{es gibt ein } k \in \mathbb{N} \text{ mit } n = f(k)\} \\ &= \{n \in [1,100] \mid \text{es gibt ein } k \in \mathbb{N} \text{ mit } n = k^2\}. \end{aligned}$$

Folglich ist

$$f|_{[1,10]}^{f([1,10])}\colon [1,10] \to \{n \in [1,100] \mid \text{es gibt ein } k \in \mathbb{N} \text{ mit } n = k^2\}$$

eine Bijektion und damit

$$|\{n \in [1,100] \mid \text{es gibt ein } k \in \mathbb{N} \text{ mit } n = k^2\}| = |[1,10]| = 10.$$ □

(18.3) Anwendungsbeispiel.

(a) Hexadezimalziffern seien als Elemente von $\{0, 1, \ldots, 9, \mathrm{A}, \mathrm{B}, \ldots, \mathrm{F}\}$ modelliert. Da

$$[0,15] \to \{0, 1, \ldots, 9, \mathrm{A}, \mathrm{B}, \ldots, \mathrm{F}\},\ 0 \mapsto 0,\ 1 \mapsto 1,\ \ldots,\ 9 \mapsto 9,\ 10 \mapsto \mathrm{A},\ 11 \mapsto \mathrm{B},\ \ldots,\ 15 \mapsto \mathrm{F}$$

eine Bijektion ist, ist die Anzahl aller Hexadezimalziffern gleich

$$|\{0, 1, \ldots, 9, \mathrm{A}, \mathrm{B}, \ldots, \mathrm{F}\}| = |[0,15]| = 16.$$

(b) Spielerkombinationen in der zweiten Runde beim Spiel Reise nach Jerusalem mit vier Startspielern seien als 3-elementige Teilmengen von $X = \{\text{Elias}, \text{Julia}, \text{Laura}, \text{Michael}\}$, d.h. als Elemente von $\{U \in \mathrm{Pot}(X) \mid |U| = 3\}$ modelliert. Da

$$X \to \{U \in \mathrm{Pot}(X) \mid |U| = 3\},\ x \mapsto X \setminus \{x\}$$

eine Bijektion ist, ist die Anzahl aller solchen Spielerkombinationen gleich

$$|\{U \in \mathrm{Pot}(X) \mid |U| = 3\}| = |X| = 4.$$

(18.4) Bemerkung (Summenregel)**.** Es seien $n \in \mathbb{N}_0$ und ein disjunktes n-Tupel endlicher Mengen $(X_1, \ldots, X_n)$ gegeben. Dann gilt

$$|\dot{\bigcup_{i \in [1,n]}} X_i| = \sum_{i \in [1,n]} |X_i|.$$

(18.5) Anwendungsbeispiel. Eine Obstschale mit drei Äpfeln, vier Bananen, zwei Birnen und zwei Orangen sei als Menge

$$[1,3] \times \{\text{Apfel}\}\ \dot\cup\ [1,4] \times \{\text{Banane}\}\ \dot\cup\ [1,2] \times \{\text{Birne}\}\ \dot\cup\ [1,2] \times \{\text{Orange}\}$$

modelliert. Nach der Summenregel (18.4) ist die Anzahl der Obststücke auf einer solchen Obstschale gleich

$$\begin{aligned} &|[1,3] \times \{\text{Apfel}\}\ \dot\cup\ [1,4] \times \{\text{Banane}\}\ \dot\cup\ [1,2] \times \{\text{Birne}\}\ \dot\cup\ [1,2] \times \{\text{Orange}\}| \\ &= |[1,3] \times \{\text{Apfel}\}| + |[1,4] \times \{\text{Banane}\}| + |[1,2] \times \{\text{Birne}\}| + |[1,2] \times \{\text{Orange}\}| \\ &= 3 + 4 + 2 + 2 = 11. \end{aligned}$$

(18.6) Korollar (Differenzregel)**.** Für jede endliche Menge X und jede Teilmenge U von X gilt

$$|X \setminus U| = |X| - |U|.$$

Beweis. Für jede endliche Menge X und jede Teilmenge U von X gilt $X = U\,\dot\cup\,(X \setminus U)$, also $|X| = |U| + |X \setminus U|$ nach der Summenregel (18.4) und damit $|X \setminus U| = |X| - |U|$. □

(18.7) Beispiel. Es ist

$$|\{n \in [1,10] \mid n \notin \mathbb{P}\}| = 6.$$

Beweis. Nach der Differenzregel (18.6) ist

$$\begin{aligned}|\{n \in [1,10] \mid n \notin \mathbb{P}\}| &= |[1,10] \setminus \{n \in [1,10] \mid n \in \mathbb{P}\}| = |[1,10] \setminus \{2,3,5,7\}| = |[1,10]| - |\{2,3,5,7\}| \\ &= 10 - 4 = 6.\end{aligned}$$

□

(18.8) Bemerkung (Produktregel)**.** Es seien $n \in \mathbb{N}_0$ und ein n-Tupel endlicher Mengen $(X_1, \ldots, X_n)$ gegeben. Dann gilt

$$|\bigtimes_{i\in[1,n]} X_i| = \prod_{i\in[1,n]} |X_i|.$$

(18.9) Anwendungsbeispiel. Ein Spielkartenset beim Kartenspiel Skat sei als Menge

$$\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \times \{7, 8, 9, 10, \mathrm{B}, \mathrm{D}, \mathrm{K}, \mathrm{A}\}$$

modelliert. Nach der Produktregel (18.8) ist die Anzahl der Spielkarten in diesem Set gleich

$$|\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \times \{7, 8, 9, 10, \mathrm{B}, \mathrm{D}, \mathrm{K}, \mathrm{A}\}| = |\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}|\,|\{7, 8, 9, 10, \mathrm{B}, \mathrm{D}, \mathrm{K}, \mathrm{A}\}| = 4 \cdot 8 = 32.$$

(18.10) Proposition (Inklusions-Exklusionsprinzip)**.** Für $n \in \mathbb{N}_0$ und jedes n-Tupel endlicher Mengen $(X_1, \ldots, X_n)$ gilt

$$|\bigcup_{i\in[1,n]} X_i| = \sum_{i\in[1,n]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,n]\\|J|=i}} |\bigcap_{j\in J} X_j|.$$

Beweis. Wir zeigen zunächst die behauptete Aussage für den Fall $n = 2$. Es seien also endliche Mengen X und Y gegeben. Nach der Differenzregel (18.6) gilt $|X \setminus Y| = |X \setminus (X \cap Y)| = |X| - |X \cap Y|$ und $|Y \setminus X| = |Y \setminus (X \cap Y)| = |Y| - |X \cap Y|$. Wegen $X \cup Y = (X \setminus Y) \,\dot\cup\, (X \cap Y) \,\dot\cup\, (Y \setminus X)$ impliziert die Summenregel (18.4) nun

$$|X \cup Y| = |(X \setminus Y) \,\dot\cup\, (X \cap Y) \,\dot\cup\, (Y \setminus X)| = |X \setminus Y| + |X \cap Y| + |Y \setminus X| = |X| + |Y| - |X \cap Y|.$$

Nun zeigen wir durch Induktion nach n, dass für $n \in \mathbb{N}_0$ und jedes n-Tupel endlicher Mengen $(X_1, \ldots, X_n)$ stets

$$|\bigcup_{i\in[1,n]} X_i| = \sum_{i\in[1,n]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,n]\\|J|=i}} |\bigcap_{j\in J} X_j|$$

gilt. Für $n = 0$ gilt

$$|\bigcup_{i\in[1,0]} X_i| = |\emptyset| = 0 = \sum_{i\in[1,0]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,0]\\|J|=i}} |\bigcap_{j\in J} X_j| = \sum_{i\in[1,n]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,n]\\|J|=i}} |\bigcap_{j\in J} X_j|.$$

Es sei also ein $n \in \mathbb{N}$ so gegeben, dass für jedes $(n-1)$-Tupel endlicher Mengen $(X'_1, \ldots, X'_{n-1})$ stets

$$|\bigcup_{i\in[1,n-1]} X'_i| = \sum_{i\in[1,n-1]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,n-1]\\|J|=i}} |\bigcap_{j\in J} X'_j|$$

gilt. Für jedes n-Tupel endlicher Mengen $(X_1, \ldots, X_n)$ gilt dann auch

$$\begin{aligned}|\bigcup_{i\in[1,n]} X_i| &= |\bigcup_{i\in[1,n-1]} X_i \cup X_n| = |\bigcup_{i\in[1,n-1]} X_i| + |X_n| - |(\bigcup_{i\in[1,n-1]} X_i) \cap X_n| \\ &= |\bigcup_{i\in[1,n-1]} X_i| + |X_n| - |\bigcup_{i\in[1,n-1]} (X_i \cap X_n)|\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i\in[1,n-1]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,n-1]\\|J|=i}} |\bigcap_{j\in J} X_j| + |X_n| - \sum_{i\in[1,n-1]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,n-1]\\|J|=i}} |\bigcap_{j\in J} (X_j \cap X_n)| \\
&= \sum_{i\in[1,n-1]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,n]\\|J|=i\\n\notin J}} |\bigcap_{j\in J} X_j| + |X_n| + \sum_{i\in[1,n-1]} (-1)^{i} \sum_{\substack{J\subseteq[1,n]\\|J|=i+1\\n\in J}} |\bigcap_{j\in J} X_j| \\
&= \sum_{i\in[1,n-1]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,n]\\|J|=i\\n\notin J}} |\bigcap_{j\in J} X_j| + |X_n| + \sum_{i\in[2,n]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,n]\\|J|=i\\n\in J}} |\bigcap_{j\in J} X_j| \\
&= \sum_{i\in[1,n]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,n]\\|J|=i\\n\notin J}} |\bigcap_{j\in J} X_j| + \sum_{i\in[1,n]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,n]\\|J|=i\\n\in J}} |\bigcap_{j\in J} X_j| \\
&= \sum_{i\in[1,n]} (-1)^{i-1} (\sum_{\substack{J\subseteq[1,n]\\|J|=i\\n\notin J}} |\bigcap_{j\in J} X_j| + \sum_{\substack{J\subseteq[1,n]\\|J|=i\\n\in J}} |\bigcap_{j\in J} X_j|) = \sum_{i\in[1,n]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,n]\\|J|=i}} |\bigcap_{j\in J} X_j|.
\end{aligned}
$$

Nach dem Induktionsprinzip gilt

$$
|\bigcup_{i\in[1,n]} X_i| = \sum_{i\in[1,n]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,n]\\|J|=i}} |\bigcap_{j\in J} X_j|
$$

für alle $n \in \mathbb{N}_0$ und jedes n-Tupel endlicher Mengen $(X_1, \ldots, X_n)$. □

(18.11) Beispiel. Es gilt

$$
|\{n \in [1,100] \mid 2 \mid n \text{ oder } 3 \mid n \text{ oder } 5 \mid n\}| = 74.
$$

Beweis. Für $k \in \mathbb{N}$ sei $X_k := \{n \in [1,100] \mid k \mid n\}$. Dann ist $|X_k| = 100 \operatorname{div} k$ für $k \in \mathbb{N}$, also insbesondere

$$
\begin{aligned}
&|X_2| = 100 \operatorname{div} 2 = 50, \\
&|X_3| = 100 \operatorname{div} 3 = 33, \\
&|X_5| = 100 \operatorname{div} 5 = 20.
\end{aligned}
$$

Wegen $2, 3, 5 \in \mathbb{P}$ gilt für $k, l \in \{2, 3, 5\}$ mit $k \neq l$ ferner

$$
\begin{aligned}
X_k \cap X_l &= \{n \in [1,100] \mid k \mid n\} \cap \{n \in [1,100] \mid l \mid n\} = \{n \in [1,100] \mid k \mid n \text{ und } l \mid n\} \\
&= \{n \in [1,100] \mid kl \mid n\} = X_{kl},
\end{aligned}
$$

also

$$
\begin{aligned}
&|X_2 \cap X_3| = |X_6| = 100 \operatorname{div} 6 = 16, \\
&|X_2 \cap X_5| = |X_{10}| = 100 \operatorname{div} 10 = 10, \\
&|X_3 \cap X_5| = |X_{15}| = 100 \operatorname{div} 15 = 6.
\end{aligned}
$$

Schließlich gilt

$$
\begin{aligned}
X_2 \cap X_3 \cap X_5 &= \{n \in [1,100] \mid 2 \mid n\} \cap \{n \in [1,100] \mid 3 \mid n\} \cap \{n \in [1,100] \mid 5 \mid n\} \\
&= \{n \in [1,100] \mid 2 \mid n \text{ und } 3 \mid n \text{ und } 5 \mid n\} = \{n \in [1,100] \mid 30 \mid n\} = X_{30},
\end{aligned}
$$

also

$$
|X_2 \cap X_3 \cap X_5| = |X_{30}| = 100 \operatorname{div} 30 = 3.
$$

Nach dem Inklusions-Exklusions-Prinzip (18.10) folgt

$$
\begin{aligned}
&|\{n \in [1,100] \mid 2 \mid n \text{ oder } 3 \mid n \text{ oder } 5 \mid n\}| \\
&= |\{n \in [1,100] \mid 2 \mid n\} \cup \{n \in [1,100] \mid 3 \mid n\} \cup \{n \in [1,100] \mid 5 \mid n\}| = |X_2 \cup X_3 \cup X_5| \\
&= |X_2| + |X_3| + |X_5| - |X_2 \cap X_3| - |X_2 \cap X_5| - |X_3 \cap X_5| + |X_2 \cap X_3 \cap X_5| \\
&= 50 + 33 + 20 - 16 - 10 - 6 + 3 = 74.
\end{aligned}
$$

□

Ein weiteres Beweisprinzip, welches sich nicht direkt zur Bestimmung von Anzahlen eignet, aber dennoch in Beweisen kombinatorischer Natur Anwendung findet, ist das sogenannte Schubfachprinzip:

(18.12) Bemerkung (Schubfachprinzip)**.** Es seien endliche Mengen X und Y und eine Abbildung $f\colon X \to Y$ gegeben. Wenn $|X| > |Y|$ ist, dann ist f nicht injektiv.

Wir erläutern das Schubfachprinzip (18.12) an Beispielen aus dem täglichen Leben:

(18.13) Anwendungsbeispiel.

(a) Eine Clique aus mindestens 13 Personen seien als Elemente einer Menge C modelliert. Die Monate im gregorianischen Kalender seien als Elemente von $M = \{\text{Januar}, \ldots, \text{Dezember}\}$ modelliert. Die Zuordnung des jeweiligen Geburtsmonats zu den betrachteten Personen sei als Abbildung $g\colon C \to M$ modelliert. Nach dem Schubfachprinzip (18.12) ist g nicht injektiv, d.h. es gibt (mindestens) zwei Personen, welche im gleichen Monat Geburtstag haben.

(b) Die Besucher einer Party (aus mindestens zwei Personen) seien als Elemente einer Menge P modelliert. Die Anzahl der anderen Leute, welche die jeweiligen Teilnehmer kennen, sei als Abbildung $a\colon P \to [1, n-1]$ modelliert. Nach dem Schubfachprinzip (18.12) ist a nicht injektiv, d.h. es gibt (mindestens) zwei Besucher, welche die gleiche Anzahl von Leuten kennen.

(c) Kugeln seien als Elemente einer Menge K modelliert. Boxen seien als Elemente einer Menge B modelliert. Eine Verteilung der Kugeln auf die Boxen sei als Abbildung $b\colon K \to B$ modelliert. Wenn es mehr Kugeln als Boxen gibt, so ist b nach dem Schubfachprinzip (18.12) nicht injektiv, d.h. es gibt bei der Verteilung stets eine Box, in welcher mehr als eine Kugel liegt.

Variationen und Permutationen

Als nächstes wollen wir Auswahlen aus einer vorgegebenen Gesamtheit modellieren und die Möglichkeiten solcher Auswahlen zählen. Dabei spielt es für die Anzahl und somit auch für unser Modell eine Rolle, ob wir die Objekte unter Beachtung der Reihenfolge auswählen und ob wir die wiederholte Auswahl desselben Objektes zulassen.
Wir beginnen mit der Auswahl von Objekten unter Beachtung der Reihenfolge und der Möglichkeit der Wiederholung. Haben wir eine Menge X gegeben und wollen aus dieser Menge vier Objekte nacheinander auswählen, so können wir diese Auswahl als Abbildung $[1, 4] \to X$ auffassen. Im Wesentlichen werden wir genau diesen Standpunkt einnehmen, wobei man in der Kombinatorik klassisch eher mit Tupeln und der zugehörigen Indexschreibweise an Stelle von Abbildungen arbeitet. Eine Auswahl von vier Objekten aus X werden wir somit als 4-Tupel mit Einträgen in X, d.h. als ein Element von X^4 auffassen.
Etwas allgemeiner möchte man die Auswahl manchmal nicht lediglich durchnummerieren, sondern Auswahlen in der Menge X für andere Elemente einer Menge I treffen. Daher definieren wir noch etwas allgemeiner:

(18.14) Definition (Variation)**.** Es sei eine Menge X gegeben.

(a) Es sei eine Menge I gegeben. Die *Menge der Variationen* in X über I ist definiert als

$$\mathrm{Var}_I(X) := X^I.$$

Ein Element von $\mathrm{Var}_I(X)$ wird eine *Variation* in X über I (oder *I-Variation* in X oder *I-Variation mit Wiederholung* in X) genannt.

(b) Es sei $k \in \mathbb{N}_0$ gegeben. Die *Menge der k-Variationen* in X ist definiert als

$$\mathrm{Var}_k(X) := \mathrm{Var}_{[1,k]}(X).$$

Ein Element von $\mathrm{Var}_k(X)$ wird eine *k-Variation* (oder *k-Variation mit Wiederholung*) in X genannt.

(18.15) Beispiel.

(a) Es ist $(5, 3, 9, 7)$ eine 4-Variation in $[1, 9]$.

(b) Es ist $(5, 3, 5, 7)$ eine 4-Variation in $[1, 9]$.

(18.16) Beispiel. Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$\begin{aligned}\mathrm{Var}_3(\{a,b,c,d\}) = \{&(a,a,a),(a,a,b),(a,a,c),(a,a,d),(a,b,a),(a,b,b),(a,b,c),(a,b,d),(a,c,a),(a,c,b),\\&(a,c,c),(a,c,d),(a,d,a),(a,d,b),(a,d,c),(a,d,d),(b,a,a),(b,a,b),(b,a,c),(b,a,d),\\&(b,b,a),(b,b,b),(b,b,c),(b,b,d),(b,c,a),(b,c,b),(b,c,c),(b,c,d),(b,d,a),(b,d,b),\\&(b,d,c),(b,d,d),(c,a,a),(c,a,b),(c,a,c),(c,a,d),(c,b,a),(c,b,b),(c,b,c),(c,b,d),\\&(c,c,a),(c,c,b),(c,c,c),(c,c,d),(c,d,a),(c,d,b),(c,d,c),(c,d,d),(d,a,a),(d,a,b),\\&(d,a,c),(d,a,d),(d,b,a),(d,b,b),(d,b,c),(d,b,d),(d,c,a),(d,c,b),(d,c,c),(d,c,d),\\&(d,d,a),(d,d,b),(d,d,c),(d,d,d)\}.\end{aligned}$$

Wir betrachten einige Beispiele aus dem täglichen Leben:

(18.17) Anwendungsbeispiel.

(a) Ein Wort bestehend aus genau sechs Buchstaben des lateinischen Alphabets (ohne Sonderzeichen) lässt sich als 6-Variation in $\{\mathrm{A},\mathrm{B},\ldots,\mathrm{Z}\}$ auffassen.

(b) Eine vierstellige PIN lässt sich als 4-Variation in $[0,9]$ auffassen.

(c) Ein Rateversuch beim Spiel Mastermind lässt sich als 4-Variation in $\{\text{blau}, \text{gelb}, \text{grün}, \text{rosa}, \text{rot}, \text{violett}\}$ auffassen.

(d) Eine Totowette (für 11 Spiele) lässt sich als 11-Variation in $\{1,0,2\}$ auffassen.

(e) Ein Byte lässt sich als $[0,7]$-Variation in $\{0,1\}$ auffassen.

(f) Die Teilnehmer einer Klausur seien als Elemente einer Menge T modelliert. Das Ergebnis der Klausur lässt sich als Variation in $\{1.0, 1.3, 1.7, 2.0, 2.3, 2.7, 3.0, 3.3, 3.7, 4.0, 5.0\}$ über T auffassen.

(g) Eine Verteilung von zehn durchnummerierten Kugeln auf vier unterschiedlich farbige Boxen lässt sich als 10-Variation in $\{\text{rot}, \text{blau}, \text{gelb}, \text{grün}\}$ auffassen.

(18.18) Bemerkung. Es seien $n, k \in \mathbb{N}_0$, eine n-elementige Menge X und eine k-elementige Menge I gegeben. Dann gilt

$$|\mathrm{Var}_I(X)| = n^k.$$

Beweis. Nach der Produktregel (18.8) gilt

$$|\mathrm{Var}_k(X)| = |X^k| = |X|^k = n^k.$$

Wegen $|I| = k$ gibt es eine Bijektion $e\colon [1,k] \to I$, welche uns wohldefinierte, sich gegenseitig invertierende Abbildungen

$$\mathrm{Var}_I(X) \to \mathrm{Var}_k(X),\ y \mapsto y \circ e,$$
$$\mathrm{Var}_k(X) \to \mathrm{Var}_I(X),\ x \mapsto x \circ e^{-1}$$

liefert. Nach Satz (3.29)(c) und der Gleichheitsregel (18.1) folgt

$$|\mathrm{Var}_I(X)| = |\mathrm{Var}_k(X)| = n^k. \qquad \square$$

(18.19) Beispiel.

(a) Es ist

$$|\mathrm{Var}_4([1,9])| = 6561.$$

(b) Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$|\mathrm{Var}_3(\{a,b,c,d\})| = 64.$$

Beweis.

(a) Nach Bemerkung (18.18) ist

$$|\mathrm{Var}_4([1,9])| = 9^4 = 6561.$$

(b) Nach Bemerkung (18.18) ist

$$|\mathrm{Var}_3(\{a,b,c,d\})| = 4^3 = 64.$$ □

Wir kommen zu unseren Beispielen aus dem täglichen Leben zurück:

(18.20) Anwendungsbeispiel.

(a) Wörter, welche aus genau sechs Buchstaben des lateinischen Alphabets (ohne Sonderzeichen) bestehen, seien als 6-Variationen in $\{\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}\}$ modelliert. Nach Bemerkung (18.18) ist die Anzahl aller solchen Wörter gleich

$$|\mathrm{Var}_6(\{\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}\})| = 26^6 = 308\,915\,776.$$

(b) Vierstellige PINs seien als 4-Variationen in $[0,9]$ modelliert. Nach Bemerkung (18.18) ist die Anzahl aller solchen PINs gleich

$$|\mathrm{Var}_4([0,9])| = 10^4 = 10\,000.$$

(c) Rateversuche beim Spiel Mastermind seien als 4-Variationen in $\{\text{blau}, \text{gelb}, \text{grün}, \text{rosa}, \text{rot}, \text{violett}\}$ modelliert. Nach Bemerkung (18.18) ist die Anzahl der Möglichkeiten für einen beliebigen Rateversuch gleich

$$|\mathrm{Var}_4(\{\text{blau}, \text{gelb}, \text{grün}, \text{rosa}, \text{rot}, \text{violett}\})| = 6^4 = 1296.$$

(d) Totowetten (für 11 Spiele) seien als 11-Variationen in $\{1, 0, 2\}$ modelliert. Nach Bemerkung (18.18) ist die Anzahl aller möglichen Totowetten gleich

$$|\mathrm{Var}_{11}(\{1,0,2\})| = 3^{11} = 177\,147.$$

(e) Bytes seien als $[0,7]$-Variationen in $\{0,1\}$ modelliert. Nach Bemerkung (18.18) ist die Anzahl aller Bytes gleich

$$|\mathrm{Var}_{[0,7]}(\{0,1\})| = 2^8 = 256.$$

(f) Die 400 Teilnehmer einer Klausur seien als Elemente einer Menge T modelliert. Die möglichen Ergebnisse der Klausur seien als Variationen in $\{1.0, 1.3, 1.7, 2.0, 2.3, 2.7, 3.0, 3.3, 3.7, 4.0, 5.0\}$ über T modelliert. Nach Bemerkung (18.18) ist die Anzahl aller möglichen Klausurergebnisse gleich

$$|\mathrm{Var}_T(\{1.0, 1.3, 1.7, 2.0, 2.3, 2.7, 3.0, 3.3, 3.7, 4.0, 5.0\})| = 11^{400} \approx 3{,}61 \cdot 10^{416}.$$

(g) Verteilungen von zehn durchnummerierten Kugeln auf vier unterschiedlich farbige Boxen seien als 10-Variationen in $\{\text{rot}, \text{blau}, \text{gelb}, \text{grün}\}$ modelliert. Nach Bemerkung (18.18) ist die Anzahl aller solchen möglichen Verteilungen gleich

$$|\mathrm{Var}_{10}(\{\text{rot}, \text{blau}, \text{gelb}, \text{grün}\})| = 4^{10} = 1\,048\,576.$$

Bevor wir zu unserem nächsten Auswahlmodell kommen, führen wir für eine gegebene Variation noch ein Konzept ein, welches diese bis auf Reihenfolge der Einträge charakterisiert, siehe Satz (18.42):

(18.21) Definition (Häufigkeitsfunktion)**.** Es seien $k \in \mathbb{N}_0$, eine Menge X, eine k-elementige Menge I und eine I-Variation x in X gegeben. Die Abbildung

$$\mu_x \colon X \to \mathbb{N}_0,\ y \mapsto |\{i \in I \mid x_i = y\}|$$

heißt *Häufigkeitsfunktion* von x in X.

Gemäß Konvention (3.9) fassen wir eine Häufigkeitsfunktion einer Variation in einer Menge X meist auch als Familie über X auf und sprechen dann von einer *Häufigkeitsfamilie* bzw. im Spezialfall $X = [1, n]$ für ein $n \in \mathbb{N}_0$ auch vom *Häufigkeitstupel* der Variation.
Etwas allgemeiner als in Definition (18.21) lassen sich Häufigkeitsfunktionen für solche Variationen in einer Menge X definieren, bei denen jedes Element von X nur endlich oft als Eintrag vorkommt.

(18.22) Beispiel.

(a) Das Häufigkeitstupel der 4-Variation $(5, 3, 9, 7)$ in $[1, 9]$ ist gegeben durch

$$\mu_{(5,3,9,7)} = (0, 0, 1, 0, 1, 0, 1, 0, 1).$$

(b) Das Häufigkeitstupel der 4-Variation $(5, 3, 5, 7)$ in $[1, 9]$ ist gegeben durch

$$\mu_{(5,3,5,7)} = (0, 0, 1, 0, 2, 0, 1, 0, 0).$$

In Korollar (18.102) werden wir die Anzahl aller Variationen, welche eine gegebene Familie als Häufigkeitsfamilie besitzen, bestimmen.
Als nächstes modellieren wir Auswahlen, bei denen wir weiterhin die Reihenfolge beachten, jedoch die Möglichkeit der Wiederholung ausschließen wollen:

(18.23) Definition (Permutation)**.** Es sei eine Menge X gegeben.

(a) Es sei eine Menge I gegeben. Die *Menge der Permutationen* in X über I ist definiert als

$$\mathrm{Perm}_I(X) := \{x \in \mathrm{Var}_I(X) \mid \text{für } i, j \in I \text{ mit } i \neq j \text{ gilt } x_i \neq x_j\}.$$

Ein Element von $\mathrm{Perm}_I(X)$ wird eine *Permutation* in X über I (oder *I-Permutation* in X oder *I-Variation ohne Wiederholung* in X) genannt.

(b) Es sei $k \in \mathbb{N}_0$ gegeben. Die *Menge der k-Permutationen* in X ist definiert als

$$\mathrm{Perm}_k(X) := \mathrm{Perm}_{[1,k]}(X).$$

Ein Element von $\mathrm{Perm}_k(X)$ wird eine *k-Permutation* (oder *k-Variation ohne Wiederholung*) in X genannt.

Eine Variation x in einer Menge X über einer Menge I ist also genau dann eine Permutation, wenn $x\colon I \to X$, $i \mapsto x_i$ injektiv ist.

(18.24) Beispiel.

(a) Es ist $(5, 3, 9, 7)$ eine 4-Permutation in $[1, 9]$.

(b) Die 4-Variation $(5, 3, 5, 7)$ in $[1, 9]$ ist keine 4-Permutation in $[1, 9]$.

(18.25) Beispiel. Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$\begin{aligned}\mathrm{Perm}_3(\{a, b, c, d\}) = \{&(a, b, c), (a, b, d), (a, c, b), (a, c, d), (a, d, b), (a, d, c), (b, a, c), (b, a, d), (b, c, a), (b, c, d),\\ &(b, d, a), (b, d, c), (c, a, b), (c, a, d), (c, b, a), (c, b, d), (c, d, a), (c, d, b), (d, a, b), (d, a, c),\\ &(d, b, a), (d, b, c), (d, c, a), (d, c, b)\}\end{aligned}$$

Als nächstes wieder einige Beispiele aus dem täglichen Leben:

(18.26) Anwendungsbeispiel.

(a) Ein Wort bestehend aus genau sechs verschiedenen Buchstaben des lateinischen Alphabets (ohne Sonderzeichen) lässt sich als 6-Permutation in $\{\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}\}$ auffassen.

(b) Eine Auftragsverteilung beim Spiel Risiko auf vier Spieler lässt sich als Permutation in der Menge der Aufträge über $\{\text{Désirée}, \text{Kirstin}, \text{Michael}, \text{Sebastian}\}$ auffassen.

(c) Die Teilnehmer eines Wettbewerbs (mit mindestens drei Teilnehmern) seien als Elemente einer Menge T modelliert. Eine Medaillenverteilung bei diesem Wettbewerb lässt sich als Permutation in T über $\{\text{gold}, \text{silber}, \text{bronze}\}$ auffassen.

(d) Eine Tabelle der Fußball-Bundesliga der Saison 2016/17 lässt sich als 18-Permutation in

$$\{\text{FC Augsburg}, \text{Hertha BSC}, \text{SV Werder Bremen}, \text{SV Darmstadt 98}, \text{Borussia Dortmund},\\ \text{Eintracht Frankfurt}, \text{SC Freiburg}, \text{FC Ingolstadt 04}, \text{FC Schalke 04}, \text{Hamburger SV},\\ \text{TSG 1899 Hoffenheim}, \text{1. FC Köln}, \text{RB Leipzig}, \text{Bayer 04 Leverkusen}, \text{1. FSV Mainz 05},\\ \text{Borussia Mönchengladbach}, \text{FC Bayern München}, \text{VfL Wolfsburg}\}$$

auffassen.

(e) Eine Mischung eines Skatkartenspiels lässt sich als 32-Permutation in $\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \times \{7, 8, 9, 10, \text{B}, \text{D}, \text{K}, \text{A}\}$ auffassen.

(f) Eine Verteilung von vier unterschiedlich farbigen Kugeln auf zehn durchnummerierte Boxen derart, dass in jeder Box höchstens eine Kugel liegt, lässt sich als Permutation in $[1, 10]$ über $\{\text{rot}, \text{blau}, \text{gelb}, \text{grün}\}$ auffassen.

Es sei eine Menge X gegeben. Für jede Menge I werden die Elemente von $\mathrm{Perm}_I(X)$ Permutationen in X über I genannt, während die Elemente der symmetrischen Gruppe S_X Permutationen von X genannt werden. Falls X endlich ist, sind Permutationen von X im Wesentlichen dasselbe wie Permutationen in X über X:

(18.27) Bemerkung. Es sei eine Menge X gegeben.

(a) Für jede Permutation π von X ist $(\pi(x))_{x \in X}$ eine Permutation in X über X.

(b) Wenn X endlich ist, dann ist für jede Permutation x in X über X die Abbildung $X \to X$, $y \mapsto x_y$ eine Permutation von X.

Beweis.

(a) Jedes $\pi \in \mathrm{S}_X$ ist bijektiv, also insbesondere injektiv, so dass $(\pi(x))_{x \in X}$ eine Permutation in X über X ist.

(b) Es sei eine Permutation x in X über X gegeben, so dass $x\colon X \to X$, $y \mapsto x_y$ injektiv ist. Wenn X endlich ist, impliziert dies aber bereits die Bijektivität von x, d.h. es gilt $x \in \mathrm{S}_X$. □

(18.28) Bemerkung. Es seien $n \in \mathbb{N}_0$, $k \in [1, n]$ und eine n-elementige Menge X gegeben. Für jedes $x \in \mathrm{Perm}_{k-1}(X)$ sei eine Abzählung e_x von $X \setminus \{x_1, \ldots, x_{k-1}\}$ gegeben. Dann sind

$$\mathrm{Perm}_{k-1}(X) \times [1, n-k+1] \to \mathrm{Perm}_k(X),\ (x, j) \mapsto (x_1, \ldots, x_{k-1}, e_x(j)),$$
$$\mathrm{Perm}_k(X) \to \mathrm{Perm}_{k-1}(X) \times [1, n-k+1],\ y \mapsto ((y_1, \ldots, y_{k-1}), e_x^{-1}(y_k))$$

wohldefinierte, sich gegenseitig invertierende Bijektionen.

Beweis. Für $x \in \mathrm{Perm}_{k-1}(X)$, $j \in [1, n-k+1]$ gilt stets $e_x(j) \in X \setminus \{x_1, \ldots, x_{k-1}\}$ und damit $(x_1, \ldots, x_{k-1}, e_x(j)) \in \mathrm{Perm}_k(X)$. Folglich haben wir eine wohldefinierte Abbildung

$$f\colon \mathrm{Perm}_{k-1}(X) \times [1, n-k+1] \to \mathrm{Perm}_k(X),\ (x, j) \mapsto (x_1, \ldots, x_{k-1}, e_x(j)).$$

Da für $y \in \mathrm{Perm}_k(X)$ insbesondere $(y_1, \ldots, y_{k-1}) \in \mathrm{Perm}_{k-1}(X)$ ist, haben wir ferner eine wohldefinierte Abbildung

$$g\colon \mathrm{Perm}_k(X) \to \mathrm{Perm}_{k-1}(X) \times [1, n-k+1],\ y \mapsto ((y_1, \ldots, y_{k-1}), e_x^{-1}(y_k)).$$

Wir erhalten

$$g(f(x, j)) = g(x_1, \ldots, x_{k-1}, e_x(j)) = ((x_1, \ldots, x_{k-1}), e_x^{-1}(e_x(j))) = (x, j)$$

für $x \in \mathrm{Perm}_{k-1}(X)$, $j \in [1, n-k+1]$ sowie

$$f(g(y)) = f((y_1, \ldots, y_{k-1}), e_x^{-1}(y_k)) = (y_1, \ldots, y_{k-1}, e_x(e_x^{-1}(y_k))) = (y_1, \ldots, y_{k-1}, y_k) = y$$

für $y \in \mathrm{Perm}_k(X)$. Somit gilt $g \circ f = \mathrm{id}_{\mathrm{Perm}_{k-1}(X) \times [1, n-k+1]}$ und $f \circ g = \mathrm{id}_{\mathrm{Perm}_k(X)}$, d.h. f und g sind sich gegenseitige invertierende Abbildungen und damit Bijektionen nach Satz (3.29)(c). □

(18.29) Beispiel. Wir haben folgende Bijektion.

$$\begin{aligned}\mathrm{Perm}_1([1,3]) \times [1,2] &\to \mathrm{Perm}_2([1,3]),\\ ((1),1) &\mapsto (1,2),\\ ((1),2) &\mapsto (1,3),\\ ((2),1) &\mapsto (2,1),\\ ((2),2) &\mapsto (2,3),\\ ((3),1) &\mapsto (3,1),\\ ((3),2) &\mapsto (3,2).\end{aligned}$$

(18.30) Korollar. Es seien $n \in \mathbb{N}_0$ und eine n-elementige Menge X gegeben. Dann ist

$$|\mathrm{Perm}_k(X)| = \begin{cases} 1, & \text{für } k = 0,\\ |\mathrm{Perm}_{k-1}(X)|\,(n-k+1), & \text{für } k \in [1,n].\end{cases}$$

Beweis. Für $k = 0$ gilt

$$|\mathrm{Perm}_k(X)| = |\mathrm{Perm}_0(X)| = |\{()\}| = 1.$$

Für $k \in [1,n]$ sind

$$\begin{aligned}&\mathrm{Perm}_{k-1}(X) \times [1, n-k+1] \to \mathrm{Perm}_k(X),\ (x,j) \mapsto (x_1,\dots,x_{k-1},e_x(j)),\\ &\mathrm{Perm}_k(X) \to \mathrm{Perm}_{k-1}(X) \times [1,n-k+1],\ y \mapsto ((y_1,\dots,y_{k-1}),e_x^{-1}(y_k))\end{aligned}$$

wohldefinierte, sich gegenseitig invertierende Bijektionen nach Proposition (18.28), nach der Gleichheitsregel (18.1) und der Produktregel (18.8) gilt also

$$|\mathrm{Perm}_k(X)| = |\mathrm{Perm}_{k-1}(X) \times [1,n-k+1]| = |\mathrm{Perm}_{k-1}(X)|\,|[1,n-k+1]|. \qquad \square$$

(18.31) Korollar. Es seien $n,k \in \mathbb{N}_0$, eine n-elementige Menge X und eine k-elementige Menge I gegeben. Dann gilt

$$|\mathrm{Perm}_I(X)| = \prod_{i\in[1,k]} (n-i+1) = \prod_{i\in[n-k+1,n]} i.$$

Wenn $k \in [0,n]$ ist, so gilt

$$|\mathrm{Perm}_I(X)| = \frac{n!}{(n-k)!}.$$

Beweis. Zunächst zeigen wir $|\mathrm{Perm}_l(X)| = \prod_{i\in[1,l]}(n-i+1)$ für $l \in \mathbb{N}_0$ durch Induktion nach l. Für $l = 0$ gilt

$$|\mathrm{Perm}_l(X)| = 1 = \prod_{i\in[1,0]} (n-i+1) = \prod_{i\in[1,l]} (n-i+1)$$

nach Korollar (18.30). Für $l \in [1,n]$ mit $|\mathrm{Perm}_{l-1}(X)| = \prod_{i\in[1,l-1]}(n-i+1)$ gilt

$$|\mathrm{Perm}_l(X)| = |\mathrm{Perm}_{l-1}(X)|\,|[1,n-l+1]| = \prod_{i\in[1,l-1]} (n-i+1)\cdot(n-l+1) = \prod_{i\in[1,l]} (n-i+1)$$

nach Korollar (18.30). Schließlich sei $l \in \mathbb{N}$ mit $l \geq n+1$ und $|\mathrm{Perm}_{l-1}(X)| = \prod_{i\in[1,l-1]}(n-i+1)$ gegeben. Dann ist

$$\mathrm{Perm}_l(X) = \emptyset$$

nach dem Schubfachprinzip (18.12), wegen $n+1 \in [1,l]$ gilt also

$$\prod_{i\in[1,l]} (n-i+1) = \Big(\prod_{i\in[1,l]\setminus\{n+1\}} (n-i+1)\Big)\cdot(n-(n+1)+1) = 0 = |\mathrm{Perm}_l(X)|.$$

Nach dem Induktionsprinzip gilt $|\mathrm{Perm}_l(X)| = \prod_{i\in[1,l]}(n-i+1)$ für alle $l \in \mathbb{N}_0$.
Wegen $|I| = k$ gibt es eine Bijektion $e\colon [1,k] \to I$, welche uns wohldefinierte, sich gegenseitig invertierende Abbildungen

$$\mathrm{Perm}_I(X) \to \mathrm{Perm}_k(X),\ y \mapsto y \circ e,$$
$$\mathrm{Perm}_k(X) \to \mathrm{Perm}_I(X),\ x \mapsto x \circ e^{-1}$$

liefert. Nach Satz (3.29)(c) und der Gleichheitsregel (18.1) folgt

$$|\mathrm{Perm}_I(X)| = |\mathrm{Perm}_k(X)| = \prod_{i\in[1,k]} (n-i+1).$$

Da $[1,k] \to [n-k+1,n]$, $i \mapsto n-i+1$ eine Bijektion ist, gilt weiter

$$|\mathrm{Perm}_I(X)| = \prod_{i\in[1,k]} (n-i+1) = \prod_{i\in[n-k+1,n]} i.$$

Wenn $k \in [0,n]$ ist, so folgt schließlich

$$|\mathrm{Perm}_I(X)| = \prod_{i\in[n-k+1,n]} i = \frac{\prod_{i\in[1,n]} i}{\prod_{i\in[1,n-k]} i} = \frac{n!}{(n-k)!}.$$ □

(18.32) Korollar. Es seien $n \in \mathbb{N}_0$ und eine n-elementige Menge X gegeben. Dann gilt

$$|\mathrm{S}_X| = n!.$$

Beweis. Nach Bemerkung (18.27) und Korollar (18.31) gilt

$$|\mathrm{S}_X| = |\mathrm{Perm}_X(X)| = \prod_{i\in[n-n+1,n]} i = \prod_{i\in[1,n]} i = n!.$$ □

(18.33) Beispiel.

(a) Es ist

$$|\mathrm{Perm}_4([1,9])| = 3024.$$

(b) Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$|\mathrm{Perm}_3(\{a,b,c,d\})| = 24.$$

(c) Es ist

$$|\mathrm{S}_5| = 120.$$

Beweis.

(a) Nach Korollar (18.31) ist

$$|\mathrm{Perm}_4([1,9])| = \prod_{i\in[1,4]} (9-i+1) = 9\cdot 8\cdot 7\cdot 6 = 3024.$$

(b) Nach Korollar (18.31) ist

$$|\mathrm{Perm}_3(\{a,b,c,d\})| = \prod_{i\in[1,3]} (4-i+1) = 4\cdot 3\cdot 2 = 24.$$

(c) Nach Korollar (18.32) ist

$$|\mathrm{S}_5| = 5! = 120.$$ □

Wir kommen zu unseren Beispielen aus dem täglichen Leben zurück:

(18.34) Anwendungsbeispiel.

(a) Wörter, welche aus genau sechs verschiedenen Buchstaben des lateinischen Alphabets (ohne Sonderzeichen) bestehen, seien als 6-Permutationen in $\{\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}\}$ modelliert. Nach Korollar (18.31) ist die Anzahl aller solchen Wörter gleich

$$|\mathrm{Perm}_6(\{\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}\})| = \prod_{i \in [1,6]} (26 - i + 1) = 26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 \cdot 21 = 165\,765\,600.$$

(b) Auftragsverteilungen beim Spiel Risiko auf vier Spieler (bei 15 zur Verteilung stehenden Aufträgen) seien Permutationen in $[1, 15]$ über $\{\text{Désirée}, \text{Kirstin}, \text{Michael}, \text{Sebastian}\}$ modelliert. Nach Korollar (18.31) ist die Anzahl der möglichen Auftragsverteilungen gleich

$$|\mathrm{Perm}_{\{\text{Désirée},\text{Kirstin},\text{Michael},\text{Sebastian}\}}([1, 15])| = \prod_{i \in [1,4]} (15 - i + 1) = 15 \cdot 14 \cdot 13 \cdot 12 = 32\,760.$$

(c) Acht Teilnehmer eines Wettbewerbs seien als Elemente einer Menge T modelliert. Medaillenverteilungen bei diesem Wettbewerb seien als Permutationen in T über $\{\text{gold}, \text{silber}, \text{bronze}\}$ modelliert. Nach Korollar (18.31) ist die Anzahl möglichen Medaillenverteilungen gleich

$$|\mathrm{Perm}_{\{\text{gold},\text{silber},\text{bronze}\}}(T)| = \prod_{i \in [1,3]} (8 - i + 1) = 8 \cdot 7 \cdot 6 = 336.$$

(d) Die möglichen Tabellen der Fußball-Bundesliga der Saison 2016/17 seien als 18-Permutationen in

$$\begin{aligned} M = \{&\text{FC Augsburg}, \text{Hertha BSC}, \text{SV Werder Bremen}, \text{SV Darmstadt 98}, \text{Borussia Dortmund},\\ &\text{Eintracht Frankfurt}, \text{SC Freiburg}, \text{FC Ingolstadt 04}, \text{FC Schalke 04}, \text{Hamburger SV},\\ &\text{TSG 1899 Hoffenheim}, \text{1. FC Köln}, \text{RB Leipzig}, \text{Bayer 04 Leverkusen}, \text{1. FSV Mainz 05},\\ &\text{Borussia Mönchengladbach}, \text{FC Bayern München}, \text{VfL Wolfsburg}\} \end{aligned}$$

modelliert. Nach Korollar (18.31) ist die Anzahl aller möglichen Tabellen gleich

$$|\mathrm{Perm}_{18}(M)| = \prod_{i \in [1,18]} (18 - i + 1) = 18! \approx 6{,}40 \cdot 10^{15}.$$

(e) Die möglichen Mischungen eines Skatkartenspiels seien als 32-Permutationen in

$$X = \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \times \{7, 8, 9, 10, \mathrm{B}, \mathrm{D}, \mathrm{K}, \mathrm{A}\}$$

modelliert. Nach Korollar (18.31) ist die Anzahl aller möglichen Mischungen gleich

$$|\mathrm{Perm}_{32}(X)| = \prod_{i \in [1,32]} (32 - i + 1) = 32! \approx 2{,}63 \cdot 10^{35}.$$

(f) Verteilungen von vier unterschiedlich farbigen Kugeln auf zehn durchnummerierte Boxen derart, dass in jeder Box höchstens eine Kugel liegt, seien als Permutationen in $[1, 10]$ über $\{\text{rot}, \text{blau}, \text{gelb}, \text{grün}\}$ modelliert. Nach Korollar (18.31) ist die Anzahl aller solchen möglichen Verteilungen gleich

$$|\mathrm{Perm}_{\{\text{rot},\text{blau},\text{gelb},\text{grün}\}}([1, 10])| = \prod_{i \in [1,4]} (10 - i + 1) = 10 \cdot 9 \cdot 8 \cdot 7 = 5040.$$

Multikombinationen und Kombinationen

Im Folgenden studieren wir Auswahlen, welche gleichzeitig stattfinden oder, mit anderen Worten, bei denen die Reihenfolge der Auswahl keine Rolle spielt. Dies können wir dadurch modellieren, dass wir solche Variationen als gleich betrachten, deren Einträge durch eine Permutation der Indizes auseinander hervorgehen. Diese schwächere Form der Gleichheit können wir wiederum mit Hilfe einer geeigneten Äquivalenzrelation formalisieren.
Zur einfacheren Beschreibung fassen wir Variationen als Abbildungen auf, vgl. Konvention (3.9).

(18.35) Definition (Eintragsgleichheit)**.** Es seien Mengen X und I gegeben. Für $x, y \in \mathrm{Var}_I(X)$ gelte genau dann $x \sim y$, wenn es eine Permutation π von I mit $y = x \circ \pi$ gibt. Die Relation $\sim$ wird *Eintragsgleichheit* von Variationen in X über I genannt.

(18.36) Beispiel. Es ist $(5, 3, 9, 7) \sim (7, 3, 5, 9)$ in $\mathrm{Var}_4([1, 9])$.

Beweis. Es sei $x := (5, 3, 9, 7)$ und $y := (7, 3, 5, 9)$. Für die Permutation $\pi\colon [1, 4] \to [1, 4]$, $1 \mapsto 4$, $2 \mapsto 2$, $3 \mapsto 1$, $4 \mapsto 3$ gilt dann

$$\begin{aligned} x_{\pi(1)} &= x_4 = 7 = y_1, \\ x_{\pi(2)} &= x_2 = 3 = y_2, \\ x_{\pi(3)} &= x_1 = 5 = y_3, \\ x_{\pi(4)} &= x_3 = 9 = y_4, \end{aligned}$$

also $y = x \circ \pi$. Folglich gilt $x \sim y$. □

(18.37) Bemerkung. Es seien Mengen X und I gegeben. Dann ist $\sim$ eine Äquivalenzrelation auf $\mathrm{Var}_I(X)$.

Beweis. Es seien $x, y, z \in \mathrm{Var}_I(X)$ mit $x \sim y$ und $y \sim z$ gegeben, so dass es $\pi, \sigma \in \mathrm{S}_I$ mit $y = x \circ \pi$ und $z = y \circ \sigma$ gibt. Dann folgt $z = y \circ \sigma = x \circ \pi \circ \sigma$ und wegen $\pi \circ \sigma \in \mathrm{S}_I$ somit $x \sim z$. Folglich ist $\sim$ transitiv.
Für alle $x \in \mathrm{Var}_I(X)$ gilt $x = x \circ \mathrm{id}_I$, wegen $\mathrm{id}_I \in \mathrm{S}_I$ also $x \sim x$. Folglich ist $\sim$ reflexiv.
Es seien $x, y \in \mathrm{Var}_I(X)$ mit $x \sim y$ gegeben, so dass es ein $\pi \in \mathrm{S}_I$ mit $y = x \circ \pi$ gibt. Dann folgt $x = y \circ \pi^{-1}$ und wegen $\pi^{-1} \in \mathrm{S}_I$ somit $y \sim x$. Folglich ist $\sim$ symmetrisch.
Insgesamt ist $\sim$ eine Äquivalenzrelation auf $\mathrm{Var}_I(X)$. □

Unser Modell für Auswahlen ohne Beachtung der Reihenfolge werden Äquivalenzklassen von Variationen unter der Eintragsgleichheit sein:

(18.38) Definition (Multikombination)**.** Es sei eine Menge X gegeben.

(a) Es sei eine Menge I gegeben. Die *Menge der Multikombinationen* in X über I ist definiert als

$$\mathrm{MComb}_I(X) := \mathrm{Var}_I(X)/\!\sim.$$

Ein Element von $\mathrm{MComb}_I(X)$ wird eine *Multikombination* in X über I (oder *I-Multikombination* in X oder *I-Kombination mit Wiederholung* in X) genannt.

Für eine Variation $x = (x_i)_{i \in I}$ in X über I schreiben wir auch

$$[x_i]_{i \in I} := [x].$$

(b) Es sei $k \in \mathbb{N}_0$ gegeben. Die *Menge der k-Multikombinationen* in X ist definiert als

$$\mathrm{MComb}_k(X) := \mathrm{MComb}_{[1,k]}(X).$$

Ein Element von $\mathrm{MComb}_k(X)$ wird eine *k-Multikombination* (oder *k-Kombination mit Wiederholung*) in X genannt.

Für eine k-Variation $x = (x_1, \ldots, x_k)$ in X schreiben wir auch

$$[x_1, \ldots, x_k] := [x].$$

(18.39) Beispiel.

(a) Es ist $[5,3,9,7] = [3,5,7,9]$ eine 4-Multikombination in $[1,9]$.

(b) Es ist $[5,3,5,7] = [3,5,5,7]$ eine 4-Multikombination in $[1,9]$.

(18.40) Beispiel. Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$\begin{aligned}\mathrm{MComb}_3(\{a,b,c,d\}) = \{&[a,a,a],[a,a,b],[a,a,c],[a,a,d],[a,b,b],[a,b,c],[a,b,d],[a,c,c],[a,c,d],[a,d,d],\\ &[b,b,b],[b,b,c],[b,b,d],[b,c,c],[b,c,d],[b,d,d],[c,c,c],[c,c,d],[c,d,d],[d,d,d]\}\end{aligned}$$

Wir betrachten wieder einige Beispiele aus dem täglichen Leben:

(18.41) Anwendungsbeispiel.

(a) Eine Belegung einer Getränkekiste mit zwölf Flaschen aus drei verschiedenen Getränkesorten lässt sich als 12-Multikombination in $\{\mathrm{Cola}, \mathrm{Fanta}, \mathrm{Sprite}\}$ auffassen.

(b) Die Kandidaten bei einer Wahl, bei der jeder Wähler genau eine (gültige) Stimme für einen Kandidaten abgibt, seien als Elemente einer Menge K modelliert. Die Wähler seien als Elemente einer Menge W modelliert. Das Wahlergebnis lässt sich als Multikombination in K über W auffassen.

(c) Ein Lostopf bestehend aus 100 Losen, wobei jedes Los entweder mit „Hauptpreis“ oder mit „Trostpreis“ oder mit „Niete“ beschriftet ist, lässt sich als 100-Multikombination in $\{\mathrm{Hauptpreis}, \mathrm{Trostpreis}, \mathrm{Niete}\}$ auffassen.

(d) Ein Wurf beim Spiel Kniffel lässt sich als 5-Multikombination in $\{\boxdot, \boxdot, \boxdot, \boxdot, \boxdot, \boxdot\}$ auffassen.

(e) Die Teilnehmer einer Klausur seien als Elemente einer Menge T modelliert. Das anonymisierte Ergebnis einer Klausur (Notenspiegel) lässt sich als Multikombination in $\{1.0, 1.3, 1.7, 2.0, 2.3, 2.7, 3.0, 3.3, 3.7, 4.0, 5.0\}$ über T auffassen.

(f) Eine Verteilung von zehn gleich aussehenden Kugeln auf vier unterschiedlich farbige Boxen lässt sich als 10-Multikombination in $\{\mathrm{rot}, \mathrm{blau}, \mathrm{gelb}, \mathrm{grün}\}$ auffassen.

Bei Multikombinationen über endlichen Mengen kommt es nicht auf die Reihenfolge der Einträge der Repräsentanten an, sondern nur auf die jeweiligen Anzahlen der verschiedenen vorkommenden Einträge. Mit anderen Worten: Die Häufigkeitsfunktionen der Repräsentanten sind gleich. Etwas genauer erhalten wir folgenden Zusammenhang zur äquivalenten Beschreibung von Multikombinationen:

(18.42) Satz. Es seien $k \in \mathbb{N}_0$, eine Menge X und eine k-elementige Menge I gegeben. Dann ist

$$\mathrm{MComb}_I(X) \to \{m \in \mathbb{N}_0^{(X)} \mid \sum_{y \in X} m_y = k\},\ [x] \mapsto \mu_x$$

eine wohldefinierte Bijektion.

Beweis. Wir betrachten die Abbildung

$$\mu_- \colon \mathrm{Var}_I(X) \to \mathbb{N}_0^X,\ x \mapsto \mu_x.$$

Nach dem Homomorphiesatz für Mengen (5.15) induziert μ_- eine wohldefinierte Injektion

$$\bar{\mu}_- \colon \mathrm{Var}_I(X)/{=_m} \to \mathbb{N}_0^X$$

mit $\mu_- = \bar{\mu}_- \circ \mathrm{quo}$, gegeben durch $\bar{\mu}_{[x]} = \mu_x = (|\{i \in I \mid x_i = y\}|)_{y \in X}$ für $x \in \mathrm{Var}_I(X)$, und mit $\operatorname{Im} \bar{\mu}_- = \operatorname{Im} \mu_-$. Um zu zeigen, dass $=_{\mu_-} = \sim$ ist, seien $x, x' \in \mathrm{Var}_I(X)$ gegeben. Zunächst gelte $x =_{\mu_-} x'$ in $\mathrm{Var}_I(X)$, d.h. es gelte $\mu_x = \mu_{x'}$ in $\mathbb{N}_0^X$. Für jedes $y \in X$ ist dann

$$|\{i \in I \mid x_i = y\}| = (\mu_x)_y = (\mu_{x'})_y = |\{i \in I \mid x'_i = y\}|,$$

d.h. es gibt eine Bijektion

$$f_y \colon \{i \in I \mid x'_i = y\} \to \{i \in I \mid x_i = y\}.$$

Wir definieren $\pi\colon I \to I$, $i \mapsto f_{x'_i}(i)$ und $\sigma\colon I \to I$, $i \mapsto f_{x_i}^{-1}(i)$. Für $i \in I$ folgt $x_{\pi(i)} = x_{f_{x'_i}(i)} = x'_i$ sowie $x'_{\sigma(i)} = x'_{f_{x_i}^{-1}(i)} = x_i$, also

$$\sigma(\pi(i)) = f_{x_{\pi(i)}}^{-1}(\pi(i)) = f_{x'_i}^{-1}(f_{x'_i}(i)) = i,$$
$$\pi(\sigma(i)) = f_{x'_{\sigma(i)}}(\sigma(i)) = f_{x_i}(f_{x_i}^{-1}(i)) = i.$$

Folglich ist $\sigma \circ \pi = \pi \circ \sigma = \mathrm{id}_I$, d.h. π und σ sind sich gegenseitig invertierende Permutationen von I. Wegen $x'_i = x_{\pi(i)}$ für $i \in I$ gilt ferner $x' = x \circ \pi$ und damit $x \sim x'$. Umgekehrt gelte $x \sim x'$ und damit $x' \sim x$, d.h. es gebe eine Permutation π von I mit $x = x' \circ \pi$. Ferner sei $y \in X$ gegeben. Für $i \in I$ mit $x_i = y$ gilt $x'_{\pi(i)} = x_i = y$ und für $i' \in I$ mit $x'_{i'} = y$ gilt $x_{\pi^{-1}(i')} = x'_{i'} = y$. Folglich schränken π und π^{-1} zu sich gegenseitig invertierenden Bijektionen

$$\{i \in I \mid x_i = y\} \to \{i' \in I \mid x'_{i'} = y\},\ i \mapsto \pi(i),$$
$$\{i' \in I \mid x'_{i'} = y\} \to \{i \in I \mid x_i = y\},\ i' \mapsto \pi^{-1}(i')$$

ein. Es gilt also

$$(\mu_x)_y = |\{i \in I \mid x_i = y\}| = |\{i' \in I \mid x'_{i'} = y\}| = (\mu_{x'})_y$$

für $y \in X$, folglich $\mu_x = \mu_{x'}$ und damit $x =_{\mu_-} x'$. Somit gilt in der Tat $=_{\mu_-} = \sim$ und folglich

$$\mathrm{Var}_I(X)/=_{\mu_-} = \mathrm{Var}_I(X)/\sim = \mathrm{MComb}_I(X).$$

Als nächstes bestimmen wir $\operatorname{Im}\bar{\mu}_- = \operatorname{Im}\mu_-$. Für $x \in \mathrm{Var}_I(X)$ gilt $I = \dot{\bigcup}_{y\in X}\{i \in I \mid x_i = y\}$, also

$$\sum_{y\in X}(\mu_x)_y = \sum_{y\in X}|\{i \in I \mid x_i = y\}| = |\dot{\bigcup_{y\in X}}\{i \in I \mid x_i = y\}| = |I| = k$$

und damit $\mu_x \in \{a \in \mathbb{N}_0^{(X)} \mid \sum_{y\in X} m_y = k\}$. Nun sei umgekehrt ein $m \in \mathbb{N}_0^{(X)}$ mit $\sum_{y\in X} m_y = k$ gegeben und es sei $l := |\{y \in X \mid m_y \neq 0\}|$. Ferner sei e eine Abzählung von I und f eine Abzählung von $\{y \in X \mid m_y \neq 0\}$. Dann gilt $[1,k] = \dot{\bigcup}_{r\in[1,l]}[\sum_{j\in[1,r-1]} m_{f(j)} + 1, \sum_{j\in[1,r]} m_{f(j)}]$. Es sei $x \in \mathrm{Var}_I(X)$ gegeben durch $x_i = f(r)$ für $i \in I$ und $r \in [1,l]$ mit $e^{-1}(i) \in [\sum_{j\in[1,r-1]} m_{f(j)} + 1, \sum_{j\in[1,r]} m_{f(j)}]$. Für $y \in X \setminus \{f(r) \mid r \in [1,l]\}$ gilt dann $(\mu_x)_y = 0 = m_y$, und für $r \in [1,l]$ gilt

$$(\mu_x)_{f(r)} = |\{i \in I \mid x_i = f(r)\}| = |\{i \in I \mid e^{-1}(i) \in [\sum_{j\in[1,r-1]} m_{f(j)} + 1, \sum_{j\in[1,r]} m_{f(j)}]\}|$$
$$= |[\sum_{j\in[1,r-1]} m_{f(j)} + 1, \sum_{j\in[1,r]} m_{f(j)}]| = m_{f(r)}.$$

Folglich gilt $(\mu_x)_y = m_y$ für alle $y \in X$, d.h. es ist $\mu_x = m$. Wir haben somit

$$\operatorname{Im}\bar{\mu}_- = \operatorname{Im}\mu_- = \{m \in \mathbb{N}_0^{(X)} \mid \sum_{y\in X} m_y = k\}.$$

Insgesamt ist

$$\bar{\mu}_-|^{\operatorname{Im}\bar{\mu}_-}\colon \mathrm{MComb}_I(X) \to \{m \in \mathbb{N}_0^{(X)} \mid \sum_{y\in X} m_y = k\},\ [x] \mapsto \mu_x$$

eine Bijektion. □

(18.43) Beispiel. Wir haben folgende Bijektion.

$$\mathrm{MComb}_2([1,3]) \to \{m \in \mathbb{N}_0^3 \mid m_1 + m_2 + m_3 = 2\},$$
$$[1,1] \mapsto (2,0,0),$$
$$[1,2] \mapsto (1,1,0),$$
$$[1,3] \mapsto (1,0,1),$$
$$[2,2] \mapsto (0,2,0),$$
$$[2,3] \mapsto (0,1,1),$$
$$[3,3] \mapsto (0,0,2).$$

Satz (18.42) legt nahe, den Begriff der Häufigkeitsfunktion bzw. Häufigkeitsfamilie auf Multikombinationen auszudehnen:

(18.44) Definition (Häufigkeitsfunktion)**.** Es seien $k \in \mathbb{N}_0$, eine Menge X, eine k-elementige Menge I und eine I-Variation x in X gegeben. Die Häufigkeitsfunktion von x in X wird auch *Häufigkeitsfunktion* von $[x]$ in X genannt und als

$$\mu_{[x]} := \mu_x \colon X \to \mathbb{N}_0,\ y \mapsto |\{i \in I \mid x_i = y\}|$$

notiert.

(18.45) Beispiel.

(a) Das Häufigkeitstupel der 4-Multikombination $[5, 3, 9, 7]$ in $[1, 9]$ ist gegeben durch

$$\mu_{[5,3,9,7]} = (0, 0, 1, 0, 1, 0, 1, 0, 1).$$

(b) Das Häufigkeitstupel der 4-Multikombination $[5, 3, 5, 7]$ in $[1, 9]$ ist gegeben durch

$$\mu_{[5,3,5,7]} = (0, 0, 1, 0, 2, 0, 1, 0, 0).$$

Da Multikombinationen sich wie Mengen verhalten, in denen Elemente mehr als einmal vorkommen dürfen, werden Multikombinationen in einer Menge X oder deren Häufigkeitsfamilien manchmal auch *Multimengen* über X genannt und dann mit Mengenklammern oder leicht modifizierten Mengenklammern notiert. Vgl. Proposition (18.108).
Multikombinationen in einer angeordneten Menge wie $[1, n]$ für ein $n \in \mathbb{N}_0$ können über kanonische Repräsentanten beschrieben werden:

(18.46) Proposition. Es seien $n, k \in \mathbb{N}_0$ gegeben. Dann ist

$$\{x \in \mathrm{Var}_k([1, n]) \mid \text{für } i \in [1, k-1] \text{ gilt } x_i \leq x_{i+1}\}$$

eine Transversale von $\mathrm{MComb}_k([1, n])$.

Beweis. Zunächst sei $y \in \mathrm{Var}_k([1, n])$ gegeben und es sei $a := (|\{i \in [1, k] \mid y_i = j\}|)_{j \in [1,n]}$. Wir definieren $x \in \mathrm{Var}_k([1, n])$ durch $x_i := l$ für $l \in [1, n]$ und $i \in [\sum_{j \in [1,l-1]} a_j + 1, \sum_{j \in [1,l]} a_j]$. Für $i \in [1, k-1]$ ist $x_i \leq x_{i+1}$. Ferner gilt für $l \in [1, n]$ stets

$$|\{i \in [1, k] \mid x_i = l\}| = |[\sum_{j \in [1,l-1]} a_j + 1, \sum_{j \in [1,l]} a_j]| = a_l = |\{i \in [1, k] \mid y_i = l\}|,$$

so dass $[y] = [x]$ nach Satz (18.42) folgt.
Als nächstes seien $x, x' \in \mathrm{Var}_k([1, n])$ mit $x_i \leq x_{i+1}$ und $x'_i \leq x'_{i+1}$ für $i \in [1, k]$ sowie $[x] = [x']$ in $\mathrm{MComb}_k([1, n])$ gegeben. Nach Satz (18.42) gilt dann auch $|\{i \in [1, k] \mid x_i = j\}| = |\{i \in [1, k] \mid x'_i = j\}|$ für $j \in [1, n]$, so dass wir induktiv $x = x'$ erhalten.
Insgesamt ist $\{x \in \mathrm{Var}_k([1, n]) \mid \text{für } i \in [1, k-1] \text{ gilt } x_i \leq x_{i+1}\}$ eine Transversale von $\mathrm{MComb}_k([1, n])$. □

Für $k \in \mathbb{N}$ lässt sich die Anzahl der k-Multikombinationen einer gegebenen endlichen Menge X rekursiv berechnen, siehe Korollar (18.49). Im Beweis benutzen wir die Zerlegung

$$\mathrm{MComb}_k(X) = \dot{\bigcup_{i \in [0,k]}} \{C \in \mathrm{MComb}_k(X) \mid (\mu_C)_y = k - i\}$$

für ein $y \in X$, wobei sich die Anzahlen der Teilmengen via folgender Bemerkung zu Anzahlen von Multikombinationen von $X \setminus \{y\}$ ergeben:

(18.47) Bemerkung. Es seien $k \in \mathbb{N}_0$, eine Menge X und $y \in X$ gegeben. Für $i \in [0, k]$ ist

$$\mathrm{MComb}_i(X \setminus \{y\}) \to \{C \in \mathrm{MComb}_k(X) \mid (\mu_C)_y = k - i\},\ [x] \mapsto [x\,(y)_{j \in [1,k-i]}]$$

eine wohldefinierte Bijektion.

(18.48) Beispiel. Wir haben folgende Bijektion.

$$\begin{aligned}\mathrm{MComb}_2([1,3]) &\to \{C \in \mathrm{MComb}_3([1,4]) \mid (\mu_C)_4 = 1\},\\ [1,1] &\mapsto [1,1,4],\\ [1,2] &\mapsto [1,2,4],\\ [1,3] &\mapsto [1,3,4],\\ [2,2] &\mapsto [2,2,4],\\ [2,3] &\mapsto [2,3,4],\\ [3,3] &\mapsto [3,3,4].\end{aligned}$$

(18.49) Korollar. Es sei eine endliche Menge X gegeben. Dann ist

$$|\mathrm{MComb}_k(X)| = \begin{cases} 1, & \text{für } k = 0, \text{ falls } X = \emptyset,\\ 0, & \text{für } k \in \mathbb{N}, \text{ falls } X = \emptyset,\\ \sum_{i\in[0,k]} |\mathrm{MComb}_i(X \setminus \{y\})|, & \text{für } k \in \mathbb{N}_0,\ y \in X.\end{cases}$$

Beweis. Es sei $k \in \mathbb{N}_0$ gegeben. Falls $X = \emptyset$ ist, so gilt

$$\mathrm{MComb}_k(X) = \mathrm{MComb}_k(\emptyset) = \begin{cases}\{[\,]\}, & \text{falls } k = 0,\\ \emptyset, & \text{falls } k \in \mathbb{N},\end{cases}$$

und damit

$$|\mathrm{MComb}_k(X)| = \begin{cases}1, & \text{falls } k = 0,\\ 0, & \text{falls } k \in \mathbb{N}.\end{cases}$$

Im Folgenden sei $X \neq \emptyset$ und es sei $y \in X$ gegeben. Dann ist

$$\mathrm{MComb}_k(X) = \dot{\bigcup_{i\in[0,k]}} \{C \in \mathrm{MComb}_k(X) \mid (\mu_C)_y = k - i\}.$$

Für $i \in [0,k]$ ist ferner

$$\mathrm{MComb}_i(X \setminus \{y\}) \to \{C \in \mathrm{MComb}_k(X) \mid (\mu_C)_y = k - i\},\ [x] \mapsto [x\,(y)_{j\in[1,k-i]}]$$

eine wohldefinierte Bijektion. Nach der Summenregel (18.4) und der Gleichheitsregel (18.1) folgt

$$\begin{aligned}|\mathrm{MComb}_k(X)| &= |\dot{\bigcup_{i\in[0,k]}} \{C \in \mathrm{MComb}_k(X) \mid (\mu_C)_y = k - i\}|\\ &= \sum_{i\in[0,k]} |\{C \in \mathrm{MComb}_k(X) \mid (\mu_C)_y = k - i\}| = \sum_{i\in[0,k]} |\mathrm{MComb}_i(X \setminus \{y\})|.\end{aligned}$$ □

Die durch Korollar (18.49) gegebene Rekursion lässt sich nun ausnutzen um eine Formel für die Anzahl der Multikombinationen in einer gegebenen Menge zu verifizieren:

(18.50) Korollar. Für $n, k \in \mathbb{N}_0$, jede n-elementige Menge X und jede k-elementige Menge I gilt

$$|\mathrm{MComb}_I(X)| = \binom{k+n-1}{k}.$$

Beweis. Um zu zeigen, dass $n, k \in \mathbb{N}_0$ und jede n-elementige Menge X stets $|\mathrm{MComb}_k(X)| = \binom{k+n-1}{k}$ gilt, führen wir Induktion nach n. Für $n = 0$, $k \in \mathbb{N}_0$ und jede n-elementige Menge X gilt $X = \emptyset$, nach Korollar (18.49), Proposition (17.7) und Bemerkung (17.6) also

$$|\mathrm{MComb}_k(X)| = \left\{\begin{cases}1, & \text{falls } k = 0,\\ 0, & \text{falls } k \in \mathbb{N}\end{cases}\right\} = \binom{k-1}{k} = \binom{k+n-1}{k}.$$

Es sei $n \in \mathbb{N}$ so gegeben, dass für $k \in \mathbb{N}_0$ und jede $(n-1)$-elementige Menge X' stets $|\mathrm{MComb}_k(X')| = \binom{k+(n-1)-1}{k} = \binom{k+n-2}{k}$ gilt. Ferner seien $k \in \mathbb{N}_0$ und eine n-elementige Menge X gegeben. Dann ist $X \neq \emptyset$, d.h. es gibt ein $y \in X$. Nach Korollar (18.49), der Induktionsvoraussetzung und Korollar (17.9) folgt

$$|\mathrm{MComb}_k(X)| = \sum_{i\in[0,k]} |\mathrm{MComb}_i(X \setminus \{y\})| = \sum_{i\in[0,k]} \binom{i+n-2}{i} = \binom{k+n-1}{k}.$$

Nach dem Induktionsprinzip gilt $|\mathrm{MComb}_k(X)| = \binom{k+n-1}{k}$ für $n, k \in \mathbb{N}_0$ und jede n-elementige Menge X.
Nun seien $n, k \in \mathbb{N}_0$, eine n-elementige Menge X und eine k-elementige Menge I gegeben. Dann gibt es eine Abzählung $e\colon [1,k] \to I$, welche uns wohldefinierte, sich gegenseitig invertierende Abbildungen

$$\mathrm{MComb}_I(X) \to \mathrm{MComb}_k(X),\ [y] \mapsto [y \circ e],$$
$$\mathrm{MComb}_k(X) \to \mathrm{MComb}_I(X),\ [x] \mapsto [x \circ e^{-1}]$$

liefert. Nach Satz (3.29)(c) und der Gleichheitsregel (18.1) folgt

$$|\mathrm{MComb}_I(X)| = |\mathrm{MComb}_k(X)| = \binom{k+n-1}{k}.$$ □

(18.51) Beispiel.

(a) Es ist

$$|\mathrm{MComb}_4([1,9])| = 495.$$

(b) Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$|\mathrm{MComb}_3(\{a,b,c,d\})| = 20.$$

Beweis.

(a) Nach Korollar (18.50) und Korollar (17.12) ist

$$|\mathrm{MComb}_4([1,9])| = \binom{4+9-1}{4} = \binom{12}{4} = \frac{12\cdot 11\cdot 10\cdot 9}{1\cdot 2\cdot 3\cdot 4} = 495.$$

(b) Nach Korollar (18.50) ist

$$|\mathrm{MComb}_3(\{a,b,c,d\})| = \binom{3+4-1}{3} = \binom{6}{3} = \frac{6\cdot 5\cdot 4}{1\cdot 2\cdot 3} = 20.$$ □

Wir kommen zu unseren Beispielen aus dem täglichen Leben zurück:

(18.52) Anwendungsbeispiel.

(a) Belegungen einer Getränkekiste mit zwölf Flaschen aus drei verschiedenen Getränkesorten seien als 12-Multikombination in $\{\mathrm{Cola}, \mathrm{Fanta}, \mathrm{Sprite}\}$ modelliert. Nach Korollar (18.50) ist die Anzahl aller möglichen Belegungen gleich

$$|\mathrm{MComb}_{12}(\{\mathrm{Cola}, \mathrm{Fanta}, \mathrm{Sprite}\})| = \binom{12+3-1}{3-1} = \binom{14}{2} = 91.$$

(b) Die vier Kandidaten bei einer Wahl, bei der jeder der 130 Wähler genau eine (gültige) Stimme für einen Kandidaten abgibt, seien als Elemente einer 4-elementigen Menge K modelliert. Die Wähler seien als Elemente einer 130-elementigen Menge W modelliert. Die Wahlergebnisse seien als Multikombinationen in K über W modelliert. Nach Korollar (18.50) ist die Anzahl aller möglichen Wahlergebnisse gleich

$$|\mathrm{MComb}_W(K)| = \binom{130+4-1}{4-1} = \binom{133}{3} = 383\,306.$$

(c) Ein Lostopf bestehend aus 100 Losen, wobei jedes Los entweder mit „Hauptpreis“ oder mit „Trostpreis“ oder mit „Niete“ beschriftet ist, sei als 100-Multikombination in {Hauptpreis, Trostpreis, Niete} modelliert. Die Anzahl aller verschiedenen möglichen Lostöpfe ist gleich

$$|\mathrm{MComb}_{100}(\{\text{Hauptpreis}, \text{Trostpreis}, \text{Niete}\})| = \binom{100+3-1}{3-1} = \binom{102}{2} = 5151.$$

(d) Würfe beim Spiel Kniffel seien als 5-Multikombination in $\{\boxdot, \boxdot, \boxdot, \boxdot, \boxdot, \boxdot\}$ modelliert. Nach Korollar (18.50) ist die Anzahl aller möglichen Würfe gleich

$$|\mathrm{MComb}_5(\{\boxdot, \boxdot, \boxdot, \boxdot, \boxdot, \boxdot\})| = \binom{5+6-1}{5} = \binom{10}{5} = 252.$$

(e) Die 400 Teilnehmer einer Klausur seien als Elemente einer Menge T modelliert. Die möglichen Notenspiegel seien als Multikombinationen in $\{1.0, 1.3, 1.7, 2.0, 2.3, 2.7, 3.0, 3.3, 3.7, 4.0, 5.0\}$ über T modelliert. Nach Korollar (18.50) ist die Anzahl aller möglichen Notenspiegel gleich

$$\begin{aligned}|\mathrm{MComb}_T(\{1.0, 1.3, 1.7, 2.0, 2.3, 2.7, 3.0, 3.3, 3.7, 4.0, 5.0\})| &= \binom{400+11-1}{11-1} = \binom{410}{10} \\ &\approx 3{,}31 \cdot 10^{19}.\end{aligned}$$

(f) Verteilungen von zehn gleich aussehenden Kugeln auf vier unterschiedlich farbige Boxen seien als 10-Multikombinationen in {rot, blau, gelb, grün} modelliert. Nach Korollar (18.50) ist die Anzahl aller solchen möglichen Verteilungen gleich

$$|\mathrm{MComb}_{10}(\{\text{rot}, \text{blau}, \text{gelb}, \text{grün}\})| = \binom{10+4-1}{4-1} = \binom{13}{3} = 286.$$

Schließlich betrachten wir den Fall von Multikombinationen, die von einer Permutation repräsentiert werden. Zunächst stellen wir fest, dass mit einem Repräsentanten auch alle anderen Permutationen sind:

(18.53) Bemerkung. Es seien Mengen X und I und I-Variationen x und y in X mit $x \sim y$ gegeben. Genau dann ist x eine I-Permutation in X, wenn y eine I-Permutation in X ist.

Beweis. Wegen $x \sim y$ gibt es ein $\pi \in \mathrm{S}_I$ mit $y = x \circ \pi$, oder äquivalent $x = y \circ \pi^{-1}$. Da π und π^{-1} bijektiv sind, ist folglich $x\colon I \to X$ genau dann injektiv, wenn $y\colon I \to X$ injektiv ist, d.h. x ist genau dann eine I-Permutation in X, wenn y eine I-Permutation in X ist. □

Im Folgenden bezeichnen wir Einschränkungen der Eintragsgleichheit $\sim$ auf die entsprechenden Mengen von Permutationen wieder als $\sim$.
Von Permutationen repräsentierte Multikombinationen modellieren Auswahlen ohne Beachtung der Reihenfolge, bei denen die Möglichkeit der Wiederholung ausgeschlossen wird. Wir geben auch diesen eine Bezeichnung:

(18.54) Definition (Kombination)**.** Es sei eine Menge X gegeben.

(a) Es sei eine Menge I gegeben. Die *Menge der Kombinationen* in X über I ist definiert als

$$\mathrm{Comb}_I(X) := \mathrm{Perm}_I(X)/\sim.$$

Ein Element von $\mathrm{Comb}_I(X)$ wird eine *Kombination* in X über I (oder *I-Kombination* in X oder *I-Kombination ohne Wiederholung* in X) genannt.

(b) Es sei $k \in \mathbb{N}_0$ gegeben. Die *Menge der k-Kombinationen* in X ist definiert als

$$\mathrm{Comb}_k(X) := \mathrm{Comb}_{[1,k]}(X).$$

Ein Element von $\mathrm{Comb}_k(X)$ wird eine *k-Kombination* (oder *k-Kombination ohne Wiederholung*) in X genannt.

(18.55) Beispiel.

(a) Es ist $[5,3,9,7] = [3,5,7,9]$ eine 4-Kombination in $[1,9]$.

(b) Die 4-Multikombination $[5,3,5,7] = [3,5,5,7]$ in $[1,9]$ ist keine 4-Kombination in $[1,9]$.

(18.56) Beispiel. Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$\mathrm{Comb}_3(\{a,b,c,d\}) = \{[a,b,c],[a,b,d],[a,c,d],[b,c,d]\}.$$

Auch für Kombinationen betrachten wir wieder einige Beispiele aus dem täglichen Leben:

(18.57) Anwendungsbeispiel.

(a) Eine Ziehung der Lottozahlen lässt sich als 6-Kombination in $[1,49]$ auffassen.

(b) Eine Skathand lässt sich als 10-Kombination in $\{\heartsuit,\diamondsuit,\spadesuit,\clubsuit\} \times \{7,8,9,10,\mathrm{B},\mathrm{D},\mathrm{K},\mathrm{A}\}$ auffassen.

(c) Die Gesamtheit der Fußball-Bundesliga-Absteiger der Saison 2016/17 lässt sich als 2-Kombination (ohne Relegationsplatz) oder 3-Kombination (mit Relegationsplatz) in

$$\{\text{FC Augsburg}, \text{Hertha BSC}, \text{SV Werder Bremen}, \text{SV Darmstadt 98}, \text{Borussia Dortmund},\\ \text{Eintracht Frankfurt}, \text{SC Freiburg}, \text{FC Ingolstadt 04}, \text{FC Schalke 04}, \text{Hamburger SV},\\ \text{TSG 1899 Hoffenheim}, \text{1. FC Köln}, \text{RB Leipzig}, \text{Bayer 04 Leverkusen}, \text{1. FSV Mainz 05},\\ \text{Borussia Mönchengladbach}, \text{FC Bayern München}, \text{VfL Wolfsburg}\}$$

auffassen.

(d) Eine Verteilung von vier gleich aussehenden Kugeln auf zehn durchnummerierte Boxen derart, dass in jeder Box höchstens eine Kugel liegt, lässt sich als 4-Kombination in $[1,10]$ auffassen.

(18.58) Bemerkung. Es seien $n,k \in \mathbb{N}_0$ gegeben. Dann ist

$$\{x \in \mathrm{Var}_k([1,n]) \mid \text{für } i \in [1,k-1] \text{ gilt } x_i < x_{i+1}\}$$

eine Transversale von $\mathrm{Comb}_k([1,n])$.

Beweis. Nach Proposition (18.46) ist $\{x \in \mathrm{Var}_k([1,n]) \mid \text{für } i \in [1,k-1] \text{ gilt } x_i \leq x_{i+1}\}$ eine Transversale von $\mathrm{Var}_k([1,n])$ bzgl. $\sim$ und damit

$$\begin{aligned}
&\{x \in \mathrm{Var}_k([1,n]) \mid \text{für } i \in [1,k-1] \text{ gilt } x_i \leq x_{i+1}\} \cap \mathrm{Perm}_k([1,n])\\
&= \{x \in \mathrm{Perm}_k([1,n]) \mid \text{für } i \in [1,k-1] \text{ gilt } x_i \leq x_{i+1}\}\\
&= \{x \in \mathrm{Perm}_k([1,n]) \mid \text{für } i \in [1,k-1] \text{ gilt } x_i < x_{i+1}\}\\
&= \{x \in \mathrm{Var}_k([1,n]) \mid \text{für } i \in [1,k-1] \text{ gilt } x_i < x_{i+1}\}
\end{aligned}$$

eine Transversale von $\mathrm{Comb}_k([1,n])$. □

Zunächst zählen wir nun Kombinationen in einer endlichen Menge. Danach führen wir den Fall von Multikombinationen in einer endlichen Menge auf den Fall von Kombinationen in einer anderen endlichen Menge zurück.

(18.59) Bemerkung. Es seien Mengen X und I sowie eine I-Permutation x in X gegeben. Dann ist

$$\mathrm{S}_I \to [x],\ \pi \mapsto x \circ \pi$$

eine Bijektion.

Beweis. Wegen

$$[x] = \{y \in \mathrm{Var}_I(X) \mid x \sim y\} = \{y \in \mathrm{Var}_I(X) \mid \text{es gibt ein } \pi \in \mathrm{S}_I \text{ mit } y = x \circ \pi\} = \{x \circ \pi \mid \pi \in \mathrm{S}_I\}$$

ist $\mathrm{S}_I \to [x]$, $\pi \mapsto x \circ \pi$ surjektiv. Für $\pi, \sigma \in \mathrm{S}_I$ mit $x \circ \pi = x \circ \sigma$ gilt $x_{\pi(i)} = x_{\sigma(i)}$ für $i \in I$, da x eine I-Permutation in X ist also auch $\pi(i) = \sigma(i)$ für $i \in I$ und damit $\pi = \sigma$. Folglich ist $\mathrm{S}_I \to [x]$, $\pi \mapsto x \circ \pi$ auch injektiv und somit insgesamt bijektiv. □

(18.60) Beispiel. Wir haben folgende Bijektion.

$$\begin{aligned}
\mathrm{S}_3 &\to [2,3,5],\\
\left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right) &\mapsto (2,3,5),\\
\left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right) &\mapsto (3,2,5),\\
\left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right) &\mapsto (5,3,2),\\
\left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right) &\mapsto (2,5,3),\\
\left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right) &\mapsto (3,5,2),\\
\left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right) &\mapsto (5,2,3).
\end{aligned}$$

(18.61) Korollar. Es seien $k \in \mathbb{N}_0$, eine Menge X und eine k-elementige Menge I gegeben. Für jede I-Kombination C in X gilt

$$|C| = k!.$$

Beweis. Es sei eine I-Kombination C in X gegeben. Dann gibt es eine I-Permutation x in X mit $C = [x]$ und nach Bemerkung (18.59) gibt es eine Bijektion $\mathrm{S}_I \to [x]$. Insbesondere ist C als Menge endlich und nach Korollar (18.32) gilt

$$|C| = |[x]| = |\mathrm{S}_I| = k!.$$ □

(18.62) Korollar. Es seien $n, k \in \mathbb{N}_0$, eine n-elementige Menge X und eine k-elementige Menge I gegeben. Dann gilt

$$|\mathrm{Comb}_I(X)| = \binom{n}{k}.$$

Beweis. Da $\mathrm{Comb}_I(X) = \mathrm{Perm}_I(X)/\!\sim$ nach dem Hauptsatz über Äquivalenzrelationen (5.20) eine Partition von $\mathrm{Perm}_I(X)$ ist, gilt

$$\mathrm{Perm}_I(X) = \dot{\bigcup_{C \in \mathrm{Comb}_I(X)}} C.$$

Die Summenregel (18.4) und Korollar (18.61) liefern

$$|\mathrm{Perm}_I(X)| = |\dot{\bigcup_{C \in \mathrm{Comb}_I(X)}} C| = \sum_{C \in \mathrm{Comb}_I(X)} |C| = \sum_{C \in \mathrm{Comb}_I(X)} k! = |\mathrm{Comb}_I(X)|\, k!.$$

Nach Korollar (18.31) folgt schließlich

$$|\mathrm{Comb}_I(X)| = \frac{|\mathrm{Perm}_I(X)|}{k!} = \frac{\prod_{i \in [1,k]}(n-i+1)}{k!} = \binom{n}{k}.$$ □

(18.63) Beispiel.

(a) Es ist

$$|\mathrm{Comb}_4([1,9])| = 126.$$

(b) Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$|\mathrm{Comb}_3(\{a,b,c,d\})| = 4.$$

Beweis.

(a) Nach Korollar (18.62) ist

$$|\mathrm{Comb}_4([1,9])| = \binom{9}{4} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3 \cdot 4} = 126.$$

(b) Nach Korollar (18.62) und Korollar (17.12) ist

$$|\mathrm{Comb}_3(\{a,b,c,d\})| = \binom{4}{3} = \binom{4}{1} = 4.$$ □

Korollar (18.62) liefert kombinatorische Beweise für Korollar (17.8)(b) und Bemerkung (17.6):

Alternativer Beweis von Korollar (17.8)(b). Nach Korollar (18.62) gilt für $n, k \in \mathbb{N}_0$ stets

$$\binom{n}{k} = |\mathrm{Comb}_k([1,n])| \in \mathbb{N}_0.$$ □

Alternativer Beweis von Bemerkung (17.6). Nach dem Schubfachprinzip (18.12) gilt für $n \in \mathbb{N}_0$, $k \in \mathbb{N}_0 \setminus [0,n]$ stets $\mathrm{Perm}_k([1,n]) = \emptyset$ und damit $\mathrm{Comb}_k([1,n]) = \emptyset$, nach Korollar (18.62) also

$$\binom{n}{k} = |\mathrm{Comb}_k([1,n])| = 0.$$ □

Wir kommen zu unseren Beispielen aus dem täglichen Leben zurück:

(18.64) Anwendungsbeispiel.

(a) Ziehungen der Lottozahlen seien als 6-Kombinationen in $[1,49]$ modelliert. Nach Korollar (18.62) ist die Anzahl aller möglichen Ziehungen der Lottozahlen gleich

$$|\mathrm{Comb}_6([1,49])| = \binom{49}{6} = 13\,983\,816.$$

(b) Skathände seien als 10-Kombinationen in $\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \times \{7,8,9,10,\mathrm{B},\mathrm{D},\mathrm{K},\mathrm{A}\}$ modelliert. Nach Korollar (18.62) und Anwendungsbeispiel (18.9) ist die Anzahl aller möglichen Skathände gleich

$$|\mathrm{Comb}_{10}(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \times \{7,8,9,10,\mathrm{B},\mathrm{D},\mathrm{K},\mathrm{A}\})| = \binom{4 \cdot 8}{10} = \binom{32}{10} = 64\,512\,240.$$

(c) Die Gesamtheit der Fußball-Bundesliga-Absteiger der Saison 2016/17 sei als 2-Kombination (Mannschaft auf Relegationsplatz steigt nicht ab) oder 3-Kombination (Mannschaft auf Relegationsplatz steigt ab) in

$$\begin{aligned} M = \{&\text{FC Augsburg, Hertha BSC, SV Werder Bremen, SV Darmstadt 98, Borussia Dortmund,}\\ &\text{Eintracht Frankfurt, SC Freiburg, FC Ingolstadt 04, FC Schalke 04, Hamburger SV,}\\ &\text{TSG 1899 Hoffenheim, 1. FC Köln, RB Leipzig, Bayer 04 Leverkusen, 1. FSV Mainz 05,}\\ &\text{Borussia Mönchengladbach, FC Bayern München, VfL Wolfsburg}\} \end{aligned}$$

modelliert. Nach der Summenregel (18.4) und Korollar (18.62) ist die Anzahl aller möglichen Absteigergesamtheiten gleich

$$|\mathrm{Comb}_2(M) \mathbin{\dot\cup} \mathrm{Comb}_3(M)| = |\mathrm{Comb}_2(M)| + |\mathrm{Comb}_3(M)| = \binom{18}{2} + \binom{18}{3} = 969.$$

(d) Verteilungen von vier gleich aussehenden Kugeln auf zehn durchnummerierte Boxen derart, dass in jeder Box höchstens eine Kugel liegt, seien als 4-Kombinationen in $[1,10]$ modelliert. Nach Korollar (18.62) ist die Anzahl aller solchen möglichen Verteilungen gleich

$$|\mathrm{Comb}_4([1,10])| = \binom{10}{4} = 210.$$

Die Formeln für die Anzahlen von Multikombinationen und Kombinationen legen die Vermutung nahe, dass es eine Verbindung zwischen Multikombinationen und Kombinationen gibt. Diese werden wir in Korollar (18.116) studieren.

Auswahlmodelle über mehreren Indexmengen

Die bisher betrachteten Modelle über Auswahlen lassen sich durch Verwendung der (äußeren) disjunkten Vereinigung, siehe Definition (2.48)(b), als Indexmenge zu Modellen über mehreren Mengen verallgemeinern. Der interessanteste Fall ist der einer Kombination über mehreren Mengen. Wir überlassen die Beweise dem Leser.

(18.65) Definition (Variation)**.** Es seien eine Menge X und $r \in \mathbb{N}_0$ gegeben.

(a) Es sei ein r-Tupel von Mengen $I = (I_1, \ldots, I_r)$ gegeben. Die *Menge der Variationen* in X über I ist definiert als

$$\mathrm{Var}_I(X) := \mathrm{Var}_{\bigsqcup I}(X).$$

Ein Element von $\mathrm{Var}_I(X)$ wird eine *Variation* in X über I (oder I*-Variation* in X oder I*-Variation mit Wiederholung* in X) genannt.

Für eine Variation $x = (x_{i_j,j})_{(i_j,j)\in\bigsqcup I}$ in X über I schreiben wir auch

$$x_{-,j} := (x_{i_j,j})_{i_j \in I_j}$$

für $j \in [1, r]$ sowie

$$(x_{-,1}, \ldots, x_{-,r}) = ((x_{i_1,1})_{i_1\in I_1}, \ldots, (x_{i_r,r})_{i_r\in I_r}) := x.$$

(b) Es sei $k \in \mathbb{N}_0^r$ gegeben. Die *Menge der k-Variationen* in X ist definiert als

$$\mathrm{Var}_k(X) = \mathrm{Var}_{k_1,\ldots,k_r}(X) := \mathrm{Var}_{([1,k_1],\ldots,[1,k_r])}(X).$$

Ein Element von $\mathrm{Var}_k(X)$ wird eine k*-Variation* (oder k*-Variation mit Wiederholung*) in X genannt.

Die in Definition (18.65)(a) festgelegte Notation entspricht (weitgehend) einer Identifikation entlang der bijektiven Abbildung

$$\mathrm{Var}_I(X) \to \mathrm{Var}_{I_1}(X) \times \ldots \times \mathrm{Var}_{I_r}(X),\ x \mapsto ((x_{i_1,1})_{i_1\in I_1}, \ldots, (x_{i_r,r})_{i_r\in I_r}).$$

(18.66) Beispiel.

(a) Es ist $((5,3),(9,7))$ eine $(2,2)$-Variation in $[1,9]$.

(b) Es ist $((5,3),(5,7))$ eine $(2,2)$-Variation in $[1,9]$.

(18.67) Beispiel. Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$\begin{aligned}\mathrm{Var}_{2,1}(\{a,b,c,d\}) = \{&((a,a),(a)),((a,a),(b)),((a,a),(c)),((a,a),(d)),((a,b),(a)),((a,b),(b)),((a,b),(c)),\\ &((a,b),(d)),((a,c),(a)),((a,c),(b)),((a,c),(c)),((a,c),(d)),((a,d),(a)),((a,d),(b)),\\ &((a,d),(c)),((a,d),(d)),((b,a),(a)),((b,a),(b)),((b,a),(c)),((b,a),(d)),((b,b),(a)),\\ &((b,b),(b)),((b,b),(c)),((b,b),(d)),((b,c),(a)),((b,c),(b)),((b,c),(c)),((b,c),(d)),\\ &((b,d),(a)),((b,d),(b)),((b,d),(c)),((b,d),(d)),((c,a),(a)),((c,a),(b)),((c,a),(c)),\\ &((c,a),(d)),((c,b),(a)),((c,b),(b)),((c,b),(c)),((c,b),(d)),((c,c),(a)),((c,c),(b)),\\ &((c,c),(c)),((c,c),(d)),((c,d),(a)),((c,d),(b)),((c,d),(c)),((c,d),(d)),((d,a),(a)),\\ &((d,a),(b)),((d,a),(c)),((d,a),(d)),((d,b),(a)),((d,b),(b)),((d,b),(c)),((d,b),(d)),\\ &((d,c),(a)),((d,c),(b)),((d,c),(c)),((d,c),(d)),((d,d),(a)),((d,d),(b)),((d,d),(c)),\\ &((d,d),(d))\}.\end{aligned}$$

(18.68) Anwendungsbeispiel. Ein Geheimzahlset für Mobiltelefone bestehend aus einer vierstelligen PIN und einer achtstelligen PUK lässt sich als $(4,8)$-Variation in $[0,9]$ auffassen.

(18.69) Bemerkung. Es seien $n, r \in \mathbb{N}_0$, $k \in \mathbb{N}_0^r$, eine n-elementige Menge X und ein r-Tupel endlicher Mengen $I = (I_1, \ldots, I_r)$ mit $|I_j| = k_j$ für $j \in [1, r]$ gegeben. Dann gilt

$$|\mathrm{Var}_I(X)| = n^{\sum_{j\in[1,r]} k_j}.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(18.70) Beispiel.

(a) Es ist

$$|\mathrm{Var}_{2,2}([1,9])| = 6561.$$

(b) Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$|\mathrm{Var}_{2,1}(\{a,b,c,d\})| = 64.$$

Beweis.

(a) Nach Bemerkung (18.69) ist

$$|\mathrm{Var}_{2,2}([1,9])| = 9^{2+2} = 9^4 = 6561.$$

(b) Nach Bemerkung (18.69) ist

$$|\mathrm{Var}_{2,1}(\{a,b,c,d\})| = 4^{2+1} = 4^3 = 64.$$ □

(18.71) Anwendungsbeispiel. Geheimzahlsets für Mobiltelefone bestehend aus einer vierstelligen PIN und einer achtstelligen PUK seien als $(4,8)$-Variationen in $[0,9]$ modelliert. Nach Bemerkung (18.69) ist die Anzahl aller solchen Geheimzahlsets gleich

$$|\mathrm{Var}_{4,8}([0,9])| = 10^{4+8} = 10^{12} = 1\,000\,000\,000\,000.$$

(18.72) Definition (Permutation)**.** Es seien eine Menge X und $r \in \mathbb{N}_0$ gegeben.

(a) Es sei ein r-Tupel von Mengen $I = (I_1, \ldots, I_r)$ gegeben. Die *Menge der Permutationen* in X über I ist definiert als

$$\mathrm{Perm}_I(X) := \mathrm{Perm}_{\bigsqcup I}(X).$$

Ein Element von $\mathrm{Perm}_I(X)$ wird eine *Permutation* in X über I (oder *I-Permutation* in X oder *I-Variation ohne Wiederholung* in X) genannt.

(b) Es sei $k \in \mathbb{N}_0^r$ gegeben. Die *Menge der k-Permutationen* in X ist definiert als

$$\mathrm{Perm}_k(X) = \mathrm{Perm}_{k_1,\ldots,k_r}(X) := \mathrm{Perm}_{([1,k_1],\ldots,[1,k_r])}(X).$$

Ein Element von $\mathrm{Perm}_k(X)$ wird eine *k-Permutation* (oder *k-Variation ohne Wiederholung*) in X genannt.

(18.73) Beispiel.

(a) Es ist $((5,3),(9,7))$ eine $(2,2)$-Permutation in $[1,9]$.

(b) Die $(2,2)$-Variation $((5,3),(5,7))$ in $[1,9]$ ist keine $(2,2)$-Permutation in $[1,9]$.

(18.74) Beispiel. Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$\begin{aligned}\mathrm{Perm}_{2,1}(\{a,b,c,d\}) = \{&((a,b),(c)),((a,b),(d)),((a,c),(b)),((a,c),(d)),((a,d),(b)),((a,d),(c)),\\ &((b,a),(c)),((b,a),(d)),((b,c),(a)),((b,c),(d)),((b,d),(a)),((b,d),(c)),\\ &((c,a),(b)),((c,a),(d)),((c,b),(a)),((c,b),(d)),((c,d),(a)),((c,d),(b)),\\ &((d,a),(b)),((d,a),(c)),((d,b),(a)),((d,b),(c)),((d,c),(a)),((d,c),(b))\}.\end{aligned}$$

(18.75) Anwendungsbeispiel. Die Besucher eines Kindergeburtstags seien als Elemente einer Menge K modelliert. Eine Aufstellung für eine Spielrunde Ruck Zuck lässt sich als $(5,5)$-Permutation in K auffassen.

(18.76) Bemerkung. Es seien $n, r \in \mathbb{N}_0$, $k \in \mathbb{N}_0^r$, eine n-elementige Menge X und ein r-Tupel endlicher Mengen $I = (I_1, \ldots, I_r)$ mit $|I_j| = k_j$ für $j \in [1, r]$ gegeben. Dann gilt

$$|\mathrm{Perm}_I(X)| = \prod_{i \in [1, \sum_{j \in [1,r]} k_j]} (n - i + 1).$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(18.77) Beispiel.

(a) Es ist

$$|\mathrm{Perm}_{2,2}([1, 9])| = 3024.$$

(b) Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$|\mathrm{Perm}_{2,1}(\{a, b, c, d\})| = 24.$$

Beweis.

(a) Nach Bemerkung (18.76) ist

$$|\mathrm{Perm}_{2,2}([1, 9])| = \prod_{i \in [1,2+2]} (9 - i + 1) = \prod_{i \in [1,4]} (9 - i + 1) = 9 \cdot 8 \cdot 7 \cdot 6 = 3024.$$

(b) Nach Bemerkung (18.76) ist

$$|\mathrm{Perm}_{2,1}(\{a, b, c, d\})| = \prod_{i \in [1,2+1]} (4 - i + 1) = \prod_{i \in [1,3]} (4 - i + 1) = 4 \cdot 3 \cdot 2 = 24.$$ □

(18.78) Anwendungsbeispiel. Die 13 Besucher eines Kindergeburtstags seien als Elemente einer 13-elementigen Menge K modelliert. Aufstellungen für eine Spielrunde Ruck Zuck seien als $(5, 5)$-Permutationen in K modelliert. Nach Bemerkung (18.76) ist die Anzahl aller möglichen Aufstellungen gleich

$$|\mathrm{Perm}_{5,5}(K)| = \prod_{i \in [1,5+5]} (13 - i + 1) = 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 = 1\,037\,836\,800.$$

(18.79) Definition (Eintragsgleichheit)**.** Es seien eine Menge X, $r \in \mathbb{N}_0$ und ein r-Tupel von Mengen $I = (I_1, \ldots, I_r)$ gegeben. Für $x, y \in \mathrm{Var}_I(X)$ gelte genau dann $x \sim y$, wenn $x_{-,j} \sim y_{-,j}$ für $j \in [1, r]$ gilt. Die Relation $\sim$ wird *Eintragsgleichheit* von Variationen in X über I genannt.

(18.80) Bemerkung. Es seien eine Menge X, $r \in \mathbb{N}_0$ und ein r-Tupel von Mengen $I = (I_1, \ldots, I_r)$ gegeben. Dann ist $\sim$ eine Äquivalenzrelation auf $\mathrm{Var}_I(X)$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(18.81) Definition (Multikombination)**.** Es seien eine Menge X und $r \in \mathbb{N}_0$ gegeben.

(a) Es sei ein r-Tupel von Mengen $I = (I_1, \ldots, I_r)$ gegeben. Die *Menge der Multikombinationen* in X über I ist definiert als

$$\mathrm{MComb}_I(X) := \mathrm{Var}_I(X)/\sim.$$

Ein Element von $\mathrm{MComb}_I(X)$ wird eine *Multikombination* in X über I (oder *I-Multikombination* in X oder *I-Kombination mit Wiederholung* in X) genannt.

Für eine Variation $x = (x_{-,1}, \ldots, x_{-,r}) = ((x_{i_1,1})_{i_1 \in I_1}, \ldots, (x_{i_r,r})_{i_r \in I_r})$ in X über I schreiben wir auch

$$([x_{-,1}], \ldots, [x_{-,r}]) = ([x_{i_1,1}]_{i_1 \in I_1}, \ldots, [x_{i_r,r}]_{i_r \in I_r}) := [x].$$

(b) Es sei $k \in \mathbb{N}_0^r$ gegeben. Die *Menge der k-Multikombinationen* in X ist definiert als

$$\mathrm{MComb}_k(X) = \mathrm{MComb}_{k_1,\ldots,k_r}(X) := \mathrm{MComb}_{([1,k_1],\ldots,[1,k_r])}(X).$$

Ein Element von $\mathrm{MComb}_k(X)$ wird eine *k-Multikombination* (oder *k-Kombination mit Wiederholung*) in X genannt.

Für eine k-Variation $x = ((x_{1,1},\ldots,x_{k_1,1}),\ldots,(x_{1,r},\ldots,x_{k_r,r}))$ in X schreiben wir auch

$$([x_{1,1},\ldots,x_{k_1,1}],\ldots,[x_{1,r},\ldots,x_{k_r,r}]) := [x].$$

(18.82) Beispiel.

(a) Es ist $([5,3],[9,7]) = ([3,5],[7,9])$ eine $(2,2)$-Multikombination in $[1,9]$.

(b) Es ist $([5,3],[5,7]) = ([3,5],[5,7])$ eine $(2,2)$-Multikombination in $[1,9]$.

(18.83) Beispiel. Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$\begin{aligned}\mathrm{MComb}_{2,1}(\{a,b,c,d\}) = \{&([a,a],[a]),([a,a],[b]),([a,a],[c]),([a,a],[d]),([a,b],[a]),([a,b],[b]),([a,b],[c]),\\ &([a,b],[d]),([a,c],[a]),([a,c],[b]),([a,c],[c]),([a,c],[d]),([a,d],[a]),([a,d],[b]),\\ &([a,d],[c]),([a,d],[d]),([b,b],[a]),([b,b],[b]),([b,b],[c]),([b,b],[d]),([b,c],[a]),\\ &([b,c],[b]),([b,c],[c]),([b,c],[d]),([b,d],[a]),([b,d],[b]),([b,d],[c]),([b,d],[d]),\\ &([c,c],[a]),([c,c],[b]),([c,c],[c]),([c,c],[d]),([c,d],[a]),([c,d],[b]),([c,d],[c]),\\ &([c,d],[d]),([d,d],[a]),([d,d],[b]),([d,d],[c]),([d,d],[d])\}.\end{aligned}$$

(18.84) Anwendungsbeispiel. Die angebotenen Eissorten einer Eisdiele seien als Elemente einer Menge E modelliert. Eine Auswahl von zwei Eisbechern bestückt mit drei bzw. zwei Kugeln lässt sich als $(3,2)$-Multikombination in E auffassen.

(18.85) Bemerkung. Es seien $n, r \in \mathbb{N}_0$, $k \in \mathbb{N}_0^r$, eine n-elementige Menge X und ein r-Tupel endlicher Mengen $I = (I_1,\ldots,I_r)$ mit $|I_j| = k_j$ für $j \in [1,r]$ gegeben. Dann gilt

$$|\mathrm{MComb}_I(X)| = \prod_{j\in[1,r]} \binom{k_j+n-1}{k_j}.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(18.86) Beispiel.

(a) Es ist

$$|\mathrm{MComb}_{2,2}([1,9])| = 2025.$$

(b) Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$|\mathrm{MComb}_{2,1}(\{a,b,c,d\})| = 40.$$

Beweis.

(a) Nach Bemerkung (18.85) ist

$$|\mathrm{MComb}_{2,2}([1,9])| = \binom{2+9-1}{2}\cdot\binom{2+9-1}{2} = \binom{10}{2}\cdot\binom{10}{2} = \frac{10\cdot 9}{1\cdot 2}\cdot\frac{10\cdot 9}{1\cdot 2} = 2025.$$

(b) Nach Bemerkung (18.85) ist

$$|\mathrm{MComb}_{2,1}(\{a,b,c,d\})| = \binom{2+4-1}{2}\cdot\binom{1+4-1}{1} = \binom{5}{2}\cdot\binom{4}{1} = \frac{5\cdot 4}{1\cdot 2}\cdot\frac{4}{1} = 40.$$ □

(18.87) Anwendungsbeispiel. Die 20 angebotenen Eissorten einer Eisdiele seien als Elemente einer 20-elementigen Menge E modelliert. Auswahlen von zwei Eisbechern bestückt mit drei bzw. zwei Kugeln seien als $(3,2)$-Multikombination in E modelliert. Nach Bemerkung (18.85) ist die Anzahl aller solchen Auswahlen gleich

$$|\mathrm{MComb}_{3,2}(E)| = \binom{3+20-1}{3} \cdot \binom{2+20-1}{2} = \binom{22}{3} \cdot \binom{21}{2} = \frac{22 \cdot 21 \cdot 20}{1 \cdot 2 \cdot 3} \cdot \frac{21 \cdot 20}{1 \cdot 2} = 323\,400.$$

(18.88) Bemerkung. Es seien eine Menge X, $r \in \mathbb{N}_0$, ein r-Tupel von Mengen $I = (I_1, \ldots, I_r)$ und I-Variationen x und y in X mit $x \sim y$ gegeben. Genau dann ist x eine I-Permutation in X, wenn y eine I-Permutation in X ist.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(18.89) Definition (Kombination)**.** Es seien eine Menge X und $r \in \mathbb{N}_0$ gegeben.

(a) Es sei ein r-Tupel von Mengen $I = (I_1, \ldots, I_r)$ gegeben. Die *Menge der Kombinationen* in X über I ist definiert als

$$\mathrm{Comb}_I(X) := \mathrm{Perm}_I(X)/\sim.$$

Ein Element von $\mathrm{Comb}_I(X)$ wird eine *Kombination* in X über I (oder *I-Kombination* in X oder *I-Kombination ohne Wiederholung* in X) genannt.

(b) Es sei $k \in \mathbb{N}_0^r$ gegeben. Die *Menge der k-Kombinationen* in X ist definiert als

$$\mathrm{Comb}_k(X) = \mathrm{Comb}_{k_1,\ldots,k_r}(X) := \mathrm{Comb}_{([1,k_1],\ldots,[1,k_r])}(X).$$

Ein Element von $\mathrm{Comb}_k(X)$ wird eine *k-Kombination* (oder *k-Kombination ohne Wiederholung*) in X genannt.

(18.90) Beispiel.

(a) Es ist $([5,3],[9,7]) = ([3,5],[7,9])$ eine $(2,2)$-Kombination in $[1,9]$.

(b) Die $(2,2)$-Multikombination $([5,3],[5,7]) = ([3,5],[5,7])$ in $[1,9]$ ist keine $(2,2)$-Kombination in $[1,9]$.

(18.91) Beispiel. Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$\begin{aligned}\mathrm{Comb}_{2,1}(\{a,b,c,d\}) = \{&([a,b],[c]),([a,b],[d]),([a,c],[b]),([a,c],[d]),([a,d],[b]),([a,d],[c]),([b,c],[a]),\\ &([b,c],[d]),([b,d],[a]),([b,d],[c]),([c,d],[a]),([c,d],[b])\}.\end{aligned}$$

(18.92) Anwendungsbeispiel. Eine Kartenverteilung beim Skat lässt sich als $(10,10,10)$-Kombination in $\{\heartsuit,\diamondsuit,\spadesuit,\clubsuit\} \times \{7,8,9,10,\mathrm{B},\mathrm{D},\mathrm{K},\mathrm{A}\}$ auffassen.

(18.93) Bemerkung. Es seien eine Menge X, $r \in \mathbb{N}_0$, ein r-Tupel von Mengen $I = (I_1, \ldots, I_r)$ sowie eine I-Permutation x in X gegeben. Dann ist

$$\mathrm{S}_{I_1} \times \ldots \times \mathrm{S}_{I_r} \to [x],\ (\pi_1, \ldots, \pi_r) \mapsto (x_{-,j} \circ \pi_j)_{j \in J}$$

eine Bijektion.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(18.94) Korollar. Es seien eine Menge X, $r \in \mathbb{N}_0$ und ein r-Tupel endlicher Mengen $I = (I_1, \ldots, I_r)$ gegeben. Für jede I-Kombination C in X gilt

$$|C| = \prod_{j \in [1,r]} |I_j|!.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(18.95) Korollar. Es seien $n, r \in \mathbb{N}_0$, $k \in \mathbb{N}_0^r$, eine n-elementige Menge X und ein r-Tupel endlicher Mengen $I = (I_1, \ldots, I_r)$ mit $|I_j| = k_j$ für $j \in [1, r]$ gegeben. Dann gilt

$$|\mathrm{Comb}_I(X)| = \binom{n}{k}.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(18.96) Beispiel.

(a) Es ist

$$|\mathrm{Comb}_{2,2}([1,9])| = 756.$$

(b) Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$|\mathrm{Comb}_{2,1}(\{a,b,c,d\})| = 12.$$

Beweis.

(a) Nach Korollar (18.62) ist

$$|\mathrm{Comb}_{2,2}([1,9])| = \binom{9}{2,2} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 1 \cdot 2} = 756.$$

(b) Nach Korollar (18.62) ist

$$|\mathrm{Comb}_{2,1}(\{a,b,c,d\})| = \binom{4}{2,1} = \frac{4 \cdot 3 \cdot 2}{1 \cdot 2 \cdot 1} = 12.$$ □

(18.97) Anwendungsbeispiel. Verteilungen beim Kartenspiel Skat seien als $(10,10,10)$-Kombinationen in $\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \times \{7,8,9,10,\mathrm{B},\mathrm{D},\mathrm{K},\mathrm{A}\}$ modelliert. Nach Korollar (18.95) ist die Anzahl aller möglichen Verteilungen gleich

$$\begin{aligned}|\mathrm{Comb}_{10,10,10}(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \times \{7,8,9,10,\mathrm{B},\mathrm{D},\mathrm{K},\mathrm{A}\})| &= \binom{32}{10,10,10} = \frac{\prod_{i \in [1,10+10+10]}(32-i+1)}{10! \cdot 10! \cdot 10!} \\ &= 2\,753\,294\,408\,504\,640.\end{aligned}$$

Repräsentanten von Multikombinationen

Als Anwendung unserer Ergebnisse über Kombinationen über mehreren Mengen bestimmen wir die Anzahl der Repräsentanten einer Multikombination.

(18.98) Beispiel. Die 4-Multikombination $[3,5,5,7]$ in $[1,9]$ ist gegeben durch

$$\begin{aligned}[3,5,5,7] = \{&(3,5,5,7),(3,5,7,5),(3,7,5,5),(5,3,5,7),(5,3,7,5),(5,5,3,7),(5,5,7,3),(5,7,3,5),\\ &(5,7,5,3),(7,3,5,5),(7,5,3,5),(7,5,5,3)\}\end{aligned}$$

(18.99) Anwendungsbeispiel. Das Wort `MISSISSIPPI` sei als 11-Variation x in $\{\mathtt{I},\mathtt{M},\mathtt{P},\mathtt{S}\}$ modelliert. Ein String, welcher durch Umordnung der Zeichen des Worts `MISSISSIPPI` gebildet wird, lässt sich als Element der 11-Multikombination $[x]$ in $\{\mathtt{I},\mathtt{M},\mathtt{P},\mathtt{S}\}$ auffassen.

(18.100) Proposition. Es seien $n, k \in \mathbb{N}_0$ und eine k-Multikombination C in $[1,n]$ gegeben. Dann ist

$$F\colon \mathrm{Comb}_{\mu_C}([1,k]) \to C$$

gegeben durch

$$F([i])_{i_{j,y}} = y$$

für $j \in [1, (\mu_C)_y]$, $y \in [1,n]$, $i \in \mathrm{Perm}_{\mu_C}([1,k])$, eine wohldefinierte Bijektion.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(18.101) Beispiel. Wir haben folgende Bijektion.

$$\begin{aligned}
&\mathrm{Comb}_{1,0,2,1}([1,4]) \to [1,3,3,4],\\
&\quad([1],[\,],[2,3],[4]) \mapsto (1,3,3,4),\\
&\quad([1],[\,],[2,4],[3]) \mapsto (1,3,4,3),\\
&\quad([1],[\,],[3,4],[2]) \mapsto (1,4,3,3),\\
&\quad([2],[\,],[1,3],[4]) \mapsto (3,1,3,4),\\
&\quad([2],[\,],[1,4],[3]) \mapsto (3,1,4,3),\\
&\quad([2],[\,],[3,4],[1]) \mapsto (4,1,3,3),\\
&\quad([3],[\,],[1,2],[4]) \mapsto (3,3,1,4),\\
&\quad([3],[\,],[1,4],[2]) \mapsto (3,4,1,3),\\
&\quad([3],[\,],[2,4],[1]) \mapsto (4,3,1,3),\\
&\quad([4],[\,],[1,2],[3]) \mapsto (3,3,4,1),\\
&\quad([4],[\,],[1,3],[2]) \mapsto (3,4,3,1),\\
&\quad([4],[\,],[2,3],[1]) \mapsto (4,3,3,1).
\end{aligned}$$

(18.102) Korollar. Es seien $n, k \in \mathbb{N}_0$, eine n-elementige Menge X, eine k-elementige Menge I und eine Abzählung e von X gegeben. Für jede I-Multikombination C in X über I gilt

$$|C| = \binom{k}{\mu_C \circ e}.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(18.103) Beispiel. Für die 4-Multikombination $[3,5,5,7]$ in $[1,9]$ gilt

$$|[3,5,5,7]| = 12.$$

Beweis. Das Häufigkeitstupel der 4-Multikombination $[3,5,5,7]$ in $[1,9]$ ist gegeben durch

$$\mu_{[3,5,5,7]} = (0,0,1,0,2,0,1,0,0).$$

Nach Korollar (18.102) und Proposition (17.22)(b) ist daher

$$|[3,5,5,7]| = \binom{4}{0,0,1,0,2,0,1,0,0} = \frac{4!}{0!\cdot 0!\cdot 1!\cdot 0!\cdot 2!\cdot 0!\cdot 1!\cdot 0!\cdot 0!} = 12.$$ □

(18.104) Anwendungsbeispiel. Das Wort `MISSISSIPPI` sei als 11-Variation x in $\{\mathtt{I},\mathtt{M},\mathtt{P},\mathtt{S}\}$ modelliert. Strings, welche durch Umordnung der Zeichen des Worts `MISSISSIPPI` gebildet werden können, seien als Elemente der 11-Multikombination $[x]$ in $\{\mathtt{I},\mathtt{M},\mathtt{P},\mathtt{S}\}$ modelliert. Die Häufigkeitsfamilie von $[x]$ ist gegeben durch

$$\begin{aligned}
(\mu_{[x]})_{\mathtt{I}} &= 4,\\
(\mu_{[x]})_{\mathtt{M}} &= 1,\\
(\mu_{[x]})_{\mathtt{P}} &= 2,\\
(\mu_{[x]})_{\mathtt{S}} &= 4.
\end{aligned}$$

Nach Korollar (18.102) ist die Anzahl aller Strings, welche durch Umordnung der Zeichen des Worts `MISSISSIPPI` gebildet werden können, gleich

$$|[x]| = \binom{11}{4,1,2,4} = \frac{11\cdot 10\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1}{1\cdot 2\cdot 3\cdot 4\cdot 1\cdot 1\cdot 2\cdot 1\cdot 2\cdot 3\cdot 4} = 34\,650.$$

Teilmengen

Als nächstes zählen wir Teilmengen mit einer vorgegebenen Anzahl an Elementen. Hierzu zeigen wir, dass solche Teilmengen gerade Kombinationen entsprechen. Multikombinationen können dementsprechend als „Mengen mit Wiederholungen“ aufgefasst werden. Die Häufigkeitsfunktion einer Multikombination, siehe Definition (18.44), entspricht dann gerade der Verallgemeinerung der Indikatorfunktion, siehe Definition (3.35).

(18.105) Definition (k-Teilmenge)**.** Es seien $k \in \mathbb{N}_0$ und eine Menge X gegeben. Die *Menge der k-Teilmengen* von X ist definiert als

$$\mathrm{Pot}_k(X) := \{U \in \mathrm{Pot}(X) \mid U \text{ ist endlich mit } |U| = k\}.$$

Ein Element von $\mathrm{Pot}_k(X)$ wird eine *k-Teilmenge* von X genannt.

(18.106) Beispiel. Es ist $\{3, 5, 7, 9\}$ eine 4-Teilmenge von $[1, 9]$.

(18.107) Beispiel. Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$\mathrm{Pot}_3(\{a, b, c, d\}) = \{\{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}\}.$$

(18.108) Proposition. Es seien $k \in \mathbb{N}_0$ und eine Menge X gegeben. Dann ist

$$\mathrm{Comb}_k(X) \to \mathrm{Pot}_k(X),\ [x] \mapsto \{x_i \mid i \in [1, k]\}$$

eine wohldefinierte Bijektion.

Beweis. Wir betrachten die Abbildung

$$f\colon \mathrm{Perm}_k(X) \to \mathrm{Pot}(X),\ x \mapsto \{x_i \mid i \in [1, k]\}.$$

Nach dem Homomorphiesatz für Mengen (5.15) induziert f eine wohldefinierte Injektion

$$\bar{f}\colon \mathrm{Perm}_k(X)/{=_f} \to \mathrm{Pot}(X)$$

mit $f = \bar{f} \circ \mathrm{quo}$, gegeben durch $\bar{f}([x]) = f(x) = \{x_i \mid i \in [1, k]\}$ für $x \in \mathrm{Perm}_k(X)$, und es ist $\mathrm{Im}\,\bar{f} = \mathrm{Im}\, f$.
Um zu zeigen, dass $=_f\ = \sim$ ist, seien $x, x' \in \mathrm{Perm}_k(X)$ gegeben. Genau dann gilt $x =_f x'$ in $\mathrm{Perm}_k(X)$, wenn $f(x) = f(x')$ in $\mathrm{Pot}(X)$ ist, d.h. wenn $\{x_i \mid i \in [1, k]\} = \{x'_i \mid i \in [1, k]\}$ gilt. Da x und x' jeweils k-Permutationen sind, ist dies äquivalent zur Existenz eines $\pi \in \mathrm{S}_k$ mit $x' = x \circ \pi$, d.h. zu $x \sim x'$. Somit gilt in der Tat $=_f\ = \sim$ und folglich $\mathrm{Perm}_k(X)/{=_f} = \mathrm{Perm}_k(X)/{\sim} = \mathrm{Comb}_k(X)$.
Ferner ist

$$\begin{aligned}\mathrm{Im}\,\bar{f} = \mathrm{Im}\, f &= \{U \in \mathrm{Pot}(X) \mid \text{es gibt ein } x \in \mathrm{Perm}_k(X) \text{ mit } U = f(x)\} \\ &= \{U \in \mathrm{Pot}(X) \mid \text{es gibt ein } x \in \mathrm{Perm}_k(X) \text{ mit } U = \{x_i \mid i \in [1, k]\}\} = \mathrm{Pot}_k(X).\end{aligned}$$

Insgesamt ist

$$\bar{f}|^{\mathrm{Im}\,\bar{f}}\colon \mathrm{Comb}_k(X) \to \mathrm{Pot}_k(X),\ [x] \mapsto \{x_i \mid i \in [1, k]\}$$

eine Bijektion. □

(18.109) Korollar. Es seien $n, k \in \mathbb{N}_0$ und eine n-elementige Menge X gegeben. Dann ist

$$|\mathrm{Pot}_k(X)| = \binom{n}{k}.$$

Beweis. Nach Proposition (18.108) gibt es eine Bijektion $\mathrm{Comb}_k(X) \to \mathrm{Pot}_k(X)$, so dass nach der Gleichheitsregel (18.1) und Korollar (18.62) bereits

$$|\mathrm{Pot}_k(X)| = |\mathrm{Comb}_k(X)| = \binom{n}{k}$$

folgt. □

(18.110) Beispiel.

(a) Es ist

$$|\mathrm{Pot}_4([1,9])| = 126.$$

(b) Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$|\mathrm{Pot}_3(\{a,b,c,d\})| = 4.$$

Beweis.

(a) Nach Korollar (18.109) ist

$$|\mathrm{Pot}_4([1,9])| = \binom{9}{4} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3 \cdot 4} = 126.$$

(b) Nach Korollar (18.109) und Korollar (17.12) ist

$$|\mathrm{Pot}_3(\{a,b,c,d\})| = \binom{4}{3} = \binom{4}{1} = 4.$$ □

Wir erhalten nochmals alternative kombinatorische Beweise für Aussagen über Binomialkoeffizienten:

Alternativer Beweis von Korollar (17.8)(b). Nach Korollar (18.109) gilt für $n, k \in \mathbb{N}_0$ stets

$$\binom{n}{k} = |\mathrm{Pot}_k([1,n])| \in \mathbb{N}_0.$$ □

Alternativer Beweis von Bemerkung (17.6). Nach Korollar (18.109) gilt für $n \in \mathbb{N}_0$, $k \in \mathbb{N}_0 \setminus [0,n]$ stets

$$\binom{n}{k} = |\mathrm{Pot}_k([1,n])| = 0.$$ □

Korollar (18.109) erlaubt uns auch, einen kombinatorischen Beweis für die Rekursionsformel (17.7) zu führen, indem wir eine Rekursionsgleichung für die Anzahl der Teilmengen einer gegebenen endlichen Menge mit vorgegebener Kardinalität herleiten:

(18.111) Bemerkung. Es sei eine endliche Menge X gegeben. Dann ist

$$|\mathrm{Pot}_k(X)| = \begin{cases} 1, & \text{für } k = 0, \\ 0, & \text{für } k \in \mathbb{N}, \text{ falls } X = \emptyset, \\ |\mathrm{Pot}_k(X \setminus \{x\})| + |\mathrm{Pot}_{k-1}(X \setminus \{x\})|, & \text{für } k \in \mathbb{N}, x \in X. \end{cases}$$

Beweis. Für $k = 0$ gilt

$$|\mathrm{Pot}_k(X)| = |\mathrm{Pot}_0(X)| = |\{\emptyset\}| = 1.$$

Falls $X = \emptyset$ ist, so gilt außerdem

$$\begin{aligned} |\mathrm{Pot}_k(X)| = |\mathrm{Pot}_k(\emptyset)| &= |\{U \in \mathrm{Pot}(\emptyset) \mid U \text{ ist endlich mit } |U| = k\}| \\ &= |\{U \in \{\emptyset\} \mid U \text{ ist endlich mit } |U| = k\}| = 0 \end{aligned}$$

für $k \in \mathbb{N}$. Im Folgenden sei $X \neq \emptyset$ und es seien $k \in \mathbb{N}$ und $x \in X$ gegeben. Dann ist

$$\mathrm{Pot}_k(X) = \{U \in \mathrm{Pot}_k(X) \mid x \notin U\} \dot\cup \{U \in \mathrm{Pot}_k(X) \mid x \in U\}.$$

Ferner gilt

$$\{U \in \mathrm{Pot}_k(X) \mid x \notin U\} = \mathrm{Pot}_k(X \setminus \{x\})$$

und es sind

$$\mathrm{Pot}_{k-1}(X \setminus \{x\}) \to \{U \in \mathrm{Pot}_k(X) \mid x \in U\},\ V \mapsto V \cup \{x\},$$
$$\{U \in \mathrm{Pot}_k(X) \mid x \in U\} \to \mathrm{Pot}_{k-1}(X \setminus \{x\}),\ U \mapsto U \setminus \{x\}$$

sich gegenseitig invertierende Bijektionen. Nach der Summenregel (18.4) und der Gleichheitsregel (18.1) folgt

$$\begin{aligned}|\mathrm{Pot}_k(X)| &= |\{U \in \mathrm{Pot}_k(X) \mid x \notin U\} \dot\cup \{U \in \mathrm{Pot}_k(X) \mid x \in U\}| \\ &= |\{U \in \mathrm{Pot}_k(X) \mid x \notin U\}| + |\{U \in \mathrm{Pot}_k(X) \mid x \in U\}| \\ &= |\mathrm{Pot}_k(X \setminus \{x\})| + |\mathrm{Pot}_{k-1}(X \setminus \{x\})|.\end{aligned}$$

□

Bemerkung (18.111) liefert einen kombinatorischen Beweis für Proposition (17.7):

Alternativer Beweis von Proposition (17.7) für $n, k \in \mathbb{N}_0$. Es seien $n, k \in \mathbb{N}_0$ gegeben. Nach Korollar (18.109) und Bemerkung (18.111) gilt

$$\begin{aligned}\binom{n}{k} = |\mathrm{Pot}_k([1,n])| &= \begin{cases} 1, & \text{falls } n \in \mathbb{N}_0,\ k = 0, \\ 0, & \text{falls } n = 0,\ k \in \mathbb{N}, \\ |\mathrm{Pot}_k([1,n-1])| + |\mathrm{Pot}_{k-1}([1,n-1])|, & \text{falls } n \in \mathbb{N},\ k \in \mathbb{N} \end{cases} \\ &= \begin{cases} 1, & \text{falls } n \in \mathbb{N}_0,\ k = 0, \\ 0, & \text{falls } n = 0,\ k \in \mathbb{N}, \\ \binom{n-1}{k} + \binom{n-1}{k-1}, & \text{falls } n \in \mathbb{N},\ k \in \mathbb{N}. \end{cases}\end{aligned}$$

□

Alternativ hätten wir natürlich auch den bisherigen Beweis von Proposition (17.7) zum Beweis von Bemerkung (18.111) verwenden können.
Als nächstes wollen wir alle Teilmengen einer endlichen Menge zählen. Hierzu nutzen wir das Konzept der Indikatorfamilie, siehe Definition (3.35).

(18.112) Proposition. Es seien $n \in \mathbb{N}_0$ und eine n-elementige Menge X gegeben. Dann gilt

$$|\mathrm{Pot}(X)| = 2^n.$$

Beweis. Nach Satz (3.37) und Satz (3.29)(c) ist $\mathrm{Pot}(X) \to \{0,1\}^X,\ U \mapsto \chi_U$ eine Bijektion, so dass nach der Gleichheitsregel (18.1) und Bemerkung (18.18) bereits

$$|\mathrm{Pot}(X)| = |\{0,1\}^X| = |\mathrm{Var}_X(\{0,1\})| = |\{0,1\}|^{|X|} = 2^n$$

folgt. □

(18.113) Beispiel. Es ist

$$|\mathrm{Pot}([1,9])| = 512.$$

Beweis. Nach Proposition (18.112) ist

$$|\mathrm{Pot}([1,9])| = 2^9 = 512.$$

□

Proposition (18.112) liefert einen kombinatorischen Beweis für Korollar (17.14):

Alternativer Beweis von Korollar (17.14). Es ist

$$\mathrm{Pot}([1,n]) = \dot\bigcup_{k \in [0,n]} \{U \in \mathrm{Pot}([1,n]) \mid U \text{ ist } k\text{-elementig}\}.$$

Nach Proposition (18.112), der Summenregel (18.4) und Korollar (18.109) folgt

$$2^n = |\mathrm{Pot}([1,n])| = |\dot\bigcup_{k \in [0,n]} \mathrm{Pot}_k([1,n])| = \sum_{k \in [0,n]} |\mathrm{Pot}_k([1,n])| = \sum_{k \in [0,n]} \binom{n}{k}.$$

Wegen $\binom{n}{k} = |\mathrm{Pot}_k([1,n])| = 0$ für $k \in \mathbb{N}_0 \setminus [0,n]$ folgt weiter

$$2^n = \sum_{k \in [0,n]} \binom{n}{k} = \sum_{k \in \mathbb{N}_0} \binom{n}{k}.$$

□

Stars and Bars

Es seien $n \in \mathbb{N}$, $k \in \mathbb{N}_0$ gegeben. Nach Korollar (18.50), Korollar (17.12) und Korollar (18.62) gilt

$$|\mathrm{MComb}_k([1,n])| = \binom{k+n-1}{k} = \binom{k+n-1}{n-1} = |\mathrm{Comb}_{n-1}([1,k+n-1])|.$$

Im Folgenden werden wir sehen, dass eine kanonische Bijektion von $\mathrm{MComb}_k([1,n])$ nach $\mathrm{Comb}_{n-1}([1,k+n-1])$ angegeben werden kann.

(18.114) Proposition. Es seien $n \in \mathbb{N}$, $k \in \mathbb{N}_0$ gegeben. Dann ist

$$\{m \in \mathbb{N}_0^n \mid \sum_{j\in[1,n]} m_j = k\} \to \mathrm{Comb}_{n-1}([1,k+n-1]),\ m \mapsto [\sum_{j\in[1,l]} m_j + l]_{l\in[1,n-1]}$$

eine wohldefinierte Bijektion.

Beweis. Falls $n = 1$ ist, so gilt

$$\{m \in \mathbb{N}_0^n \mid \sum_{j\in[1,n]} m_j = k\} = \{m \in \mathbb{N}_0^1 \mid \sum_{j\in[1,1]} m_j = k\} = \{m \in \mathbb{N}_0^1 \mid m_1 = k\} = \{(k)\}$$

und

$$\mathrm{Comb}_{n-1}([1,k+n-1]) = \mathrm{Comb}_{1-1}([1,k+1-1]) = \mathrm{Comb}_0([1,k]) = \{[\,]\},$$

so dass

$$f\colon \{m \in \mathbb{N}_0^n \mid \sum_{j\in[1,n]} m_j = k\} \to \mathrm{Comb}_{n-1}([1,k+n-1]),\ m \mapsto [\sum_{j\in[1,l]} m_j + l]_{l\in[1,n-1]}$$

notwendigerweise eine wohldefinierte Bijektion ist.
Im Folgenden gelte $n \geq 2$. Für $m \in \mathbb{N}_0^n$ mit $\sum_{j\in[1,n]} m_j = k$ und $l \in [1,n-2]$ gilt

$$\sum_{j\in[1,l]} m_j + l < \sum_{j\in[1,l+1]} m_j + l + 1.$$

Folglich erhalten wir eine wohldefinierte Abbildung

$$f\colon \{m \in \mathbb{N}_0^n \mid \sum_{j\in[1,n]} m_j = k\} \to \mathrm{Comb}_{n-1}([1,k+n-1]),\ m \mapsto [\sum_{j\in[1,l]} m_j + l]_{l\in[1,n-1]}.$$

Für $x \in \mathrm{Var}_{n-1}([1,k+n-1])$ mit $x_l < x_{l+1}$ für $l \in [1,n-2]$ gilt ferner

$$\begin{aligned}
&x_1 - 1 + \sum_{j\in[2,n-1]} (x_j - x_{j-1} - 1) + k + n - x_{n-1} - 1\\
&= x_1 - 1 + \sum_{j\in[2,n-1]} x_j - \sum_{j\in[2,n-1]} x_{j-1} - \sum_{j\in[2,n-1]} 1 + k + n - x_{n-1} - 1\\
&= \sum_{j\in[1,n-1]} x_j - \sum_{j\in[2,n]} x_{j-1} - \sum_{j\in[1,n]} 1 + k + n = k.
\end{aligned}$$

Da $\{x \in \mathrm{Var}_{n-1}([1,k+n-1]) \mid \text{für } l \in [1,n-2] \text{ gilt } x_l < x_{l+1}\}$ nach Bemerkung (18.58) eine Transversale von $\mathrm{Comb}_{n-1}([1,k+n-1])$ ist, erhalten wir somit eine wohldefinierte Abbildung

$$g\colon \mathrm{Comb}_{n-1}([1,k+n-1]) \to \{m \in \mathbb{N}_0^n \mid \sum_{j\in[1,n]} m_j = k\},$$

welche für $x \in \mathrm{Var}_{n-1}([1,k+n-1])$ mit $x_l < x_{l+1}$ für $l \in [1,n-2]$ durch

$$g([x])_j = \begin{cases} x_1 - 1 & \text{für } j = 1,\\ x_j - x_{j-1} - 1 & \text{für } j \in [2,n-1],\\ k + n - x_{n-1} - 1 & \text{für } j = n \end{cases}$$

gegeben ist.
Für $m \in \mathbb{N}_0^n$ mit $\sum_{j\in[1,n]} m_j = k$ gilt

$$g(f(m))_j = g([\sum_{r\in[1,l]} m_r + l]_{l\in[1,n-1]})_j$$
$$= \left\{\begin{array}{ll} \sum_{r\in[1,1]} m_r + 1 - 1 & \text{falls } j = 1, \\ \sum_{r\in[1,j]} m_r + j - (\sum_{r\in[1,j-1]} m_r + j - 1) - 1 & \text{falls } j \in [2, n-1], \\ k + n - (\sum_{r\in[1,n-1]} m_r + n - 1) - 1 & \text{falls } j = n \end{array}\right\} = m_j$$

für $j \in [1, n]$, also $g(f(m)) = m$. Für $x \in \mathrm{Var}_{n-1}([1, k+n-1])$ mit $x_l < x_{l+1}$ für $l \in [1, n-2]$ gilt

$$\sum_{j\in[1,l]} g([x])_j + l = g([x])_1 + \sum_{j\in[2,l]} g([x])_j + l = x_1 - 1 + \sum_{j\in[2,l]} (x_j - x_{j-1} - 1) + l$$
$$= x_1 - 1 + \sum_{j\in[2,l]} x_j - \sum_{j\in[2,l]} x_{j-1} - \sum_{j\in[2,l]} 1 + l = \sum_{j\in[1,l]} x_j - \sum_{j\in[2,l]} x_{j-1} - \sum_{j\in[1,l]} 1 + l = x_l$$

für $l \in [1, n-1]$, also

$$f(g([x])) = [\sum_{j\in[1,l]} g([x])_j + l]_{l\in[1,n-1]} = [x_l]_{l\in[1,n-1]} = [x].$$

Folglich ist $g \circ f = \mathrm{id}_{\{m\in\mathbb{N}_0^n \mid \sum_{j\in[1,n]} m_j = k\}}$ und $f \circ g = \mathrm{id}_{\mathrm{Comb}_{n-1}([1,k+n-1])}$, d.h. f ist eine invertierbare Abbildung mit $f^{-1} = g$ und damit bijektiv nach Satz (3.29)(c). □

(18.115) Beispiel. Wir haben folgende Bijektion.

$$\{m \in \mathbb{N}_0^3 \mid \sum_{j\in[1,3]} m_j = 2\} \to \mathrm{Comb}_2([1,4]),$$
$$(2,0,0) \mapsto [3,4],$$
$$(1,1,0) \mapsto [2,4],$$
$$(1,0,1) \mapsto [2,3],$$
$$(0,2,0) \mapsto [1,4],$$
$$(0,1,1) \mapsto [1,3],$$
$$(0,0,2) \mapsto [1,2].$$

(18.116) Korollar. Es seien $n \in \mathbb{N}$, $k \in \mathbb{N}_0$ und eine k-elementige Menge I gegeben. Dann ist

$$\mathrm{MComb}_I([1,n]) \to \mathrm{Comb}_{n-1}([1,k+n-1]),\ [x] \mapsto [|\{i \in I \mid x_i \in [1,l]\}| + l]_{l\in[1,n-1]}$$

eine wohldefinierte Bijektion.

Beweis. Nach Satz (18.42) ist

$$\mu_- : : \mathrm{MComb}_I([1,n]) \to \{m \in \mathbb{N}_0^n \mid \sum_{j\in[1,n]} m_j = k\},\ [x] \mapsto \mu_{[x]}$$

eine wohldefinierte Bijektion und nach Proposition (18.114) ist

$$g\colon \{m \in \mathbb{N}_0^n \mid \sum_{j\in[1,n]} m_j = k\} \to \mathrm{Comb}_{n-1}([1,k+n-1]),\ m \mapsto [\sum_{j\in[1,l]} m_j + l]_{l\in[1,n-1]}$$

eine wohldefinierte Bijektion. Folglich ist auch $g \circ \mu_-$ eine Bijektion. Nach der Summenregel (18.4) gilt

$$g(\mu_{[x]}) = g((|\{i \in I \mid x_i = j\}|)_{j\in[1,n]}) = [\sum_{j\in[1,l]} |\{i \in I \mid x_i = j\}| + l]_{l\in[1,n-1]}$$
$$= [|\dot{\bigcup_{j\in[1,l]}} \{i \in I \mid x_i = j\}| + l]_{l\in[1,n-1]} = [|\{i \in I \mid x_i \in [1,l]\}| + l]_{l\in[1,n-1]}$$

für $x \in \mathrm{Var}_I([1,n])$. □

(18.117) Beispiel. Wir haben folgende Bijektion.

$$\begin{aligned}\mathrm{MComb}_2([1,3]) &\to \mathrm{Comb}_2([1,4]),\\ [1,1] &\mapsto [3,4],\\ [1,2] &\mapsto [2,4],\\ [1,3] &\mapsto [2,3],\\ [2,2] &\mapsto [1,4],\\ [2,3] &\mapsto [1,3],\\ [3,3] &\mapsto [1,2].\end{aligned}$$

Alternativer Beweis von Korollar (18.50). Wenn $n = 0$, $k = 0$ ist, dann ist $|\mathrm{Var}_I(X)| = n^k = 0^0 = 1$, also

$$|\mathrm{MComb}_I(X)| = 1 = \binom{-1}{0} = \binom{k+n-1}{k}.$$

Wenn $n = 0$, $k \in \mathbb{N}$ ist, dann ist $|\mathrm{Var}_I(X)| = n^k = 0^k = 0$, nach Bemerkung (17.6) gilt also

$$|\mathrm{MComb}_I(X)| = 0 = \binom{k-1}{k} = \binom{k+n-1}{k}.$$

Im Folgenden sei daher $n \in \mathbb{N}$, $k \in \mathbb{N}_0$. Nach Korollar (18.116) gibt es eine Bijektion

$$\mathrm{MComb}_I([1,n]) \to \mathrm{Comb}_{n-1}([1,k+n-1]),$$

so dass nach der Gleichheitsregel (18.1) und Korollar (17.12) insbesondere

$$|\mathrm{MComb}_I([1,n])| = |\mathrm{Comb}_{n-1}([1,k+n-1])| = \binom{k+n-1}{n-1} = \binom{k+n-1}{k}$$

gilt.
Wegen $|X| = n$ gibt es eine Bijektion $e\colon [1,n] \to X$, welche uns wohldefinierte, sich gegenseitig invertierende Abbildungen

$$\begin{aligned}&\mathrm{MComb}_I([1,n]) \to \mathrm{MComb}_I(X),\ [x] \mapsto [e \circ x],\\ &\mathrm{MComb}_I(X) \to \mathrm{MComb}_I([1,n]),\ [y] \mapsto [e^{-1} \circ y]\end{aligned}$$

liefert. Nach der Gleichheitsregel (18.1) und Korollar (17.12) gilt insbesondere

$$|\mathrm{MComb}_I(X)| = |\mathrm{MComb}_I([1,n])| = \binom{k+n-1}{k}.$$ □

Die in Satz (3.37) etablierte Bijektion zwischen Teilmengen einer Menge X und Familien lässt sich zur Veranschaulichung der Bijektion aus Korollar (18.116) zwischen Multikombinationen und Kombinationen verwenden. Hierzu schränken wir zunächst die Bijektion aus Satz (3.37) auf die Menge aller Teilmengen von gegebener Kardinalität ein und benutzen diese Bijektion sowie die Bijektionen aus Proposition (18.108) und Korollar (18.116), um einerseits eine Bijektion zwischen Multikombinationen und gewissen Tupeln in $\{0,1\}$, welche wir als Strings notieren, vgl. Definition (10.2), und andererseits eine Bijektion zwischen Kombinationen und diesen Strings herzuleiten.

(18.118) Bemerkung. Es seien $k \in \mathbb{N}_0$ und eine Menge X gegeben. Die Abbildungen

$$\begin{aligned}&\mathrm{Pot}_k(X) \to \{w \in \{0,1\}^X \mid |\{x \in X \mid w_x = 1\}| = k\},\ U \mapsto \chi_U,\\ &\{w \in \{0,1\}^X \mid |\{x \in X \mid w_x = 1\}| = k\} \to \mathrm{Pot}_k(X),\ w \mapsto \{x \in X \mid w_x = 1\}\end{aligned}$$

sind zueinander invers.

Beweis. Diese Abbildungen entstehen durch Einschränken der sich gegenseitig invertierenden Abbildungen aus Satz (3.37). □

(18.119) Beispiel. Wir haben folgende Bijektion.

$$\begin{aligned}\mathrm{Pot}_2([1,4]) &\to \{0,1\}^4,\\ \{1,2\} &\mapsto 1100,\\ \{1,3\} &\mapsto 1010,\\ \{1,4\} &\mapsto 1001,\\ \{2,3\} &\mapsto 0110,\\ \{2,4\} &\mapsto 0101,\\ \{3,4\} &\mapsto 0011.\end{aligned}$$

(18.120) Korollar. Es seien $k \in \mathbb{N}_0$ und eine Menge X gegeben. Dann ist

$$\mathrm{Comb}_k(X) \to \{w \in \{0,1\}^X \mid |\{x \in X \mid w_x = 1\}| = k\},\ [x] \mapsto \chi_{\{x_i \mid i \in [1,k]\}}$$

eine wohldefinierte Bijektion.

Beweis. Nach Proposition (18.108) ist

$$\mathrm{Comb}_k(X) \to \mathrm{Pot}_k(X),\ [x] \mapsto \{x_i \mid i \in [1,k]\}$$

eine wohldefinierte Bijektion und nach Bemerkung (18.118) und Satz (3.29)(c) ist

$$\mathrm{Pot}_k(X) \to \{w \in \{0,1\}^X \mid |\{x \in X \mid w_x = 1\}| = k\},\ U \mapsto \chi_U$$

eine wohldefinierte Bijektion. Folglich ist auch das Kompositum

$$\mathrm{Comb}_k(X) \to \{w \in \{0,1\}^X \mid |\{x \in X \mid w_x = 1\}| = k\},\ [x] \mapsto \chi_{\{x_i \mid i \in [1,k]\}}$$

eine wohldefinierte Bijektion. □

(18.121) Beispiel. Wir haben folgende Bijektion.

$$\begin{aligned}\mathrm{Comb}_2([1,4]) &\to \{0,1\}^4,\\ [1,2] &\mapsto 1100,\\ [1,3] &\mapsto 1010,\\ [1,4] &\mapsto 1001,\\ [2,3] &\mapsto 0110,\\ [2,4] &\mapsto 0101,\\ [3,4] &\mapsto 0011.\end{aligned}$$

(18.122) Korollar. Es seien $n \in \mathbb{N}$, $k \in \mathbb{N}_0$ gegeben. Dann ist

$$\begin{aligned}\mathrm{MComb}_k([1,n]) \to \{w \in \{0,1\}^{k+n-1} \mid |\{j \in [1,k+n-1] \mid w_j = 1\}| = n-1\},\\ [x] \mapsto \chi_{\{|\{i \in [1,k] \mid x_i \in [1,l]\}| + l \mid l \in [1,n-1]\}}\end{aligned}$$

eine wohldefinierte Bijektion.

Beweis. Nach Korollar (18.116) ist

$$\mathrm{MComb}_k([1,n]) \to \mathrm{Comb}_{n-1}([1,k+n-1]),\ [x] \mapsto [|\{i \in [1,k] \mid x_i \in [1,l]\}| + l]_{l \in [1,n-1]}$$

eine wohldefinierte Bijektion und nach Korollar (18.120) ist

$$\mathrm{Comb}_{n-1}([1,k+n-1]) \to \{w \in \{0,1\}^{k+n-1} \mid |\{j \in [1,k+n-1] \mid w_j = 1\}| = n-1\},\ [y] \mapsto \chi_{\{y_l \mid l \in [1,n-1]\}}$$

eine wohldefinierte Bijektion. Folglich ist auch das Kompositum

$$\begin{aligned}\mathrm{MComb}_k([1,n]) \to \{w \in \{0,1\}^{k+n-1} \mid |\{j \in [1,k+n-1] \mid w_j = 1\}| = n-1\},\\ [x] \mapsto \chi_{\{|\{i \in [1,k] \mid x_i \in [1,l]\}| + l \mid l \in [1,n-1]\}}\end{aligned}$$

eine wohldefinierte Bijektion. □

(18.123) Beispiel. Wir haben folgende Bijektion.

$$\begin{aligned}\mathrm{MComb}_2([1,3]) &\to \{w \in \{0,1\}^4 \mid |\{j \in [1,4] \mid w_j = 1\}| = 2\},\\ [1,1] &\mapsto 0011,\\ [1,2] &\mapsto 0101,\\ [1,3] &\mapsto 0110,\\ [2,2] &\mapsto 1001,\\ [2,3] &\mapsto 1010,\\ [3,3] &\mapsto 1100.\end{aligned}$$

Wir veranschaulichen einige der diversen Bijektionen aus diesem Abschnitt am Beispiel von 4-Multikombinationen in $[1,3]$, welche ihren zugehörigen Häufigkeitstupeln, 2-Kombinationen in $[1,4+3-1] = [1,6]$ sowie Strings in $\{0,1\}$ der Länge 6 entsprechen, welche genau 2 mal den Eintrag 1 haben. Die Korrespondenz zu den Strings in $\{0,1\}$ ist unter dem Namen *stars and bars* bekannt, man schreibt dann auch $\star$ (star) statt 0 sowie $|$ (bar) statt 1 und verwendet die Stringnotation aus Definition (10.2), verzichtet also auf Klammern und Kommata.
Nach Satz (18.42) entspricht beispielsweise die 4-Multikombination $[1,1,2,3]$ dem Häufigkeitstupel $(2,1,1)$. Nach Korollar (18.122) gehört hierzu der String $\star\star|\star|\star$, welchen wir erhalten, indem wir gerade an den Stellen $3 = 2+1$ und $5 = 2+1+2 = (2+1)+(1+1)$ den Eintrag $|$ und sonst den Eintrag $\star$ setzen. Die $\star$-Einträge entsprechen in ihrer Anzahl dabei gerade den Einträgen des Häufigkeitstupels, während die $|$-Einträge der Abgrenzung der $\star$-Einträge dienen. Auf der anderen Seite entspricht dies nach Korollar (18.120) gerade der 2-Kombination $[3,5]$, da die $|$-Einträge an den Stellen 3 und 5 zu finden sind.

$\mathrm{MComb}_4([1,3])$	$\{m \in \mathbb{N}_0^3 \mid \sum_{j\in[1,4]} m_j = 4\}$	$\{w \in \{\star,\|\}^6 \mid \|\{s \in [1,6] \mid w_s = \|\}\| = 2\}$	$\mathrm{Comb}_2([1,6])$
$[1,1,1,1]$	$(4,0,0)$	$\star\star\star\star\|\|$	$[5,6]$
$[1,1,1,2]$	$(3,1,0)$	$\star\star\star\|\star\|$	$[4,6]$
$[1,1,1,3]$	$(3,0,1)$	$\star\star\star\|\|\star$	$[4,5]$
$[1,1,2,2]$	$(2,2,0)$	$\star\star\|\star\star\|$	$[3,6]$
$[1,1,2,3]$	$(2,1,1)$	$\star\star\|\star\|\star$	$[3,5]$
$[1,1,3,3]$	$(2,0,2)$	$\star\star\|\|\star\star$	$[3,4]$
$[1,2,2,2]$	$(1,3,0)$	$\star\|\star\star\star\|$	$[2,6]$
$[1,2,2,3]$	$(1,2,1)$	$\star\|\star\star\|\star$	$[2,5]$
$[1,2,3,3]$	$(1,1,2)$	$\star\|\star\|\star\star$	$[2,4]$
$[1,3,3,3]$	$(1,0,3)$	$\star\|\|\star\star\star$	$[2,3]$
$[2,2,2,2]$	$(0,4,0)$	$\|\star\star\star\star\|$	$[1,6]$
$[2,2,2,3]$	$(0,3,1)$	$\|\star\star\star\|\star$	$[1,5]$
$[2,2,3,3]$	$(0,2,2)$	$\|\star\star\|\star\star$	$[1,4]$
$[2,3,3,3]$	$(0,1,3)$	$\|\star\|\star\star\star$	$[1,3]$
$[3,3,3,3]$	$(0,0,4)$	$\|\|\star\star\star\star$	$[1,2]$

(18.124) Definition (stars-and-bars-String)**.** Es seien $n \in \mathbb{N}$, $k \in \mathbb{N}_0$ und eine k-Variation x in X gegeben. Der String

$$\chi_{\{|\{i\in[1,k]|x_i\in[1,l]\}|+l|l\in[1,n-1]\}}$$

heißt *stars-and-bars-String* von $[x]$ in X.

(18.125) Beispiel.

(a) Der stars-and-bars-String der 4-Multikombination $[5,3,9,7]$ in $[1,9]$ ist gegeben durch

110110110110.

(b) Der stars-and-bars-String der 4-Multikombination $[5,3,5,7]$ in $[1,9]$ ist gegeben durch

110110011011.

Partitionen

Unterteilungen einer Gesamtheit in „gleichberechtigte“ Teilgesamtheiten lassen sich mit Hilfe von Partitionen, siehe Definition (5.18), modellieren. Wie bei Teilmengen sind wir in erster Linie an Partitionen mit einer vorgegebenen Anzahl an Teilen interessiert:

(18.126) Definition (k-Partition)**.** Es seien $k \in \mathbb{N}_0$ und eine Menge X gegeben. Die *Menge der k-Partitionen* von X ist definiert als

$$\mathrm{Part}_k(X) := \{\mathcal{P} \mid \mathcal{P} \text{ ist eine endliche Partition von } X \text{ mit } |\mathcal{P}| = k\}.$$

Ein Element von $\mathrm{Part}_k(X)$ wird eine *k-Partition* von X genannt.

(18.127) Beispiel. Es ist $\{\{1,3,5,8\},\{2,7\},\{4,9\},\{6\}\}$ eine 4-Partition von $[1,9]$.

(18.128) Beispiel. Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$\begin{aligned}\mathrm{Part}_3(\{a,b,c,d\}) = \{&\{\{a,b\},\{c\},\{d\}\},\{\{a,c\},\{b\},\{d\}\},\{\{a,d\},\{b\},\{c\}\},\{\{b,c\},\{a\},\{d\}\},\\ &\{\{b,d\},\{a\},\{c\}\},\{\{c,d\},\{a\},\{b\}\}\}.\end{aligned}$$

Auch einige Beispiele aus dem täglichen Leben lassen sich durch Partitionen modellieren:

(18.129) Anwendungsbeispiel.

(a) Eine Gesamtheit von 20 Studierenden sei als 20-elementige Menge S modelliert. Eine Aufteilung der Studierenden in fünf Lerngruppen (derart, dass keine Lerngruppe leer bleibt) lässt sich als 5-Partition von S auffassen.

(b) Eine Verteilung von zehn durchnummerierten Kugeln auf vier gleich aussehende Boxen derart, dass keine Box leer bleibt, lässt sich als 4-Partition von $[1,10]$ auffassen.

Um für $k \in \mathbb{N}$ die Anzahl der k-Partitionen einer gegebenen endlichen, nicht-leeren Menge X zu bestimmen, gehen wir wie bei Multikombinationen vor und ermitteln für diese Anzahl eine geeignete Rekursion. Hierzu bedienen wir uns des gleichen Tricks wie im Beweis von Bemerkung (18.111) und betrachten die Zerlegung

$$\mathrm{Part}_k(X) = \{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \notin \mathcal{P}\} \,\dot\cup\, \{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \in \mathcal{P}\}$$

für ein $x \in X$. Die Anzahlen der beiden Teilmengen können wir dann nach folgender Proposition rekursiv bestimmen:

(18.130) Proposition. Es seien eine Menge X und ein $x \in X$ gegeben.

(a) Es sei $k \in \mathbb{N}_0$ gegeben und für jedes $\mathcal{Q} \in \mathrm{Part}_k(X \setminus \{x\})$ sei eine Abzählung $e_\mathcal{Q}$ von $\mathcal{Q}$ gegeben. Dann ist

$$\mathrm{Part}_k(X \setminus \{x\}) \times [1,k] \to \{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \notin \mathcal{P}\},\ (\mathcal{Q},i) \mapsto (\mathcal{Q} \setminus \{e_\mathcal{Q}(i)\}) \cup \{e_\mathcal{Q}(i) \,\dot\cup\, \{x\}\}$$

eine wohldefinierte Bijektion.

(b) Es sei $k \in \mathbb{N}$ gegeben. Dann sind

$$\begin{aligned}&\mathrm{Part}_{k-1}(X \setminus \{x\}) \to \{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \in \mathcal{P}\},\ \mathcal{Q} \mapsto \mathcal{Q} \cup \{\{x\}\},\\ &\{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \in \mathcal{P}\} \to \mathrm{Part}_{k-1}(X \setminus \{x\}),\ \mathcal{P} \mapsto \mathcal{P} \setminus \{\{x\}\}\end{aligned}$$

wohldefinierte, sich gegenseitig invertierende Bijektionen.

Beweis.

(a) Für $\mathcal{Q} \in \mathrm{Part}_k(X \setminus \{x\})$ und $i \in [1,k]$ gilt

$$X = (X \setminus \{x\}) \,\dot\cup\, \{x\} = \dot{\bigcup_{Q \in \mathcal{Q}}} Q \,\dot\cup\, \{x\} = \dot{\bigcup_{Q \in \mathcal{Q} \setminus \{e_\mathcal{Q}(i)\}}} Q \,\dot\cup\, e_\mathcal{Q}(i) \,\dot\cup\, \{x\},$$

also ist $(\mathcal{Q} \setminus \{e_{\mathcal{Q}}(i)\}) \cup \{e_{\mathcal{Q}}(i) \dot\cup \{x\}\} \in \mathrm{Part}_k(X)$, und wegen $e_{\mathcal{Q}}(i) \neq \emptyset$ ist $e_{\mathcal{Q}}(i) \dot\cup \{x\} \neq \{x\}$ und damit $\{x\} \notin (\mathcal{Q} \setminus \{e_{\mathcal{Q}}(i)\}) \cup \{e_{\mathcal{Q}}(i) \dot\cup \{x\}\}$. Folglich haben wir eine wohldefinierte Abbildung

$$f\colon \mathrm{Part}_k(X \setminus \{x\}) \times [1,k] \to \{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \notin \mathcal{P}\},\ (\mathcal{Q}, i) \mapsto (\mathcal{Q} \setminus \{e_{\mathcal{Q}}(i)\}) \cup \{e_{\mathcal{Q}}(i) \dot\cup \{x\}\}.$$

Um zu zeigen, dass f injektiv ist, seien $(\mathcal{Q}, i), (\mathcal{Q}', i') \in \mathrm{Part}_k(X \setminus \{x\}) \times [1,k]$ mit $f(\mathcal{Q}, i) = f(\mathcal{Q}', i')$ gegeben, also so, dass

$$\mathcal{P} := (\mathcal{Q} \setminus \{e_{\mathcal{Q}}(i)\}) \cup \{e_{\mathcal{Q}}(i) \dot\cup \{x\}\} = (\mathcal{Q}' \setminus \{e_{\mathcal{Q}'}(i')\}) \cup \{e_{\mathcal{Q}'}(i') \dot\cup \{x\}\}$$

gilt. Dann ist $e_{\mathcal{Q}}(i) \dot\cup \{x\} = e_{\mathcal{Q}'}(i') \dot\cup \{x\}$ der Teil von x in $\mathcal{P}$. Es folgt $\mathcal{Q} \setminus \{e_{\mathcal{Q}}(i)\} = \mathcal{Q}' \setminus \{e_{\mathcal{Q}'}(i')\}$ sowie $e_{\mathcal{Q}}(i) = e_{\mathcal{Q}'}(i')$, also $\mathcal{Q} = \mathcal{Q}'$. Wegen $e_{\mathcal{Q}}(i) = e_{\mathcal{Q}'}(i')$ impliziert die Injektivität von $e_{\mathcal{Q}} = e_{\mathcal{Q}'}$ dann aber auch $i = i'$. Folglich ist f injektiv.

Um zu zeigen, dass f surjektiv ist, sei ein $\mathcal{P} \in \mathrm{Part}_k(X)$ mit $\{x\} \notin \mathcal{P}$ gegeben. Wir setzen

$$\mathcal{Q} := \{P \setminus \{x\} \mid P \in \mathcal{P}\}.$$

Ferner sei $i \in [1,k]$ das eindeutige Element mit $e_{\mathcal{Q}}(i) \cup \{x\} \in \mathcal{P}$. Dann ist $\mathcal{P} \setminus \{e_{\mathcal{Q}}(i) \cup \{x\}\} = \mathcal{Q} \setminus \{e_{\mathcal{Q}}(i)\}$ und damit $\mathcal{P} = (\mathcal{Q} \setminus \{e_{\mathcal{Q}}(i)\}) \cup \{e_{\mathcal{Q}}(i) \cup \{x\}\} = f(\mathcal{Q})$. Folglich ist f surjektiv.

(b) Für $\mathcal{Q} \in \mathrm{Part}_{k-1}(X \setminus \{x\})$ gilt

$$X = (X \setminus \{x\}) \dot\cup \{x\} = \dot\bigcup_{Q \in \mathcal{Q}} Q \dot\cup \{x\},$$

also ist $\mathcal{Q} \cup \{\{x\}\} \in \mathrm{Part}_k(X)$ und $\{x\} \in \mathcal{Q} \cup \{\{x\}\}$. Folglich haben wir eine wohldefinierte Abbildung

$$f\colon \mathrm{Part}_{k-1}(X \setminus \{x\}) \to \{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \in \mathcal{P}\},\ \mathcal{Q} \mapsto \mathcal{Q} \cup \{\{x\}\}.$$

Für $\mathcal{P} \in \mathrm{Part}_k(X)$ mit $\{x\} \in \mathcal{P}$ ist ferner

$$X = \dot\bigcup_{P \in \mathcal{P}} P = \dot\bigcup_{P \in \mathcal{P} \setminus \{x\}} P \dot\cup \{x\},$$

also $X \setminus \{x\} = \dot\bigcup_{P \in \mathcal{P} \setminus \{x\}} P$ und damit $\mathcal{P} \setminus \{x\} \in \mathrm{Part}_{k-1}(X \setminus \{x\})$. Folglich haben wir auch eine wohldefinierte Abbildung

$$g\colon \{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \in \mathcal{P}\} \to \mathrm{Part}_{k-1}(X \setminus \{x\}),\ \mathcal{P} \mapsto \mathcal{P} \setminus \{\{x\}\}.$$

Wir erhalten

$$g(f(\mathcal{Q})) = (\mathcal{Q} \cup \{\{x\}\}) \setminus \{\{x\}\} = \mathcal{Q}$$

für $\mathcal{Q} \in \mathrm{Part}_{k-1}(X \setminus \{x\})$, also $g \circ f = \mathrm{id}_{\mathrm{Part}_{k-1}(X \setminus \{x\})}$, sowie

$$f(g(\mathcal{P})) = (\mathcal{P} \setminus \{\{x\}\}) \cup \{\{x\}\} = \mathcal{P}$$

für $\mathcal{P} \in \mathrm{Part}_k(X)$ mit $\{x\} \in \mathcal{P}$, also $f \circ g = \mathrm{id}_{\{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \in \mathcal{P}\}}$. Folglich sind f und g sich gegenseitige invertierende Abbildungen und damit Bijektionen nach Satz (3.29)(c). □

(18.131) Beispiel.

(a) Wir haben folgende Bijektion.

$$\begin{aligned}
&\mathrm{Part}_2([1,3]) \times [1,2] \to \{\mathcal{P} \in \mathrm{Part}_2([1,4]) \mid \{4\} \notin \mathcal{P}\},\\
&\quad (\{\{1,2\},\{3\}\},1) \mapsto \{\{1,2,4\},\{3\}\},\\
&\quad (\{\{1,2\},\{3\}\},2) \mapsto \{\{1,2\},\{3,4\}\},\\
&\quad (\{\{1,3\},\{2\}\},1) \mapsto \{\{1,3,4\},\{2\}\},\\
&\quad (\{\{1,3\},\{2\}\},2) \mapsto \{\{1,3\},\{2,4\}\},\\
&\quad (\{\{2,3\},\{1\}\},1) \mapsto \{\{2,3,4\},\{1\}\},\\
&\quad (\{\{2,3\},\{1\}\},2) \mapsto \{\{2,3\},\{1,4\}\}.
\end{aligned}$$

(b) Wir haben folgende Bijektion.

$$\begin{aligned}&\mathrm{Part}_1([1,3]) \to \{\mathcal{P} \in \mathrm{Part}_2([1,4]) \mid \{4\} \in \mathcal{P}\},\\ &\quad \{\{1,2,3\}\} \mapsto \{\{1,2,3\},\{4\}\}.\end{aligned}$$

(18.132) Korollar. Es sei eine endliche Menge X gegeben. Dann ist

$$|\mathrm{Part}_k(X)| = \begin{cases} 1, & \text{für } k = 0, \text{ falls } X = \emptyset,\\ 0, & \text{für } k = 0, \text{ falls } X \neq \emptyset,\\ 0, & \text{für } k \in \mathbb{N}, \text{ falls } X = \emptyset,\\ k\,|\mathrm{Part}_k(X \setminus \{x\})| + |\mathrm{Part}_{k-1}(X \setminus \{x\})|, & \text{für } k \in \mathbb{N},\ x \in X. \end{cases}$$

Beweis. Für $k = 0$ gilt

$$|\mathrm{Part}_k(X)| = |\mathrm{Part}_0(X)| = \begin{cases} 1, & \text{falls } X = \emptyset,\\ 0, & \text{falls } X \neq \emptyset. \end{cases}$$

Falls $X = \emptyset$ ist, so gilt außerdem

$$|\mathrm{Part}_k(X)| = |\mathrm{Part}_k(\emptyset)| = 0$$

für $k \in \mathbb{N}$. Im Folgenden sei $X \neq \emptyset$ und es seien $k \in \mathbb{N}$ und $x \in X$ gegeben. Dann ist

$$\mathrm{Part}_k(X) = \{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \notin \mathcal{P}\} \dot\cup \{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \in \mathcal{P}\}.$$

Nach Proposition (18.130) gibt es dann Bijektionen

$$\begin{aligned}&\mathrm{Part}_k(X \setminus \{x\}) \times [1,k] \to \{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \notin \mathcal{P}\},\\ &\mathrm{Part}_{k-1}(X \setminus \{x\}) \to \{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \in \mathcal{P}\},\end{aligned}$$

und nach der Summenregel (18.4), der Gleichheitsregel (18.1) und der Produktregel (18.8) folgt

$$\begin{aligned}|\mathrm{Part}_k(X)| &= |\{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \notin \mathcal{P}\} \dot\cup \{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \in \mathcal{P}\}|\\ &= |\{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \notin \mathcal{P}\}| + |\{\mathcal{P} \in \mathrm{Part}_k(X) \mid \{x\} \in \mathcal{P}\}|\\ &= |\mathrm{Part}_k(X \setminus \{x\}) \times [1,k]| + |\mathrm{Part}_{k-1}(X \setminus \{x\})|\\ &= |\mathrm{Part}_k(X \setminus \{x\})|\,|[1,k]| + |\mathrm{Part}_{k-1}(X \setminus \{x\})| = k\,|\mathrm{Part}_k(X \setminus \{x\})| + |\mathrm{Part}_{k-1}(X \setminus \{x\})|. \qquad \square\end{aligned}$$

(18.133) Korollar. Für $n, k \in \mathbb{N}_0$ und jede n-elementige Menge X ist

$$|\mathrm{Part}_k(X)| = \left\{ n \atop k \right\}.$$

Beweis. Wir führen Induktion nach n. Für $n = 0$, $k \in \mathbb{N}_0$ und jede n-elementige Menge X gilt $X = \emptyset$, nach Korollar (18.132) also

$$|\mathrm{Part}_k(X)| = \left.\begin{cases} 1, & \text{falls } k = 0,\\ 0, & \text{falls } k \in \mathbb{N} \end{cases}\right\} = \left\{ 0 \atop k \right\} = \left\{ n \atop k \right\}.$$

Es sei $n \in \mathbb{N}$ so gegeben, dass für $k \in \mathbb{N}_0$ und jede endliche Menge X' mit $|X'| = n-1$ stets $|\mathrm{Part}_k(X')| = \left\{ n-1 \atop k \right\}$ gilt. Ferner seien $k \in \mathbb{N}_0$ und eine n-elementige Menge X gegeben. Dann ist $X \neq \emptyset$, d.h. es gibt ein $x \in X$. Nach Korollar (18.132) und der Induktionsvoraussetzung folgt

$$\begin{aligned}|\mathrm{Part}_k(X)| &= \left.\begin{cases} 0, & \text{falls } k = 0,\\ k\,|\mathrm{Part}_k(X \setminus \{x\})| + |\mathrm{Part}_{k-1}(X \setminus \{x\})|, & \text{falls } k \in \mathbb{N} \end{cases}\right\}\\ &= \left.\begin{cases} 0, & \text{falls } k = 0,\\ k \left\{ n-1 \atop k \right\} + \left\{ n-1 \atop k-1 \right\}, & \text{falls } k \in \mathbb{N} \end{cases}\right\} = \left\{ n \atop k \right\}.\end{aligned}$$

Nach dem Induktionsprinzip gilt $|\mathrm{Part}_k(X)| = \left\{ n \atop k \right\}$ für $n, k \in \mathbb{N}_0$ und jede n-elementige Menge X. $\square$

(18.134) Beispiel.

(a) Es ist

$$|\mathrm{Part}_4([1,9])| = 7770.$$

(b) Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$|\mathrm{Part}_3(\{a,b,c,d\})| = 6.$$

Beweis.

(a) Nach Korollar (18.133) ist

$$|\mathrm{Part}_4([1,9])| = \left\{ 9 \atop 4 \right\} = 7770.$$

(b) Nach Korollar (18.133) ist

$$|\mathrm{Part}_3(\{a,b,c,d\})| = \left\{ 4 \atop 3 \right\} = 6.$$ □

Wir kommen zu unseren Beispielen aus dem täglichen Leben zurück:

(18.135) Anwendungsbeispiel.

(a) Eine Gesamtheit von 20 Studierenden sei als 20-elementige Menge S modelliert. Aufteilungen der Studierenden in fünf Lerngruppen (derart, dass keine Lerngruppe leer bleibt) seien als 5-Partitionen von S modelliert. Nach Korollar (18.133) ist die Anzahl aller solchen möglichen Aufteilungen gleich

$$|\mathrm{Part}_5(S)| = \left\{ 20 \atop 5 \right\} = 749\,206\,090\,500.$$

(b) Verteilungen von zehn durchnummerierten Kugeln auf vier gleich aussehende Boxen derart, dass keine Box leer bleibt, seien als 4-Partitionen von $[1, 10]$ modelliert. Nach Korollar (18.133) ist die Anzahl aller solchen möglichen Verteilungen gleich

$$|\mathrm{Part}_4([1,10])| = \left\{ 10 \atop 4 \right\} = 34\,105.$$

Abbildungen

Nun widmen wir uns Abbildungen zwischen endlichen Mengen. Da Abbildungen und Familien einander entsprechen, siehe Bemerkung (3.8) und Konvention (3.9), können wir diesen Fall auf den bereits behandelten von Variationen, siehe Definition (18.14), zurückführen:

(18.136) Bemerkung. Es seien $m, n \in \mathbb{N}_0$ und endliche Mengen X und Y mit $|X| = m$ und $|Y| = n$ gegeben. Dann gilt

$$|\mathrm{Map}(X,Y)| = n^m.$$

Beweis. Nach Bemerkung (18.18) gilt

$$|\mathrm{Map}(X,Y)| = |Y^X| = |\mathrm{Var}_X(Y)| = |Y|^{|X|} = n^m.$$ □

Auch injektive Abbildungen haben wir im Wesentlichen bereits behandelt – diese entsprechen gerade den Permutationen, siehe Definition (18.23):

(18.137) Bemerkung. Es seien $m, n \in \mathbb{N}_0$ und endliche Mengen X und Y mit $|X| = m$ und $|Y| = n$ gegeben. Dann gilt

$$|\mathrm{Map}_{\mathrm{inj}}(X, Y)| = \prod_{i \in [1,m]} (n - i + 1) = \prod_{i \in [n-m+1,n]} i.$$

Wenn $m \in [0, n]$ ist, so gilt

$$|\mathrm{Map}_{\mathrm{inj}}(X, Y)| = \frac{n!}{(n-m)!}.$$

Beweis. Nach Korollar (18.31) gilt

$$|\mathrm{Map}_{\mathrm{inj}}(X, Y)| = |\mathrm{Perm}_X(Y)| = \prod_{i \in [1,m]} (n - i + 1) = \prod_{i \in [n-m+1,n]} i.$$

Wenn $m \in [0, n]$ ist, so gilt nach Korollar (18.31) ferner

$$|\mathrm{Map}_{\mathrm{inj}}(X, Y)| = |\mathrm{Perm}_X(Y)| = \frac{n!}{(n-m)!}.$$ □

Es bleiben surjektive Abbildungen zwischen endlichen Mengen zu zählen. Surjektive Abbildungen modellieren Unterteilungen von Gesamtheiten in zu unterscheidende Unterteile, wie wir an folgenden Beispielen aus dem täglichen Leben sehen:

(18.138) Anwendungsbeispiel.

(a) Eine Gesamtheit von 400 Studierenden sei als 400-elementige Menge S modelliert. Zehn Tutoren seien als Elemente einer 10-elementigen Menge T modelliert. Eine Aufteilung der Studierenden in Tutoriengruppen (derart, dass keine Gruppe leer bleibt) lässt sich als surjektive Abbildung von S nach T auffassen.

(b) Fünf unterschiedliche Süßigkeiten seien als Elemente von $\{\text{Bonbon}, \text{Keks}, \text{Lutscher}, \text{Schokoriegel}, \text{Weingummi}\}$ modelliert. Drei Kinder seien als Elemente von $\{\text{Elias}, \text{Julia}, \text{Laura}\}$ modelliert. Eine Verteilung der Süßigkeiten auf die Kinder (derart, dass jedes Kind mindestens eine Süßigkeit kriegt) lässt sich als surjektive Abbildung von $\{\text{Bonbon}, \text{Keks}, \text{Lutscher}, \text{Schokoriegel}, \text{Weingummi}\}$ nach $\{\text{Elias}, \text{Julia}, \text{Laura}\}$ auffassen.

(c) Eine Verteilung von zehn durchnummerierten Kugeln auf vier unterschiedlich farbige Boxen derart, dass keine Box leer bleibt, lässt sich als surjektive Abbildung von $[1, 10]$ nach $\{\text{rot}, \text{blau}, \text{gelb}, \text{grün}\}$ auffassen.

Damit besitzen surjektive Abbildungen vom Modellierungsaspekt Ähnlichkeiten zu den zuvor behandelten Partitionen; lediglich der Unterscheidungsaspekt kommt neu hinzu. Daher ist es auch nicht verwunderlich, dass das Zählen surjektiver Abbildungen analog vonstatten geht und sich eine ähnliche Formel für die Anzahl surjektiver Abbildungen ergibt, siehe Korollar (18.142).

(18.139) Proposition. Es seien eine Menge X und ein $x \in X$ gegeben.

(a) Es sei $n \in \mathbb{N}_0$ gegeben. Dann sind

$$F \colon \mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\}, [1, n]) \times [1, n] \to \{f \in \mathrm{Map}_{\mathrm{surj}}(X, [1, n]) \mid f^{-1}(\{f(x)\}) \neq \{x\}\}$$

gegeben durch

$$(F(g, j))(x') = \begin{cases} g(x') & \text{für } x' \in X \setminus \{x\}, \\ j & \text{für } x' = x, \end{cases}$$

für $(g, j) \in \mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\}, [1, n]) \times [1, n]$, und

$$G \colon \{f \in \mathrm{Map}_{\mathrm{surj}}(X, [1, n]) \mid f^{-1}(\{f(x)\}) \neq \{x\}\} \to \mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\}, [1, n]) \times [1, n], \\ f \mapsto (f|_{X \setminus \{x\}}, f(x))$$

wohldefinierte, sich gegenseitig invertierende Bijektionen.

(b) Es sei $n \in \mathbb{N}$ gegeben. Dann sind

$$F\colon \mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\}, [1, n-1]) \times [1, n] \to \{f \in \mathrm{Map}_{\mathrm{surj}}(X, [1, n]) \mid f^{-1}(\{f(x)\}) = \{x\}\}$$

gegeben durch

$$(F(g,j))(x') = \begin{cases} g(x') & \text{für } x' \in X \setminus \{x\} \text{ mit } g(x') \in [1, j-1], \\ g(x')+1 & \text{für } x' \in X \setminus \{x\} \text{ mit } g(x') \in [j, n-1], \\ j & \text{für } x' = x \end{cases}$$

für $(g,j) \in \mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\}, [1, n-1]) \times [1, n]$, und

$$G\colon \{f \in \mathrm{Map}_{\mathrm{surj}}(X, [1, n]) \mid f^{-1}(\{f(x)\}) = \{x\}\} \to \mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\}, [1, n-1]) \times [1, n]$$

gegeben durch $G(f) = (G(f)_1, f(x))$ mit

$$(G(f)_1)(x') = \begin{cases} f(x') & \text{für } x' \in X \setminus \{x\} \text{ mit } f(x') \in [1, j-1], \\ f(x')-1 & \text{für } x' \in X \setminus \{x\} \text{ mit } f(x') \in [j+1, n] \end{cases}$$

für $f \in \mathrm{Map}_{\mathrm{surj}}(X, [1, n])$ mit $f^{-1}(\{f(x)\}) = \{x\}$, wohldefinierte, sich gegenseitig invertierende Bijektionen.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(18.140) Beispiel.

(a) Wir haben folgende Bijektion.

$$\begin{aligned}
&\mathrm{Map}_{\mathrm{surj}}([1,3],[1,2]) \times [1,2] \to \{f \in \mathrm{Map}_{\mathrm{surj}}([1,4],[1,2]) \mid f^{-1}(\{f(4)\}) \neq \{4\}\}, \\
&\quad((1 \mapsto 1, 2 \mapsto 1, 3 \mapsto 2), 1) \mapsto (1 \mapsto 1, 2 \mapsto 1, 3 \mapsto 2, 4 \mapsto 1), \\
&\quad((1 \mapsto 1, 2 \mapsto 1, 3 \mapsto 2), 2) \mapsto (1 \mapsto 1, 2 \mapsto 1, 3 \mapsto 2, 4 \mapsto 2), \\
&\quad((1 \mapsto 2, 2 \mapsto 2, 3 \mapsto 1), 1) \mapsto (1 \mapsto 2, 2 \mapsto 2, 3 \mapsto 1, 4 \mapsto 1), \\
&\quad((1 \mapsto 2, 2 \mapsto 2, 3 \mapsto 1), 2) \mapsto (1 \mapsto 2, 2 \mapsto 2, 3 \mapsto 1, 4 \mapsto 2), \\
&\quad((1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 1), 1) \mapsto (1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 1, 4 \mapsto 1), \\
&\quad((1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 1), 2) \mapsto (1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 1, 4 \mapsto 2), \\
&\quad((1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 2), 1) \mapsto (1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 2, 4 \mapsto 1), \\
&\quad((1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 2), 2) \mapsto (1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 2, 4 \mapsto 2), \\
&\quad((1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 1), 1) \mapsto (1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 1, 4 \mapsto 1), \\
&\quad((1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 1), 2) \mapsto (1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 1, 4 \mapsto 2), \\
&\quad((1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 2), 1) \mapsto (1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 2, 4 \mapsto 1), \\
&\quad((1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 2), 2) \mapsto (1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 2, 4 \mapsto 2).
\end{aligned}$$

(b) Wir haben folgende Bijektion.

$$\begin{aligned}
&\mathrm{Map}_{\mathrm{surj}}([1,3],[1,1]) \times [1,2] \to \{f \in \mathrm{Map}_{\mathrm{surj}}([1,4],[1,2]) \mid f^{-1}(\{f(4)\}) = \{4\}\}, \\
&\quad((1 \mapsto 1, 2 \mapsto 1, 3 \mapsto 1), 1) \mapsto (1 \mapsto 2, 2 \mapsto 2, 3 \mapsto 2, 4 \mapsto 1), \\
&\quad((1 \mapsto 1, 2 \mapsto 1, 3 \mapsto 1), 2) \mapsto (1 \mapsto 1, 2 \mapsto 1, 3 \mapsto 1, 4 \mapsto 2).
\end{aligned}$$

(18.141) Korollar. Es sei eine endliche Menge X gegeben. Dann ist

$$|\mathrm{Map}_{\mathrm{surj}}(X, [1, n])| = \begin{cases} 1, & \text{für } n = 0, \text{ falls } X = \emptyset, \\ 0, & \text{für } n = 0, \text{ falls } X \neq \emptyset, \\ 0, & \text{für } n \in \mathbb{N}, \text{ falls } X = \emptyset, \\ n(|\mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\}, [1, n])| + |\mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\}, [1, n-1])|), & \text{für } n \in \mathbb{N},\ x \in X. \end{cases}$$

Beweis. Für $n = 0$ gilt

$$|\mathrm{Map}_{\mathrm{surj}}(X,[1,n])| = |\mathrm{Map}_{\mathrm{surj}}(X,[1,0])| = |\mathrm{Map}_{\mathrm{surj}}(X,\emptyset)| = \begin{cases} 1, & \text{falls } X = \emptyset, \\ 0, & \text{falls } X \neq \emptyset. \end{cases}$$

Falls $X = \emptyset$ ist, so gilt außerdem

$$|\mathrm{Map}_{\mathrm{surj}}(X,[1,n])| = |\mathrm{Map}_{\mathrm{surj}}(\emptyset,[1,n])| = 0$$

für $n \in \mathbb{N}$. Im Folgenden sei $X \neq \emptyset$ und es seien $n \in \mathbb{N}$ und $x \in X$ gegeben. Dann ist

$$\begin{aligned} &\mathrm{Map}_{\mathrm{surj}}(X,[1,n]) \\ &= \{f \in \mathrm{Map}_{\mathrm{surj}}(X,[1,n]) \mid f^{-1}(\{f(x)\}) \neq \{x\}\} \dot\cup \{f \in \mathrm{Map}_{\mathrm{surj}}(X,[1,n]) \mid f^{-1}(\{f(x)\}) = \{x\}\}. \end{aligned}$$

Nach Proposition (18.139) gibt es dann Bijektionen

$$\begin{aligned} &\mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\},[1,n]) \times [1,n] \to \{f \in \mathrm{Map}_{\mathrm{surj}}(X,[1,n]) \mid f^{-1}(\{f(x)\}) \neq \{x\}\}, \\ &\mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\},[1,n-1]) \times [1,n] \to \{f \in \mathrm{Map}_{\mathrm{surj}}(X,[1,n]) \mid f^{-1}(\{f(x)\}) = \{x\}\}, \end{aligned}$$

und nach der Summenregel (18.4), der Gleichheitsregel (18.1) und der Produktregel (18.8) folgt

$$\begin{aligned} &|\mathrm{Map}_{\mathrm{surj}}(X,[1,n])| \\ &= |\{f \in \mathrm{Map}_{\mathrm{surj}}(X,[1,n]) \mid f^{-1}(\{f(x)\}) \neq \{x\}\} \dot\cup \{f \in \mathrm{Map}_{\mathrm{surj}}(X,[1,n]) \mid f^{-1}(\{f(x)\}) = \{x\}\}| \\ &= |\{f \in \mathrm{Map}_{\mathrm{surj}}(X,[1,n]) \mid f^{-1}(\{f(x)\}) \neq \{x\}\}| + |\{f \in \mathrm{Map}_{\mathrm{surj}}(X,[1,n]) \mid f^{-1}(\{f(x)\}) = \{x\}\}| \\ &= |\mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\},[1,n]) \times [1,n]| + |\mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\},[1,n-1]) \times [1,n]| \\ &= |\mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\},[1,n])|\,|[1,n]| + |\mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\},[1,n-1])|\,|[1,n]| \\ &= n(|\mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\},[1,n])| + |\mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\},[1,n-1])|). \end{aligned}$$

□

(18.142) Korollar. Für $m, n \in \mathbb{N}_0$, jede m-elementige Menge X und jede n-elementige Menge Y ist

$$|\mathrm{Map}_{\mathrm{surj}}(X,Y)| = n! \left\{ {m \atop n} \right\}.$$

Beweis. Um zu zeigen, dass für $m, n \in \mathbb{N}_0$ und jede m-elementige Menge X stets $|\mathrm{Map}_{\mathrm{surj}}(X,[1,n])| = n! \left\{ {m \atop n} \right\}$ gilt, führen wir Induktion nach m. Für $m = 0$, $n \in \mathbb{N}_0$ und jede m-elementige Menge X gilt $X = \emptyset$, nach Korollar (18.141) also

$$|\mathrm{Map}_{\mathrm{surj}}(X,[1,n])| = \left.\begin{cases} 1, & \text{falls } n = 0, \\ 0, & \text{falls } n \in \mathbb{N} \end{cases}\right\} = \left.\begin{cases} 1! \cdot 1, & \text{falls } n = 0, \\ n! \cdot 0, & \text{falls } n \in \mathbb{N} \end{cases}\right\} = n! \left\{ {0 \atop n} \right\} = n! \left\{ {m \atop n} \right\}.$$

Es sei $m \in \mathbb{N}$ so gegeben, dass für $n \in \mathbb{N}_0$ und jede $(m-1)$-elementige Menge X' stets $|\mathrm{Map}_{\mathrm{surj}}(X',[1,n])| = n! \left\{ {m-1 \atop n} \right\}$ gilt. Ferner seien $m \in \mathbb{N}_0$ und eine m-elementige Menge X gegeben. Dann ist $X \neq \emptyset$, d.h. es gibt ein $x \in X$. Nach Korollar (18.141) und der Induktionsvoraussetzung folgt

$$\begin{aligned} |\mathrm{Map}_{\mathrm{surj}}(X,[1,n])| &= \left.\begin{cases} 0, & \text{falls } n = 0, \\ n\,(|\mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\},[1,n])| + |\mathrm{Map}_{\mathrm{surj}}(X \setminus \{x\},[1,n-1])|), & \text{falls } n \in \mathbb{N} \end{cases}\right\} \\ &= \left.\begin{cases} 0! \cdot \left\{ {m \atop 0} \right\}, & \text{falls } n = 0, \\ n\,(n! \left\{ {m-1 \atop n} \right\} + (n-1)! \left\{ {m-1 \atop n-1} \right\}), & \text{falls } n \in \mathbb{N} \end{cases}\right\} \\ &= \left.\begin{cases} 0! \cdot \left\{ {m \atop 0} \right\}, & \text{falls } n = 0, \\ n!\,(n \left\{ {m-1 \atop n} \right\} + \left\{ {m-1 \atop n-1} \right\}), & \text{falls } n \in \mathbb{N} \end{cases}\right\} = n! \left\{ {m \atop n} \right\}. \end{aligned}$$

Nach dem Induktionsprinzip gilt $|\mathrm{Map}_{\mathrm{surj}}(X,[1,n])| = n! \left\{ {m \atop n} \right\}$ für $m, n \in \mathbb{N}_0$ und jede m-elementige Menge X.

Nun seien $m, n \in \mathbb{N}_0$, eine m-elementige Menge X und eine n-elementige Menge Y gegeben. Dann gibt es eine Bijektion $e\colon [1,n] \to Y$, welche uns wohldefinierte, sich gegenseitig invertierende Abbildungen

$$\begin{aligned}&\mathrm{Map}_{\mathrm{surj}}(X,[1,n]) \to \mathrm{Map}_{\mathrm{surj}}(X,Y),\ f \mapsto e \circ f,\\ &\mathrm{Map}_{\mathrm{surj}}(X,Y) \to \mathrm{Map}_{\mathrm{surj}}(X,[1,n]),\ g \mapsto e^{-1} \circ g\end{aligned}$$

liefert. Nach Satz (3.29)(c) und der Gleichheitsregel (18.1) folgt

$$|\mathrm{Map}_{\mathrm{surj}}(X,Y)| = |\mathrm{Map}_{\mathrm{surj}}(X,[1,n])| = n! \left\{ {m \atop n} \right\}. \qquad \square$$

(18.143) Beispiel.

(a) Es ist

$$|\mathrm{Map}_{\mathrm{surj}}([1,9],[1,4])| = 186480.$$

(b) Es seien verschiedene Objekte a, b, c, d gegeben. Dann ist

$$|\mathrm{Map}_{\mathrm{surj}}(\{a,b,c,d\},[1,3])| = 36.$$

Beweis.

(a) Nach Korollar (18.142) ist $|\mathrm{Map}_{\mathrm{surj}}([1,9],[1,4])| = 4! \left\{ {9 \atop 4} \right\} = 186480$.

(b) Nach Korollar (18.142) ist $|\mathrm{Map}_{\mathrm{surj}}(\{a,b,c,d\},[1,3])| = 3! \left\{ {4 \atop 3} \right\} = 36$. $\square$

Wir kommen zu unseren Beispielen aus dem täglichen Leben zurück:

(18.144) Anwendungsbeispiel.

(a) Eine Gesamtheit von 400 Studierenden sei als 400-elementige Menge S modelliert. Zehn Tutoren seien als Elemente einer 10-elementigen Menge T modelliert. Aufteilungen der Studierenden in Tutoriengruppen (derart, dass keine Gruppe leer bleibt) seien als surjektive Abbildungen von S nach T modelliert. Nach Korollar (18.142) ist die Anzahl aller solchen möglichen Aufteilungen gleich

$$|\mathrm{Map}_{\mathrm{surj}}(S,T)| = 10! \left\{ {400 \atop 10} \right\} \approx 1{,}00 \cdot 10^{200}.$$

(b) Fünf unterschiedliche Süßigkeiten seien als Elemente von $\{\text{Bonbon}, \text{Keks}, \text{Lutscher}, \text{Schokoriegel}, \text{Weingummi}\}$ modelliert. Drei Kinder seien als Elemente von $\{\text{Elias}, \text{Julia}, \text{Laura}\}$ modelliert. Verteilungen der Süßigkeiten auf die Kinder (derart, dass jedes Kind mindestens eine Süßigkeit kriegt) seien als surjektive Abbildungen von $\{\text{Bonbon}, \text{Keks}, \text{Lutscher}, \text{Schokoriegel}, \text{Weingummi}\}$ nach $\{\text{Elias}, \text{Julia}, \text{Laura}\}$ modelliert. Nach Korollar (18.142) ist die Anzahl aller solchen möglichen Verteilungen gleich

$$\begin{aligned}|\mathrm{Map}_{\mathrm{surj}}(\{\text{Bonbon}, \text{Keks}, \text{Lutscher}, \text{Schokoriegel}, \text{Weingummi}\}, \{\text{Elias}, \text{Julia}, \text{Laura}\})| &= 3! \left\{ {5 \atop 3} \right\}\\ &= 150.\end{aligned}$$

(c) Verteilungen von zehn durchnummerierten Kugeln auf vier unterschiedlich farbige Boxen derart, dass keine Box leer bleibt, seien als surjektive Abbildungen von $[1,10]$ nach $\{\text{rot}, \text{blau}, \text{gelb}, \text{grün}\}$ modelliert. Nach Korollar (18.133) ist die Anzahl aller solchen möglichen Verteilungen gleich

$$|\mathrm{Map}_{\mathrm{surj}}([1,10],\{\text{rot}, \text{blau}, \text{gelb}, \text{grün}\})| = 4! \left\{ {10 \atop 4} \right\} = 818\,520.$$

Dass in Korollar (18.142) Stirlingzahlen wie bei Partitionen auftauchen, ist nicht verwunderlich: Jede surjektive Abbildung $f\colon X \to Y$ von einer m-elementigen Menge X in eine n-elementige Menge Y gibt Anlass zur n-Partition $X/{=_f}$ der Fasern von f. Der Faktor $n!$ ergibt sich aus der Tatsache, dass mit jeder solchen Abbildung $f\colon X \to Y$ auch $\pi \circ f\colon X \to Y$ für $\pi \in \mathrm{S}_Y$ eine surjektive Abbildung mit $X/{=_{\pi \circ f}} = X/{=_f}$ ist. Dies führt zu einem alternativen Beweis für Korollar (18.142). Die Details seien dem Leser zur Übung überlassen.

Permutationen

Schließlich zählen wir Permutationen von Mengen, siehe Definition (14.1), mit einer vorgegebenen Anzahl an Bahnen. Da die Bahnen gerade den Zykeln entsprechen, lassen sich hierdurch Unterteilungen in zyklische Gebilde modellieren.

(18.145) Notation. Es seien $n, k \in \mathbb{N}_0$ gegeben. Wir setzen

$$\mathrm{S}_{n,k} := \{\pi \in \mathrm{S}_n \mid |[1,n]/\pi| = k\}.$$

(18.146) Beispiel. Es ist $(1,3,5,8)(2,7)(4,9) = (1,3,5,8)(2,7)(4,9)(6) \in \mathrm{S}_{9,4}$.

(18.147) Beispiel. Es ist

$$\mathrm{S}_{4,2} = \{(1,2,3),(1,2,4),(1,3,2),(1,3,4),(1,4,2),(1,4,3),(2,3,4),(2,4,3),(1,2)(3,4),(1,3)(2,4),\\ (1,4)(2,3)\}.$$

Ein Beispiel aus dem täglichen Leben:

(18.148) Anwendungsbeispiel. Eine Sitzordnung auf einer Feier mit 50 Teilnehmern um zehn runde Tische derart, dass kein Tisch leer bleibt, lässt sich als Element von $\mathrm{S}_{50,10}$ auffassen.

Ein ähnlicher Trick wie in den Beweisen von Bemerkung (18.111), Korollar (18.132) und Korollar (18.142) führt auch beim Zählen von Permutationen mit vorgegebener Anzahl von Bahnen zum Ziel: Diesmal betrachten wir die Zerlegung

$$\mathrm{S}_{n,k} = \{\pi \in \mathrm{S}_{n,k} \mid \pi(n) \neq n\} \dot\cup \{\pi \in \mathrm{S}_{n,k} \mid \pi(n) = n\}$$

und bestimmen wie in Proposition (18.130) und Proposition (18.139) die Anzahl der beiden Teilmengen rekursiv:

(18.149) Proposition. Es sei $n \in \mathbb{N}$ gegeben.

(a) Es sei $k \in \mathbb{N}_0$ gegeben. Dann sind

$$F\colon \mathrm{S}_{n-1,k} \times [1,n-1] \to \{\pi \in \mathrm{S}_{n,k} \mid \pi(n) \neq n\}$$

gegeben durch

$$(F(\sigma,j))(i) = \begin{cases} \sigma(i) & \text{für } i \in [1,n-1] \setminus \{j\}, \\ n & \text{für } i = j, \\ \sigma(j) & \text{für } i = n, \end{cases}$$

für $(\sigma, j) \in \mathrm{S}_{n-1,k} \times [1,n-1]$, und

$$G\colon \{\pi \in \mathrm{S}_{n,k} \mid \pi(n) \neq n\} \to \mathrm{S}_{n-1,k} \times [1,n-1]$$

gegeben durch $G(\pi) = (G(\pi)_1, \pi^{-1}(n))$ mit

$$(G(\pi)_1)(i) = \begin{cases} \pi(i) & \text{für } i \in [1,n-1] \text{ mit } \pi(i) \neq n, \\ \pi(n) & \text{für } i \in [1,n-1] \text{ mit } \pi(i) = n, \end{cases}$$

für $\pi \in \mathrm{S}_{n,k}$ mit $\pi(n) \neq n$, wohldefinierte, sich gegenseitig invertierende Bijektionen.

(b) Es sei $k \in \mathbb{N}$ gegeben. Dann sind

$$F\colon \mathrm{S}_{n-1,k-1} \to \{\pi \in \mathrm{S}_{n,k} \mid \pi(n) = n\}$$

gegeben durch

$$(F(\sigma))(i) = \begin{cases} \sigma(i) & \text{für } i \in [1,n-1], \\ n & \text{für } i = n, \end{cases}$$

für $\sigma \in \mathrm{S}_{n-1,k-1}$, und

$$G\colon \{\pi \in \mathrm{S}_{n,k} \mid \pi(n) = n\} \to \mathrm{S}_{n-1,k-1},\ \pi \mapsto \pi|^{[1,n-1]}_{[1,n-1]}$$

wohldefinierte, sich gegenseitig invertierende Bijektionen.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(18.150) Beispiel.

(a) Wir haben folgende Bijektion.

$$\begin{aligned}
&\mathrm{S}_{3,2} \times [1,3] \to \{\pi \in \mathrm{S}_{4,2} \mid \pi(4) \neq 4\},\\
&\quad ((1,2),1) \mapsto (1,4,2),\\
&\quad ((1,2),2) \mapsto (1,2,4),\\
&\quad ((1,2),3) \mapsto (1,2)(3,4),\\
&\quad ((1,3),1) \mapsto (1,4,3),\\
&\quad ((1,3),2) \mapsto (1,3)(2,4),\\
&\quad ((1,3),3) \mapsto (1,3,4),\\
&\quad ((2,3),1) \mapsto (1,4)(2,3),\\
&\quad ((2,3),2) \mapsto (2,4,3),\\
&\quad ((2,3),3) \mapsto (2,3,4).
\end{aligned}$$

(b) Wir haben folgende Bijektion.

$$\begin{aligned}
&\mathrm{S}_{3,1} \to \{\pi \in \mathrm{S}_{4,2} \mid \pi(4) = 4\},\\
&(1,2,3) \mapsto (1,2,3),\\
&(1,3,2) \mapsto (1,3,2).
\end{aligned}$$

(18.151) Korollar. Es ist

$$|\mathrm{S}_{n,k}| = \begin{cases} 1, & \text{für } n = 0,\ k = 0,\\ 0, & \text{für } n \in \mathbb{N},\ k = 0 \text{ und für } n = 0,\ k \in \mathbb{N},\\ (n-1)\,|\mathrm{S}_{n-1,k}| + |\mathrm{S}_{n-1,k-1}|, & \text{für } n \in \mathbb{N},\ k \in \mathbb{N}. \end{cases}$$

Beweis. Für $n = 0$, $k = 0$ gilt

$$|\mathrm{S}_{n,k}| = |\mathrm{S}_{0,0}| = \{\pi \in \mathrm{S}_0 \mid |[1,0]/\pi| = 0\} = 1,$$

für $n \in \mathbb{N}$, $k = 0$ gilt

$$|\mathrm{S}_{n,k}| = |\mathrm{S}_{n,0}| = \{\pi \in \mathrm{S}_n \mid |[1,n]/\pi| = 0\} = 0,$$

und für $n = 0$, $k \in \mathbb{N}$ gilt

$$|\mathrm{S}_{n,k}| = |\mathrm{S}_{0,k}| = \{\pi \in \mathrm{S}_n \mid |[1,0]/\pi| = k\} = 0.$$

Im Folgenden seien $n, k \in \mathbb{N}$ gegeben. Dann ist

$$\mathrm{S}_{n,k} = \{\pi \in \mathrm{S}_{n,k} \mid \pi(n) \neq n\} \dot\cup \{\pi \in \mathrm{S}_{n,k} \mid \pi(n) = n\}.$$

Nach Proposition (18.149) gibt es Bijektionen

$$\begin{aligned}
&\mathrm{S}_{n-1,k} \times [1,n-1] \to \{\pi \in \mathrm{S}_{n,k} \mid \pi(n) \neq n\},\\
&\mathrm{S}_{n-1,k-1} \to \{\pi \in \mathrm{S}_{n,k} \mid \pi(n) = n\},
\end{aligned}$$

und nach der Summenregel (18.4), der Gleichheitsregel (18.1) und der Produktregel (18.8) folgt

$$\begin{aligned}
|\mathrm{S}_{n,k}| &= |\{\pi \in \mathrm{S}_{n,k} \mid \pi(n) \neq n\} \dot\cup \{\pi \in \mathrm{S}_{n,k} \mid \pi(n) = n\}|\\
&= |\{\pi \in \mathrm{S}_{n,k} \mid \pi(n) \neq n\}| + |\{\pi \in \mathrm{S}_{n,k} \mid \pi(n) = n\}| = |\mathrm{S}_{n-1,k} \times [1,n-1]| + |\mathrm{S}_{n-1,k-1}|\\
&= |\mathrm{S}_{n-1,k}|\,|[1,n-1]| + |\mathrm{S}_{n-1,k-1}| = (n-1)\,|\mathrm{S}_{n-1,k}| + |\mathrm{S}_{n-1,k-1}|.
\end{aligned}$$

□

(18.152) Korollar. Für $n, k \in \mathbb{N}_0$ ist

$$|\mathrm{S}_{n,k}| = \begin{bmatrix} n \\ k \end{bmatrix}.$$

Beweis. Wir führen Induktion nach n. Für $n = 0$, $k \in \mathbb{N}_0$ gilt

$$|\mathrm{S}_{n,k}| = \begin{cases} 1, & \text{falls } k = 0, \\ 0, & \text{falls } k \in \mathbb{N} \end{cases} = \begin{bmatrix} 0 \\ k \end{bmatrix} = \begin{bmatrix} n \\ k \end{bmatrix}$$

nach Korollar (18.151). Es sei $n \in \mathbb{N}$ so gegeben, dass für $k \in \mathbb{N}_0$ stets $|\mathrm{S}_{n-1,k}| = \left[\begin{smallmatrix} n-1 \\ k \end{smallmatrix}\right]$ gilt. Für $k \in \mathbb{N}_0$ gilt nach Korollar (18.151), der Induktionsvoraussetzung und Bemerkung (17.29) dann auch

$$|\mathrm{S}_{n,k}| = \begin{cases} 0, & \text{falls } k = 0, \\ (n-1)\,|\mathrm{S}_{n-1,k}| + |\mathrm{S}_{n-1,k-1}|, & \text{falls } k \in \mathbb{N} \end{cases} = \begin{cases} 0, & \text{falls } k = 0, \\ (n-1)\left[\begin{smallmatrix} n-1 \\ k \end{smallmatrix}\right] + \left[\begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix}\right], & \text{falls } k \in \mathbb{N} \end{cases} = \begin{bmatrix} n \\ k \end{bmatrix}.$$

Nach dem Induktionsprinzip gilt $|\mathrm{S}_{n,k}| = \left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]$ für alle $n, k \in \mathbb{N}_0$. □

(18.153) Beispiel.

(a) Es ist $|\mathrm{S}_{9,4}| = 67284$.

(b) Es ist $|\mathrm{S}_{4,2}| = 11$.

Beweis.

(a) Nach Korollar (18.152) ist $|\mathrm{S}_{9,4}| = \left[\begin{smallmatrix} 9 \\ 4 \end{smallmatrix}\right] = 67284$.

(b) Nach Korollar (18.152) ist $|\mathrm{S}_{4,2}| = \left[\begin{smallmatrix} 4 \\ 2 \end{smallmatrix}\right] = 11$. □

Wir kommen zu unserem Beispiel aus dem täglichen Leben zurück:

(18.154) Anwendungsbeispiel. Sitzordnungen auf einer Feier mit 50 Teilnehmern um zehn runde Tische derart, dass kein Tisch leer bleibt, seien als Elemente von $\mathrm{S}_{50,10}$ modelliert. Nach Korollar (18.152) ist die Anzahl aller solchen möglichen Sitzordnungen gleich

$$|\mathrm{S}_{50,10}| = \begin{bmatrix} 50 \\ 10 \end{bmatrix} \approx 1{,}02 \cdot 10^{62}.$$

19 Wahrscheinlichkeitstheorie

In der Wahrscheinlichkeitstheorie beschäftigen wir uns mit mathematischen Modellen für Vorgänge, deren Ausgang abhängig vom Zufall ist, sogenannte *Zufallsexperimente*. Hierbei geben wir lediglich einen groben Überblick über die relevantesten Konzepte für den Fall, dass das zu modellierende Zufallsexperiment nur endlich viele mögliche Ergebnisse hat, und überlassen den Fall unendlich vieler Ausgänge ([52]) weiterführenden Veranstaltungen. Nach der Einführung eines axiomatischen Modells für Zufallsexperimente mit endlich vielen Ausgängen und der Betrachtung eines Standardfalls betrachten wir mit Zufallsgrößen, Produktwahrscheinlichkeitsräumen und bedingter Wahrscheinlichkeit Möglichkeiten, um aus gegebenen Modellen neue Modelle zu konstruieren. Dies wenden wir an, um die in Abschnitt 18 eingeführten Auswahlmodelle geeignet im Rahmen der Wahrscheinlichkeitsrechnung zu interpretieren. Danach reißen wir das Konzept der stochastischen Unabhängigkeit an und beschließen den Abschnitt schließlich mit Begriffen zum Studium reellwertiger Zufallsgrößen.

[52] De facto wird dieser Fall üblicherweise in zwei Fälle untergliedert: Den abzählbaren Fall, bei dem die Formalisierungen der möglichen Ergebnisse in Bijektion zur Menge der natürlichen Zahlen stehen, und den überabzählbaren Fall. Bereits für den abzählbaren Fall wird das Konzept der Konvergenz aus der Analysis benötigt.

Quasiendliche Wahrscheinlichkeitsräume

Das zentrale Konzept dieses Abschnitts ist der eines (quasi)endlichen Wahrscheinlichkeitsraums, ein mathematisches Modell für Zufallsexperimente mit endlich vielen Ausgängen. Da wir bei konkreten Fragestellungen üblicherweise an der Wahrscheinlichkeit gewisser Ereignisse statt an der Wahrscheinlichkeit einzelner Ergebnisse des Zufallsexperiments interessiert sind, wird in unserem Modell bereits den diesen Ereignissen entsprechenden Objekten (welche wir Ereignisse des Wahrscheinlichkeitsraums nennen werden) eine Wahrscheinlichkeit zugeordnet. Dieses Vorgehen ist etabliert und erlaubt eine Verallgemeinerung auf allgemeine Wahrscheinlichkeitsräume – Modelle mit unendlichen Ergebnismengen. In Proposition (19.9) werden wir jedoch sehen, dass die Wahrscheinlichkeiten sämtlicher Ereignisse eines quasiendlichen Wahrscheinlichkeitsraums durch die Wahrscheinlichkeiten der Ausgänge des zu modellierenden Zufallsexperiments festgelegt sind.
Auch wenn wir in den Beispielen meist endliche Ergebnismengen haben werden, betrachten wir auch Wahrscheinlichkeitsräume mit unendlichen Ergebnismengen, bei denen nur endlich viele Ergebnisse eine positive Wahrscheinlichkeit haben. Hierdurch können wir mittels reellwertiger Zufallsgrößen Wahrscheinlichkeitsverteilungen auf der Menge der reellen Zahlen konstruieren und diese Verteilungen mittels Erwartungswert und Varianz, siehe Definition (19.56) und Definition (19.63) beschreiben.

(19.1) Definition ((quasi)endlicher Wahrscheinlichkeitsraum)**.**

(a) Ein *quasiendlicher Wahrscheinlichkeitsraum* besteht aus einer nicht leeren Menge X zusammen mit einer Abbildung $P\colon \mathrm{Pot}(X) \to \mathbb{R}$ derart, dass folgende Axiome gelten.

- *Nichtnegativität.* Für $A \in \mathrm{Pot}(X)$ ist

  $$P(A) \geq 0.$$

- *Normiertheit.* Es ist

  $$P(X) = 1.$$

- *Additivität.* Für disjunkte $A, B \in \mathrm{Pot}(X)$ gilt

  $$P(A \mathbin{\dot\cup} B) = P(A) + P(B).$$

- *Endlichkeit und Normiertheit des Trägers.* Die Teilmenge $\{x \in X \mid P(\{x\}) > 0\}$ von X ist endlich und es gilt

  $$\sum_{x \in X} P(\{x\}) = \sum_{\substack{x \in X \\ P(\{x\})>0}} P(\{x\}) = 1.$$

Unter Missbrauch der Notation bezeichnen wir sowohl den besagten quasiendlichen Wahrscheinlichkeitsraum als auch die unterliegende Menge mit X. Die unterliegende Menge von X wird *Ergebnismenge* (oder *Grundmenge*) von X genannt. Ein Element von X wird *Ergebnis* (oder *Ausgang*) von X genannt. Die Potenzmenge $\mathrm{Pot}(X)$ wird *Ereignismenge* (oder *Ereignisraum*) von X genannt. Ein Element von $\mathrm{Pot}(X)$ wird *Ereignis* von X genannt. Das Element $\emptyset$ von $\mathrm{Pot}(X)$ wird *unmögliches Ereignis* von X genannt. Das Element X von $\mathrm{Pot}(X)$ wird *sicheres Ereignis* von X genannt. Die Abbildung P wird *Wahrscheinlichkeitsverteilung* (oder *Wahrscheinlichkeitsmaß*) von X genannt. Für jedes Ereignis A von X wird $P(A)$ die *Wahrscheinlichkeit* von A in X genannt.

Für einen quasiendlichen Wahrscheinlichkeitsraum X mit Wahrscheinlichkeitsverteilung P schreiben wir $\mathrm{P} = \mathrm{P}^X := P$ sowie $\mathrm{P}(x) := \mathrm{P}(\{x\})$ für jedes Ergebnis x von X.

(b) Ein *endlicher Wahrscheinlichkeitsraum* ist ein quasiendlicher Wahrscheinlichkeitsraum dessen Ergebnismenge endlich ist. ([53])

[53] Es lässt sich zeigen, dass für endliche Mengen die Endlichkeit und Normiertheit des Trägers automatisch erfüllt ist. Vgl. Proposition (19.10)(b).

Der allgemeinere Begriff eines (beliebigen) *Wahrscheinlichkeitsraums* wird üblicherweise auf einem sogenannten *Messraum* definiert, d.h. auf einer Menge X versehen mit einer sogenannten Sigmaalgebra. Dabei ist eine *Sigmaalgebra* eine Teilmenge von $\mathrm{Pot}(X)$, welche abgeschlossen unter gewissen Mengenoperationen ist. Für jede Menge X ist $\mathrm{Pot}(X)$ stets eine Sigmaalgebra. Somit können wir jede Menge X als Messraum versehen mit $\mathrm{Pot}(X)$ auffassen. Die Definition für allgemeinere Messräume wird benötigt, da sich zeigen lässt, dass es auf gewissen unendlichen Mengen X wie bspw. $\mathbb{R}$ keine Wahrscheinlichkeitsverteilungen mit gewissen wünschenswerten Eigenschaften gibt.
Ferner fordert man für das allgemeinere Konzept eines Wahrscheinlichkeitsraums die sogenannte *Sigmaadditivität*, ein Axiom, welches im Allgemeinen echt stärker als die in Definition (19.1) geforderte Additivität ist. Wegen der Endlichkeit des Trägers sind Additivität und Sigmaadditivität unter Annahme der übrigen Axiome äquivalent.

(19.2) Beispiel.

(a) Es wird $\{0,1\}$ ein endlicher Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}(A) = \begin{cases} 0 & \text{für } A = \emptyset, \\ \frac{1}{2} & \text{für } A \in \{\{0\},\{1\}\}, \\ 1 & \text{für } A = \{0,1\}. \end{cases}$$

(b) Es wird $\{0,1\}$ ein endlicher Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}(A) = \begin{cases} 0 & \text{für } A = \emptyset, \\ \frac{1}{4} & \text{für } A = \{0\}, \\ \frac{3}{4} & \text{für } A = \{1\}, \\ 1 & \text{für } A = \{0,1\}. \end{cases}$$

(c) Es wird $\mathbb{R}$ ein quasiendlicher Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}(A) = \begin{cases} 1 & \text{für } A \in \mathrm{Pot}(\mathbb{R}) \text{ mit } 0 \in A, \\ 0 & \text{für } A \in \mathrm{Pot}(\mathbb{R}) \text{ mit } 0 \notin A. \end{cases}$$

Beweis.

(a) Es sei $P\colon \mathrm{Pot}(\{0,1\}) \to \mathbb{R}$ gegeben durch

$$P(A) = \begin{cases} 0 & \text{für } A = \emptyset, \\ \frac{1}{2} & \text{für } A \in \{\{0\},\{1\}\}, \\ 1 & \text{für } A = \{0,1\}. \end{cases}$$

Wir verifizieren die Axiome eines quasiendlichen Wahrscheinlichkeitsraums:

- *Nichtnegativität.* Für $A \in \mathrm{Pot}(X)$ ist

$$P(A) = \left.\begin{cases} 0, & \text{falls } A = \emptyset, \\ \frac{1}{2}, & \text{falls } A \in \{\{0\},\{1\}\}, \\ 1, & \text{falls } A = \{0,1\} \end{cases}\right\} \geq 0.$$

- *Normiertheit.* Es ist

$$P(\{0,1\}) = 1.$$

- *Additivität.* Es gilt

$$P(\emptyset \mathbin{\dot\cup} \emptyset) = P(\emptyset) = 0 = 0 + 0 = P(\emptyset) + P(\emptyset),$$

$$P(\emptyset \dot\cup \{0\}) = P(\{0\}) = \frac{1}{2} = 0 + \frac{1}{2} = P(\emptyset) + P(\{0\}),$$
$$P(\emptyset \dot\cup \{1\}) = P(\{1\}) = \frac{1}{2} = 0 + \frac{1}{2} = P(\emptyset) + P(\{1\}),$$
$$P(\emptyset \dot\cup \{0,1\}) = P(\{0,1\}) = 1 = 0 + 1 = P(\emptyset) + P(\{0,1\}),$$
$$P(\{0\} \dot\cup \{1\}) = P(\{0,1\}) = 1 = \frac{1}{2} + \frac{1}{2} = P(\{0\}) + P(\{1\}).$$

Für disjunkte $A, B \in \operatorname{Pot}(X)$ ist außerdem $A \dot\cup B = B \dot\cup A$ und $P(A)+P(B) = P(B)+P(A)$. Folglich gilt

$$P(A \dot\cup B) = P(A) + P(B)$$

für alle disjunkten $A, B \in \operatorname{Pot}(X)$.

- *Endlichkeit und Normiertheit des Trägers.* Es ist

$$\{x \in \{0,1\} \mid P(\{x\}) > 0\} = \{x \in \{0,1\} \mid \{x\} \in \{\{0\},\{1\}\}\} = \{0,1\}$$

endlich und es gilt

$$\sum_{x \in \{0,1\}} P(\{x\}) = P(\{0\}) + P(\{1\}) = \frac{1}{2} + \frac{1}{2} = 1.$$

Insgesamt wird $\{0,1\}$ ein quasiendlicher Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung $\mathrm{P} = P$.

(b) Dies sei dem Leser zur Übung überlassen.

(c) Es sei $P\colon \operatorname{Pot}(X) \to \mathbb{R}$ gegeben durch

$$P(A) = \begin{cases} 1 & \text{für } A \in \operatorname{Pot}(\mathbb{R}) \text{ mit } 0 \in A, \\ 0, & \text{für } A \in \operatorname{Pot}(\mathbb{R}) \text{ mit } 0 \notin A. \end{cases}$$

Wir verifizieren die Axiome eines quasiendlichen Wahrscheinlichkeitsraums:

- *Nichtnegativität.* Für $A \in \operatorname{Pot}(X)$ ist

$$P(A) = \left.\begin{cases} 1, & \text{falls } A \in \operatorname{Pot}(\mathbb{R}) \text{ mit } 0 \in A, \\ 0, & \text{falls } A \in \operatorname{Pot}(\mathbb{R}) \text{ mit } 0 \notin A \end{cases}\right\} \geq 0.$$

- *Normiertheit.* Wegen $0 \in \mathbb{R}$ ist

$$P(\mathbb{R}) = 1.$$

- *Additivität.* Es seien disjunkte $A, B \in \operatorname{Pot}(X)$ gegeben. Genau dann gilt $0 \in A \dot\cup B$, wenn $0 \in A$ oder $0 \in B$ ist, und genau dann gilt $0 \in A$, wenn $0 \notin B$ ist. Folglich gilt

$$P(A \dot\cup B) = \left.\begin{cases} 1, & \text{falls } 0 \in A \dot\cup B, \\ 0, & \text{falls } 0 \notin A \dot\cup B \end{cases}\right\} = \left.\begin{cases} 1+0, & \text{falls } 0 \in A,\ 0 \notin B \\ 0+1, & \text{falls } 0 \notin A,\ 0 \in B, \\ 0+0, & \text{falls } 0 \notin A,\ 0 \notin B \end{cases}\right\} = P(A) + P(B).$$

- *Endlichkeit und Normiertheit des Trägers.* Es ist

$$\{x \in \mathbb{R} \mid P(\{x\}) > 0\} = \{x \in \mathbb{R} \mid \{x\} = \{0\}\} = \{0\}$$

eine endliche Teilmenge von $\mathbb{R}$ und es gilt

$$\sum_{x \in X} P(\{x\}) = P(\{0\}) = 1.$$

Insgesamt wird $\mathbb{R}$ ein quasiendlicher Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung $\mathrm{P} = P$. □

(19.3) Anwendungsbeispiel.

(a) Die möglichen (realen) Ergebnisse eines Münzwurfs mit einer gewöhnlichen Münze seien als (formale) Ergebnisse des endlichen Wahrscheinlichkeitsraums $\{\text{Kopf}, \text{Zahl}\}$ mit der Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}(A) = \begin{cases} 0 & \text{für } A = \emptyset, \\ \frac{1}{2} & \text{für } A \in \{\{\text{Kopf}\}, \{\text{Zahl}\}\}, \\ 1 & \text{für } A = \{\text{Kopf}, \text{Zahl}\}. \end{cases}$$

modelliert, wobei Kopf dem Ergebnis entspreche, dass die Münze nach dem Wurf den Kopf zeigt, und Zahl dem Ergebnis entspreche, dass die Münze nach dem Wurf die Zahl zeigt. Die Wahrscheinlichkeit, dass die Münze nach dem Wurf den Kopf zeigt, ist dann gleich

$$\mathrm{P}(\text{Kopf}) = \frac{1}{2}.$$

(b) Die möglichen (realen) Ergebnisse eines Münzwurfs mit einer gezinkten Münze seien als (formale) Ergebnisse des endlichen Wahrscheinlichkeitsraums $\{\text{Kopf}, \text{Zahl}\}$ mit der Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}(A) = \begin{cases} 0 & \text{für } A = \emptyset, \\ \frac{1}{4} & \text{für } A = \{\text{Kopf}\}, \\ \frac{3}{4} & \text{für } A = \{\text{Zahl}\}, \\ 1 & \text{für } A = \{\text{Kopf}, \text{Zahl}\}. \end{cases}$$

modelliert, wobei Kopf dem Ergebnis entspreche, dass die Münze nach dem Wurf den Kopf zeigt, und Zahl dem Ergebnis entspreche, dass die Münze nach dem Wurf die Zahl zeigt. Die Wahrscheinlichkeit, dass die Münze nach dem Wurf den Kopf zeigt, ist dann gleich

$$\mathrm{P}(\text{Kopf}) = \frac{1}{4}.$$

Wir studieren einige Eigenschaften von quasiendlichen Wahrscheinlichkeitsräumen:

(19.4) Bemerkung. Es sei ein quasiendlicher Wahrscheinlichkeitsraum X gegeben. Für alle Ereignisse A und B von X mit $A \subseteq B$ gilt

$$\mathrm{P}(B \setminus A) = \mathrm{P}(B) - \mathrm{P}(A)$$

und

$$\mathrm{P}(A) \leq \mathrm{P}(B).$$

Beweis. Es seien Ereignisse A und B von X mit $A \subseteq B$ gegeben. Dann gilt $B = A \mathbin{\dot\cup} (B \setminus A)$, also

$$\mathrm{P}(B) = \mathrm{P}(A \mathbin{\dot\cup} (B \setminus A)) = \mathrm{P}(A) + \mathrm{P}(B \setminus A)$$

und damit $\mathrm{P}(B \setminus A) = \mathrm{P}(B) - \mathrm{P}(A)$. Wegen

$$0 \leq \mathrm{P}(B \setminus A) = \mathrm{P}(B) - \mathrm{P}(A)$$

folgt insbesondere $\mathrm{P}(A) \leq \mathrm{P}(B)$. □

(19.5) Korollar. Es sei ein quasiendlicher Wahrscheinlichkeitsraum X gegeben. Es gilt

$$\mathrm{P}(\emptyset) = 0.$$

Beweis. Nach Bemerkung (19.4) gilt

$$\mathrm{P}(\emptyset) = \mathrm{P}(\emptyset \setminus \emptyset) = \mathrm{P}(\emptyset) - \mathrm{P}(\emptyset) = 0.$$ □

(19.6) Korollar. Es sei ein quasiendlicher Wahrscheinlichkeitsraum X gegeben. Für jedes Ereignis A von X gilt

$$\mathrm{P}(X \setminus A) = 1 - \mathrm{P}(A)$$

und

$$\mathrm{P}(A) \leq 1.$$

Beweis. Für jedes Ereignis A von X gilt

$$\mathrm{P}(X \setminus A) = \mathrm{P}(X) - \mathrm{P}(A) = 1 - \mathrm{P}(A)$$

nach Bemerkung (19.4). Wegen

$$0 \leq \mathrm{P}(X \setminus A) = 1 - \mathrm{P}(A)$$

folgt insbesondere $\mathrm{P}(A) \leq 1$. □

(19.7) Bemerkung (Gesetz der totalen Wahrscheinlichkeit)**.** Es sei ein quasiendlicher Wahrscheinlichkeitsraum X gegeben. Für jedes Ereignis A von X, jedes $n \in \mathbb{N}_0$ und jedes disjunkte n-Tupel von Ereignissen $(B_1, \ldots, B_n)$ von X ([54]) mit $A \subseteq \dot{\bigcup}_{i\in[1,n]} B_i$ gilt

$$\mathrm{P}(A) = \sum_{i\in[1,n]} \mathrm{P}(A \cap B_i).$$

Beweis. Für jedes Ereignis A von X, jedes $n \in \mathbb{N}_0$ und jedes disjunkte n-Tupel von Ereignissen $(B_1, \ldots, B_n)$ von X mit $A \subseteq \dot{\bigcup}_{i\in[1,n]} B_i$ gilt $A = A \cap \dot{\bigcup}_{i\in[1,n]} B_i = \dot{\bigcup}_{i\in[1,n]}(A \cap B_i)$, also

$$\mathrm{P}(A) = \mathrm{P}(\dot{\bigcup_{i\in[1,n]}} (A \cap B_i)) = \sum_{i\in[1,n]} \mathrm{P}(A \cap B_i).$$ □

(19.8) Proposition. Es sei ein quasiendlicher Wahrscheinlichkeitsraum X gegeben. Für $n \in \mathbb{N}_0$ und jedes n-Tupel von Ereignissen $(A_1, \ldots, A_n)$ von X gilt

$$\mathrm{P}(\bigcup_{i\in[1,n]} A_i) = \sum_{i\in[1,n]} (-1)^{i-1} \sum_{\substack{J\subseteq[1,n]\\|J|=i}} \mathrm{P}(\bigcap_{j\in J} A_j).$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

(19.9) Proposition. Es sei ein quasiendlicher Wahrscheinlichkeitsraum X gegeben. Für jedes Ereignis A von X gilt

$$\mathrm{P}(A) = \mathrm{P}(\{x \in A \mid \mathrm{P}(x) > 0\}) = \sum_{\substack{x\in A\\ \mathrm{P}(x)>0}} \mathrm{P}(x) = \sum_{x\in A} \mathrm{P}(x).$$

Beweis. Für jedes Ereignis A von X gilt

$$\mathrm{P}(\{x \in A \mid \mathrm{P}(x) > 0\}) = \mathrm{P}(\dot{\bigcup_{\substack{x\in A\\ \mathrm{P}(\{x\})>0}}} \{x\}) = \sum_{\substack{x\in A\\ \mathrm{P}(x)>0}} \mathrm{P}(x) = \sum_{x\in A} \mathrm{P}(x).$$

[54] Wir nehmen also an, dass B_i für $i \in [1, n]$ ein Ereignis von X ist.

Insbesondere gilt also

$$\mathrm{P}(\{x \in X \mid \mathrm{P}(x) > 0\}) = \sum_{x \in X} \mathrm{P}(x) = 1.$$

Nun sei ein Ereignis A von X gegeben. Dann gilt $\{x \in X \mid \mathrm{P}(x) > 0\} \subseteq A \cup \{x \in X \mid \mathrm{P}(x) > 0\}$, nach Bemerkung (19.4) und Korollar (19.6) also

$$1 = \mathrm{P}(\{x \in X \mid \mathrm{P}(x) > 0\}) \leq \mathrm{P}(A \cup \{x \in X \mid \mathrm{P}(x) > 0\}) \leq 1$$

und damit

$$\begin{aligned} 1 &= \mathrm{P}(A \cup \{x \in X \mid \mathrm{P}(x) > 0\}) = \mathrm{P}(A) + \mathrm{P}(\{x \in X \mid \mathrm{P}(x) > 0\}) - \mathrm{P}(A \cap \{x \in X \mid \mathrm{P}(x) > 0\}) \\ &= \mathrm{P}(A) + 1 - \mathrm{P}(\{x \in A \mid \mathrm{P}(x) > 0\}) \end{aligned}$$

nach Proposition (19.8). Es folgt

$$\mathrm{P}(A) = \mathrm{P}(\{x \in A \mid \mathrm{P}(x) > 0\}) = \sum_{x \in A} \mathrm{P}(x). \qquad \square$$

In Proposition (19.9) haben wir gesehen, dass sich die Wahrscheinlichkeit jedes Ereignisses eines quasiendlichen Wahrscheinlichkeitsraums in eine Summe der Wahrscheinlichkeiten der zugehörigen Ergebnisse zerlegen lässt. Umgekehrt liefert dies eine Methode zur Konstruktion von Wahrscheinlichkeitsräumen:

(19.10) Proposition.

(a) Es seien eine Menge X und eine Abbildung $f\colon X \to \mathbb{R}$ so gegeben, dass folgende Eigenschaften gelten.

- *Nichtnegativität.* Für $x \in X$ ist

  $$f(x) \geq 0.$$

- *Endlichkeit des Trägers.* Die Teilmenge

  $$\{x \in X \mid f(x) > 0\}$$

  von X ist endlich.
- *Normiertheit.* Es ist

  $$\sum_{x \in X} f(x) = 1.$$

Dann wird X ein quasiendlicher Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}(A) = \sum_{x \in A} f(x)$$

für jedes Ereignis A von X.

(b) Es seien eine endliche Menge X und eine Abbildung $f\colon X \to \mathbb{R}$ so gegeben, dass folgende Eigenschaften gelten.

- *Nichtnegativität.* Für $x \in X$ ist

  $$f(x) \geq 0.$$

- *Normiertheit.* Es ist

  $$\sum_{x \in X} f(x) = 1.$$

Dann wird X zu einem endlichen Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}(A) = \sum_{x \in A} f(x)$$

für jedes Ereignis A von X.

Beweis.

(a) Es sei $P\colon \mathrm{Pot}(X) \to \mathbb{R}$, $A \mapsto \sum_{x \in A} f(x)$. Wir verifizieren die Axiome eines quasiendlichen Wahrscheinlichkeitsraums:

- *Nichtnegativität.* Für $A \in \mathrm{Pot}(X)$ ist $f(x) \geq 0$ für $x \in A$, also auch
$$P(A) = \sum_{x \in A} f(x) \geq 0.$$
- *Normiertheit.* Es ist
$$P(X) = \sum_{x \in X} f(x) = 1.$$
- *Additivität.* Für disjunkte $A, B \in \mathrm{Pot}(X)$ gilt
$$P(A \mathbin{\dot\cup} B) = \sum_{x \in A \dot\cup B} f(x) = \sum_{x \in A} f(x) + \sum_{x \in B} f(x) = P(A) + P(B).$$
- *Endlichkeit und Normiertheit des Trägers.* Für $x \in X$ gilt
$$P(\{x\}) = \sum_{y \in \{x\}} f(y) = f(x).$$
Folglich ist $\{x \in X \mid P(\{x\}) > 0\} = \{x \in X \mid f(x) > 0\}$ endlich und es gilt
$$\sum_{x \in X} P(\{x\}) = \sum_{x \in X} f(x) = 1.$$

Insgesamt wird X ein quasiendlicher Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung $\mathrm{P}^X = P$.

(b) Da $\{x \in X \mid f(x) > 0\}$ als Teilmenge der endlichen Menge X selbst endlich ist, folgt dies aus (a). □

(19.11) Beispiel. Es wird $\{0,1,2\}$ zu einem endlichen Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}(A) = \begin{cases} 0 & \text{für } A \in \{\emptyset, \{0\}\}, \\ \frac{1}{3} & \text{für } A \in \{\{1\}, \{0,1\}\}, \\ \frac{2}{3} & \text{für } A \in \{\{2\}, \{0,2\}\}, \\ 1 & \text{für } A \in \{\{1,2\}, \{0,1,2\}\}. \end{cases}$$

Beweis. Es sei $f\colon \{0,1,2\} \to \mathbb{R}$, $x \mapsto \frac{x}{3}$. Dann ist $f(x) \geq 0$ für $x \in \{0,1,2\}$ und es gilt

$$\sum_{x \in \{0,1,2\}} f(x) = \sum_{x \in \{0,1,2\}} \frac{x}{3} = \frac{0}{3} + \frac{1}{3} + \frac{2}{3} = 1.$$

Nach Proposition (19.10)(b) wird $\{0,1,2\}$ zu einem endlichen Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}(A) = \sum_{x \in A} f(x) = \left\{ \begin{array}{ll} 0, & \text{falls } 1 \notin A,\ 2 \notin A, \\ \frac{1}{3}, & \text{falls } 1 \in A,\ 2 \notin A, \\ \frac{2}{3}, & \text{falls } 1 \notin A,\ 2 \in A, \\ 1, & \text{falls } 1 \in A,\ 2 \in A \end{array} \right\} = \begin{cases} 0, & \text{falls } A \in \{\emptyset, \{0\}\}, \\ \frac{1}{3}, & \text{falls } A \in \{\{1\}, \{0,1\}\}, \\ \frac{2}{3}, & \text{falls } A \in \{\{2\}, \{0,2\}\}, \\ 1, & \text{falls } A \in \{\{1,2\}, \{0,1,2\}\}, \end{cases}$$

für jedes Ereignis A von $\{0,1,2\}$. □

Laplaceräume

Nimmt man an, dass die Ergebnisse eines Zufallsexperiments alle gleichberechtigt sind, so modelliert man dieses durch einen Laplaceraum, bei der sich die Wahrscheinlichkeit eines Ereignisses aus dem Verhältnis der für das Ereignis günstigen Ergebnisse und der Anzahl aller Ergebnisse ergibt:

(19.12) Definition (Laplaceraum)**.** Ein *Laplaceraum* (oder *uniformer Raum* oder *Laplaceexperiment*) ist ein endlicher Wahrscheinlichkeitsraum X mit Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}(A) = \frac{|A|}{|X|}$$

für jedes Ereignis A von X.

Die Wahrscheinlichkeit eines Ereignisses in einem Laplaceraum lässt sich also durch Berechnung der Kardinalitäten einer endlichen Menge und einer Teilmenge bestimmen. Mit anderen Worten: Wahrscheinlichkeitstheoretische Fragestellungen in Laplaceräumen entsprechen im Wesentlichen kombinatorischen Fragestellungen.

(19.13) Beispiel.

(a) Der Wahrscheinlichkeitsraum X mit Ergebnismenge $X = \{0, 1\}$ und Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}(A) = \begin{cases} 0 & \text{für } A = \emptyset, \\ \frac{1}{2} & \text{für } A \in \{\{0\}, \{1\}\}, \\ 1 & \text{für } A = \{0, 1\}. \end{cases}$$

ist ein Laplaceraum.

(b) Der Wahrscheinlichkeitsraum Y mit Ergebnismenge $Y = \{0, 1\}$ und Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}(A) = \begin{cases} 0 & \text{für } A = \emptyset, \\ \frac{1}{4} & \text{für } A = \{0\}, \\ \frac{3}{4} & \text{für } A = \{1\}, \\ 1 & \text{für } A = \{0, 1\}. \end{cases}$$

ist kein Laplaceraum.

Beweis.

(a) Es ist $|X| = |\{0, 1\}| = 2$. Wegen

$$\begin{aligned} \mathrm{P}(\emptyset) = 0 = \frac{0}{2} &= \frac{|\emptyset|}{|X|}, \\ \mathrm{P}(\{0\}) = \frac{1}{2} &= \frac{|\{0\}|}{|X|}, \\ \mathrm{P}(\{1\}) = \frac{1}{2} &= \frac{|\{1\}|}{|X|}, \\ \mathrm{P}(\{0, 1\}) = 1 = \frac{2}{2} &= \frac{|\{0, 1\}|}{|X|} \end{aligned}$$

ist X ein Laplaceraum.

(b) Es ist $|Y| = |\{0, 1\}| = 2$. Wegen

$$\mathrm{P}(\{0\}) = \frac{1}{4} \neq \frac{1}{2} = \frac{|\{0\}|}{|Y|}$$

ist Y kein Laplaceraum. □

(19.14) Bemerkung. Es sei ein endlicher Wahrscheinlichkeitsraum X gegeben. Genau dann ist X ein Laplaceraum, wenn

$$\mathrm{P}(x) = \frac{1}{|X|}$$

für jedes Ergebnis x von X gilt.

Beweis. Wenn X ein Laplaceraum ist, so gilt $\mathrm{P}(A) = \frac{|A|}{|X|}$ für jedes Ereignis A von X, also insbesondere

$$\mathrm{P}(x) = \frac{|\{x\}|}{|X|} = \frac{1}{|X|}$$

für jedes Ergebnis x von X. Umgekehrt, wenn $\mathrm{P}(x) = \frac{1}{|X|}$ für jedes Ergebnis x von X gilt, so ist nach Proposition (19.9) auch

$$\mathrm{P}(A) = \sum_{x \in A} \mathrm{P}(x) = \sum_{x \in A} \frac{1}{|X|} = \frac{|A|}{|X|}$$

für jedes Ereignis A von X, d.h. X ist ein Laplaceraum. □

Bisher haben wir Laplaceräume nur beschrieben. Nun zeigen wir, dass eine Gleichverteilung auf jeder endlichen Menge existiert, d.h. dass sich jede endliche Menge als Laplaceraum auffassen lässt:

(19.15) Bemerkung. Es sei eine nicht leere endliche Menge X gegeben. Dann wird X zu einem Laplaceraum $X = X_{\mathrm{Laplace}}$ mit Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}^{X_{\mathrm{Laplace}}}(A) = \frac{|A|}{|X|}$$

für jedes Ereignis A von X_{Laplace}.

Beweis. Es sei $f\colon X \to \mathbb{R}$, $x \mapsto \frac{1}{|X|}$. Dann ist $f(x) \geq 0$ für $x \in X$ und es gilt

$$\sum_{x \in X} f(x) = \sum_{x \in X} \frac{1}{|X|} = |X| \, \frac{1}{|X|} = 1.$$

Nach Proposition (19.10)(b) wird X zu einem endlichen Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}(A) = \sum_{x \in A} f(x) = \sum_{x \in A} \frac{1}{|X|} = |A| \, \frac{1}{|X|} = \frac{|A|}{|X|}$$

für jedes Ereignis A von X. □

Alternativer Beweis von Bemerkung (19.15). Es sei $P\colon \mathrm{Pot}(X) \to \mathbb{R}$, $A \mapsto \frac{|A|}{|X|}$. Wir verifizieren die Axiome eines quasiendlichen Wahrscheinlichkeitsraums:

- *Nichtnegativität.* Für $A \in \mathrm{Pot}(X)$ ist

$$P(A) = \frac{|A|}{|X|} \geq 0.$$

- *Normiertheit.* Es ist

$$P(X) = \frac{|X|}{|X|} = 1.$$

- *Additivität.* Für disjunkte $A, B \in \mathrm{Pot}(X)$ gilt

$$P(A \mathbin{\dot\cup} B) = \frac{|A \mathbin{\dot\cup} B|}{|X|} = \frac{|A| + |B|}{|X|} = \frac{|A|}{|X|} + \frac{|B|}{|X|} = P(A) + P(B).$$

- *Endlichkeit und Normiertheit des Trägers.* Für $x \in X$ ist

$$P(\{x\}) = \frac{|\{x\}|}{|X|} = \frac{1}{|X|} > 0.$$

Insbesondere ist $\{x \in X \mid P(\{x\}) > 0\} = X$ endlich und es gilt

$$\sum_{x \in X} P(\{x\}) = \sum_{x \in X} \frac{1}{|X|} = |X| \frac{1}{|X|} = 1.$$

Insgesamt wird X zu einem endlichen Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung $\mathrm{P}^X = P$. □

(19.16) Definition (Laplaceraum)**.** Es sei eine nicht leere endliche Menge X gegeben. Der endliche Wahrscheinlichkeitsraum $X = X_{\mathrm{Laplace}}$ aus Bemerkung (19.15) wird *Laplaceraum* (oder *uniformer Raum*) auf X genannt. Die Wahrscheinlichkeitsverteilung von X_{Laplace} wird auch *Gleichverteilung* auf X genannt und als $\mathrm{P}_{\mathrm{unif}} = \mathrm{P}^X_{\mathrm{unif}} := \mathrm{P}^{X_{\mathrm{Laplace}}}$ notiert.

Sofern wir keine anderweitigen Vereinbarungen treffen, fassen wir eine Menge nach Bemerkung (19.15) stets als Laplaceraum auf.

(19.17) Beispiel. Es wird $[1, 6]$ zu einem Laplaceraum.

Beweis. Dies folgt aus Bemerkung (19.15). □

(19.18) Anwendungsbeispiel. Die möglichen (realen) Ergebnisse eines Würfelwurfs mit einem gewöhnlichen Würfel seien als (formale) Ergebnisse des Laplaceraums $[1, 6]$ modelliert, wobei x für $x \in [1, 6]$ dem Ergebnis entspricht, dass der Würfel nach dem Wurf die Seite mit genau x Augen zeigt.
Das (reale) Ereignis, dass der Würfel nach dem Wurf mindestens fünf Augen zeigt, entspricht dem (formalen) Ereignis $\{5, 6\}$ von $[1, 6]$. Seine Wahrscheinlichkeit ist gleich

$$\mathrm{P}(\{5, 6\}) = \frac{|\{5, 6\}|}{|[1, 6]|} = \frac{2}{6} = \frac{1}{3}.$$

Das (reale) Ereignis, dass der Würfel nach dem Wurf eine gerade Anzahl an Augen zeigt, entspricht dem (formalen) Ereignis $\{2, 4, 6\}$ von $[1, 6]$. Seine Wahrscheinlichkeit ist gleich

$$\mathrm{P}(\{2, 4, 6\}) = \frac{|\{2, 4, 6\}|}{|[1, 6]|} = \frac{3}{6} = \frac{1}{2}.$$

Zufallsgrößen

Als nächstes wollen wir Methoden kennenlernen, um aus gegebenen Wahrscheinlichkeitsräumen neue Wahrscheinlichkeitsräume zu konstruieren. Die fruchtbarste Methode liefern dabei sogenannte Zufallsgrößen, mit deren Hilfe sich die für eine gegebene Fragestellung relevanten Merkmale eines Zufallsexperiments extrahieren lassen.
Wir veranschaulichen die Idee an einem einführenden Beispiel:

(19.19) Anwendungsbeispiel. In einer Urne befinden sich zehn rote und 20 schwarze Kugeln. Es wird blind eine Kugel entnommen. Die möglichen (realen) Ergebnisse dieser Entnahme seien als (formale) Ergebnisse des Laplaceraums $U = [1, 10] \times \{\mathrm{rot}\} \mathbin{\dot\cup} [1, 20] \times \{\mathrm{schwarz}\}$ modelliert. Die Anzahl der Ergebnisse ist nach der Summenregel (18.4) gleich

$$|U| = |[1, 10] \times \{\mathrm{rot}\} \mathbin{\dot\cup} [1, 20] \times \{\mathrm{schwarz}\}| = |[1, 10] \times \{\mathrm{rot}\}| + |[1, 20] \times \{\mathrm{schwarz}\}| = 10 + 20 = 30.$$

Das (reale) Ereignis, dass die gezogene Kugel rot ist, entspricht dem (formalen) Ereignis $[1, 10] \times \{\mathrm{rot}\}$ von U. Seine Wahrscheinlichkeit ist gleich

$$\mathrm{P}^U([1, 10] \times \{\mathrm{rot}\}) = \frac{|[1, 10] \times \{\mathrm{rot}\}|}{|U|} = \frac{10}{30} = \frac{1}{3}.$$

Das (reale) Ereignis, dass die gezogene Kugel schwarz ist, entspricht dem (formalen) Ereignis $[1,20]\times\{\text{schwarz}\}$ von U. Seine Wahrscheinlichkeit ist gleich

$$\mathrm{P}^U([1,20]\times\{\text{schwarz}\}) = \frac{|[1,20]\times\{\text{schwarz}\}|}{|U|} = \frac{20}{30} = \frac{2}{3}.$$

Die Menge $C = \{\text{rot}, \text{schwarz}\}$ wird zu einem endlichen Wahrscheinlichkeitsraum mit der Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}^C(B) = \begin{cases} 0 & \text{für } B = \emptyset, \\ \frac{1}{3} & \text{für } B = \{\text{rot}\}, \\ \frac{2}{3} & \text{für } B = \{\text{schwarz}\}, \\ 1 & \text{für } B = \{\text{rot}, \text{schwarz}\}. \end{cases}$$

In Anwendungsbeispiel (19.19) interessieren wir uns also nicht in erster Linie für Ereignisse im Wahrscheinlichkeitsraum U (auch wenn wir diese letzten Endes zur Berechnung der Wahrscheinlichkeiten benötigen), sondern für Elemente der Menge C, welcher sich ebenfalls als Wahrscheinlichkeitsraum auffassen lässt. Der Fokus auf das interessierende Merkmal lässt sich mit Hilfe einer Zufallsgröße modellieren:

(19.20) Definition (Zufallsgröße)**.** Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und eine Menge Y gegeben. Eine *Zufallsgröße* (oder *Zufallsvariable*) auf X mit *Werten* in Y (oder *Y-wertige Zufallsgröße* auf X oder *Y-wertige Zufallsvariable* auf X) ist eine Abbildung $f\colon X \to Y$.

(19.21) Beispiel. Die Abbildung $[1,6] \to [0,1]$, $x \mapsto x \bmod 2$ ist eine Zufallsgröße auf $[1,6]$ mit Werten in $[0,1]$.

(19.22) Anwendungsbeispiel.

(a) In einer Urne befinden sich zehn rote und 20 schwarze Kugeln. Es wird blind eine Kugel entnommen. Die möglichen (realen) Ergebnisse dieser Entnahme seien als (formale) Ergebnisse des Laplaceraums $U = [1,10]\times\{\text{rot}\} \dot\cup [1,20]\times\{\text{schwarz}\}$ modelliert. Die Farben der Kugeln seien als Elemente der Menge $\{\text{rot}, \text{schwarz}\}$ modelliert. Die Zuordnung der zugehörigen Farbe zu jeder Kugel in der Urne lässt sich als Zufallsgröße $a\colon U \to \{\text{rot}, \text{schwarz}\}$ gegeben durch $a(x, \text{rot}) = \text{rot}$ für $x \in [1,10]$ und $a(x, \text{schwarz}) = \text{schwarz}$ für $x \in [1,20]$ auffassen.

(b) Die möglichen (realen) Ergebnisse eines Würfelwurfs mit einem gewöhnlichen Würfel seien als (formale) Ergebnisse des Laplaceraums $[1,6]$ modelliert. Die Zuordnung der Parität zu jeder Augenzahl lässt sich als Zufallsgröße $p\colon [1,6] \to \{\text{gerade}, \text{ungerade}\}$ gegeben durch

$$p(x) = \begin{cases} \text{gerade} & \text{für } x \in \{2,4,6\}, \\ \text{ungerade} & \text{für } x \in \{1,3,5\}, \end{cases}$$

auffassen.

Der Sinn einer Zufallsgröße ist die Konstruktion einer Wahrscheinlichkeitsverteilung auf ihrer Zielmenge:

(19.23) Proposition. Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und eine Zufallsgröße $f\colon X \to Y$ gegeben. Dann wird Y ein quasiendlicher Wahrscheinlichkeitsraum $Y = Y_f$ mit Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}^{Y_f}(B) = \mathrm{P}^X(f^{-1}(B)) = \sum_{\substack{x\in X \\ f(x)\in B}} \mathrm{P}^X(x)$$

für jedes Ereignis B in Y_f.

Beweis. Es sei $Q\colon \mathrm{Pot}(Y) \to \mathbb{R}$, $B \mapsto \mathrm{P}(f^{-1}(B))$. Nach Proposition (19.9) gilt dann

$$Q(B) = \mathrm{P}(f^{-1}(B)) = \sum_{x\in f^{-1}(B)} \mathrm{P}(x) = \sum_{\substack{x\in X \\ f(x)\in B}} \mathrm{P}(x)$$

für $B \in \mathrm{Pot}(Y)$. Wir verifizieren die Axiome eines quasiendlichen Wahrscheinlichkeitsraums:

- *Nichtnegativität.* Für $B \in \operatorname{Pot}(Y)$ ist
$$Q(B) = \mathrm{P}(f^{-1}(B)) \geq 0.$$
- *Normiertheit.* Wegen $f^{-1}(Y) = X$ ist
$$Q(Y) = \mathrm{P}(f^{-1}(Y)) = \mathrm{P}(X) = 1.$$
- *Additivität.* Für disjunkte $B, B' \in \operatorname{Pot}(Y)$ sind $f^{-1}(B)$ und $f^{-1}(B')$ disjunkt und es gilt
$$\begin{aligned} Q(B \mathbin{\dot\cup} B') &= \mathrm{P}(f^{-1}(B \mathbin{\dot\cup} B')) = \mathrm{P}(f^{-1}(B) \mathbin{\dot\cup} f^{-1}(B')) = \mathrm{P}(f^{-1}(B)) + \mathrm{P}(f^{-1}(B')) \\ &= Q(B) + Q(B'). \end{aligned}$$
- *Endlichkeit und Normiertheit des Trägers.* Für $y \in Y$ mit $Q(\{y\}) > 0$ gilt
$$\sum_{\substack{x \in X \\ f(x)=y}} \mathrm{P}(x) = Q(\{y\}) > 0,$$
es gibt also insbesondere ein $x \in X$ mit $f(x) = y$ und $\mathrm{P}(x) > 0$. Folglich ist $\{y \in Y \mid Q(\{y\}) > 0\}$ eine Teilmenge von $\{f(x) \mid \mathrm{P}(x) > 0\} = f(\{x \in X \mid \mathrm{P}(x) > 0\})$. Als Bild der endlichen Teilmenge $\{x \in X \mid \mathrm{P}(x) > 0\}$ von X unter f ist aber $f(\{x \in X \mid \mathrm{P}(x) > 0\})$ endlich, also ist auch $\{y \in Y \mid Q(\{y\}) > 0\}$ endlich. Ferner gilt
$$\sum_{y \in Y} Q(\{y\}) = \sum_{y \in Y} \sum_{\substack{x \in X \\ f(x)=y}} \mathrm{P}(x) = \sum_{x \in X} \mathrm{P}(x) = 1.$$

Insgesamt wird Y ein quasiendlicher Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung $\mathrm{P}^Y = Q$. □

(19.24) Definition (durch Zufallsgröße induzierter Wahrscheinlichkeitsraum)**.** Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und eine Zufallsgröße $f\colon X \to Y$ gegeben. Der Wahrscheinlichkeitsraum $Y = Y_f$ aus Proposition (19.23) wird der durch f induzierte *Wahrscheinlichkeitsraum* genannt. Die Wahrscheinlichkeitsverteilung von Y_f wird auch *Wahrscheinlichkeitsverteilung* von f genannt und als $\mathrm{P}_f = \mathrm{P}_f^Y := \mathrm{P}^{Y_f}$ notiert.

(19.25) Beispiel. Der durch die Zufallsgröße $[1, 6] \to [0, 1]$, $x \mapsto x \bmod 2$ induzierte Wahrscheinlichkeitsraum ist der Laplaceraum mit Ergebnismenge $[0, 1]$.

Beweis. Es sei $r\colon [1, 6] \to [0, 1]$, $x \mapsto x \bmod 2$. Die von r induzierte Wahrscheinlichkeitsverteilung auf $[0, 1]$ erfüllt
$$\mathrm{P}(y) = \mathrm{P}(r^{-1}(\{y\})) = \left.\begin{cases} \mathrm{P}(\{2, 4, 6\}), & \text{falls } y = 0, \\ \mathrm{P}(\{1, 3, 5\}), & \text{falls } y = 1 \end{cases}\right\} = \frac{1}{2}$$
für jedes Ergebnis y von $[0, 1]$. □

(19.26) Anwendungsbeispiel.

(a) In einer Urne befinden sich zehn rote und 20 schwarze Kugeln. Es wird blind eine Kugel entnommen. Die möglichen (realen) Ergebnisse dieser Entnahme seien als (formale) Ergebnisse des Laplaceraums $U = [1, 10] \times \{\text{rot}\} \mathbin{\dot\cup} [1, 20] \times \{\text{schwarz}\}$ modelliert. Die Farben der Kugeln seien als Elemente der Menge $C = \{\text{rot}, \text{schwarz}\}$ modelliert. Die Zuordnung der zugehörigen Farbe zu jeder Kugel in der Urne sei als Zufallsgröße $a\colon U \to C$ gegeben durch $a(x, \text{rot}) = \text{rot}$ für $x \in [1, 10]$ und $a(x, \text{schwarz}) = \text{schwarz}$ für $x \in [1, 20]$ modelliert.

Die Wahrscheinlichkeitsverteilung des durch a induzierten Wahrscheinlichkeitsraums mit Ergebnismenge C ist nach Anwendungsbeispiel (19.19) gegeben durch
$$\mathrm{P}^C(B) = \mathrm{P}^U(a^{-1}(B)) = \begin{cases} 0 & \text{für } B = \emptyset, \\ \frac{1}{3} & \text{für } B = \{\text{rot}\}, \\ \frac{2}{3} & \text{für } B = \{\text{schwarz}\}, \\ 1 & \text{für } B = \{\text{rot}, \text{schwarz}\}. \end{cases}$$

(b) Die möglichen (realen) Ergebnisse eines Würfelwurfs mit einem gewöhnlichen Würfel seien als (formale) Ergebnisse des Laplaceraums $[1,6]$ modelliert. Paritäten seien als Elemente von $Q = \{\text{gerade}, \text{ungerade}\}$ modelliert. Die Zuordnung der Parität zu jeder Augenzahl sei als Zufallsgröße $p\colon [1,6] \to Q$ gegeben durch

$$p(x) = \begin{cases} \text{gerade} & \text{für } x \in \{2,4,6\}, \\ \text{ungerade} & \text{für } x \in \{1,3,5\}, \end{cases}$$

modelliert.

Der durch p induzierte Wahrscheinlichkeitsraum ist der Laplaceraum mit Ergebnismenge Q, vgl. Beispiel (19.25).

Alternativer Beweis von Beispiel (19.2)(c). Die von der Inklusion $\operatorname{inc}\colon \{0\} \to \mathbb{R}$, aufgefasst als Zufallsgröße auf dem Laplaceraum $\{0\}$, induzierte Wahrscheinlichkeitsverteilung auf $\mathbb{R}$ ist gegeben durch

$$\mathrm{P}(A) = \mathrm{P}(\operatorname{inc}^{-1}(A)) = \left.\begin{cases} \mathrm{P}(\{0\}), & \text{falls } 0 \in A, \\ \mathrm{P}(\emptyset), & \text{falls } 0 \notin A \end{cases}\right\} = \begin{cases} 1, & \text{falls } 0 \in A, \\ 0, & \text{falls } 0 \notin A, \end{cases}$$

für jedes Ereignis A von $\mathbb{R}$. □

Zufallsgrößen auf quasiendlichen Wahrscheinlichkeitsräume induzieren nach Proposition (19.23) die Struktur eines quasiendlichen Wahrscheinlichkeitsraums auf Ihrer Zielmenge. Umgekehrt liefert jeder quasiendliche Wahrscheinlichkeitsraum eine Zufallsgröße:

(19.27) Bemerkung. Es sei ein quasiendlicher Wahrscheinlichkeitsraum X gegeben. Dann ist die Identität $\mathrm{id}_X\colon X \to X$ eine Zufallsgröße auf X mit Werten in X. Die Wahrscheinlichkeitsverteilung des durch id_X induzierten Wahrscheinlichkeitsraums X_{id_X} ist die Wahrscheinlichkeitsverteilung von X.

(19.28) Bemerkung. Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und eine Zufallsgröße $f\colon X \to Y$ gegeben. Für $y \in Y \setminus \operatorname{Im} f$ ist

$$\mathrm{P}^Y(y) = 0.$$

Beweis. Für $y \in Y \setminus \operatorname{Im} f$ ist $f^{-1}(\{y\}) = \emptyset$, nach Korollar (19.5) also

$$\mathrm{P}^Y(y) = \mathrm{P}^X(f^{-1}(\{y\})) = \mathrm{P}^X(\emptyset) = 0.$$ □

Produktwahrscheinlichkeitsräume

Unabhängige Zufallsexperimente lassen sich mit Produkträumen modellieren.

(19.29) Proposition. Es seien eine endliche Menge I und eine Familie von quasiendlichen Wahrscheinlichkeitsräumen $(X_i)_{i\in I}$ über I gegeben. Dann wird $\bigtimes_{i\in I} X_i$ ein quasiendlicher Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}^{\bigtimes_{i\in I} X_i}(A) = \sum_{x\in A} \prod_{i\in I} \mathrm{P}^{X_i}(x_i)$$

für jedes Ereignis A in $\bigtimes_{i\in I} X_i$.

Beweis. Es sei $f\colon \bigtimes_{i\in I} X_i \to \mathbb{R},\ x \mapsto \prod_{i\in I} \mathrm{P}^{X_i}(x_i)$. Wir verifizieren die Bedingungen aus Proposition (19.10)(a):

- *Nichtnegativität.* Für $x \in \bigtimes_{i\in I} X_i$ ist $\mathrm{P}^{X_i}(x_i) \geq 0$ für jedes $i \in I$, also auch

$$f(x) = \prod_{i\in I} \mathrm{P}^{X_i}(x_i) \geq 0.$$

- *Endlichkeit des Trägers.* Für jedes $i \in I$ ist $\{x \in \bigtimes_{i\in I} X_i \mid \mathrm{P}^{X_i}(x_i) > 0\}$ endlich. Folglich ist auch

$$\{x \in \bigtimes_{i\in I} X_i \mid f(x) > 0\} = \{x \in \bigtimes_{i\in I} X_i \mid \prod_{i\in I} \mathrm{P}^{X_i}(x_i) > 0\} = \{x \in \bigtimes_{i\in I} X_i \mid \mathrm{P}^{X_i}(x_i) > 0 \text{ für } i \in I\}$$
$$= \bigcap_{i\in I} \{x \in \bigtimes_{i\in I} X_i \mid \mathrm{P}^{X_i}(x_i) > 0\}$$

  endlich.

- *Normiertheit.* Für jedes $i \in I$ ist $\sum_{x_i\in X_i} \mathrm{P}^{X_i}(x_i) = 1$. Folglich ist auch

$$\sum_{x\in\bigtimes_{i\in I} X_i} f(x) = \sum_{x\in\bigtimes_{i\in I} X_i} \prod_{i\in I} \mathrm{P}^{X_i}(x_i) = \prod_{i\in I} \sum_{x_i\in X_i} \mathrm{P}^{X_i}(x_i) = \prod_{i\in I} 1 = 1.$$

Nach Proposition (19.10)(a) wird $\bigtimes_{i\in I} X_i$ ein quasiendlicher Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}^{\bigtimes_{i\in I} X_i}(A) = \sum_{x\in A} f(x) = \sum_{x\in A} \prod_{i\in I} \mathrm{P}^{X_i}(x_i)$$

für jedes Ereignis A in $\bigtimes_{i\in I} X_i$. □

(19.30) Definition (Produktwahrscheinlichkeitsraum)**.** Es seien eine endliche Menge I und eine Familie von quasiendlichen Wahrscheinlichkeitsräumen $(X_i)_{i\in I}$ über I gegeben. Der Wahrscheinlichkeitsraum $\bigtimes_{i\in I} X_i$ mit der Wahrscheinlichkeitsverteilung aus Proposition (19.29) heißt *Produktwahrscheinlichkeitsraum* (oder *Produktraum* oder *Produkt von Wahrscheinlichkeitsräumen* oder *Produkt*) von $(X_i)_{i\in I}$.

(19.31) Beispiel. Es sei X der Laplaceraum mit Ergebnismenge $\{0, 1\}$ und Y der endliche Wahrscheinlichkeitsraum mit Ergebnismenge $\{0, 1\}$ und Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}(B) = \begin{cases} 0 & \text{für } B = \emptyset, \\ \frac{1}{4} & \text{für } B = \{0\}, \\ \frac{3}{4} & \text{für } B = \{1\}, \\ 1 & \text{für } B = \{0, 1\}. \end{cases}$$

(a) Der Produktraum $X \times X$ ist der Laplaceraum mit Ergebnismenge $\{0, 1\} \times \{0, 1\}$.

(b) Der Produktraum $Y \times Y$ ist ein Wahrscheinlichkeitsraum mit Ergebnismenge $\{0, 1\} \times \{0, 1\}$. Die Wahrscheinlichkeitsverteilung von $Y \times Y$ erfüllt

$$\mathrm{P}^{Y\times Y}(y_1, y_2) = \begin{cases} \frac{1}{16} & \text{für } (y_1, y_2) = (0, 0), \\ \frac{3}{16} & \text{für } (y_1, y_2) \in \{(1, 0), (0, 1)\}, \\ \frac{9}{16} & \text{für } (y_1, y_2) = (1, 1). \end{cases}$$

(c) Der Produktraum $X \times Y$ ist ein Wahrscheinlichkeitsraum mit Ergebnismenge $\{0, 1\} \times \{0, 1\}$. Die Wahrscheinlichkeitsverteilung von $Y \times Y$ erfüllt

$$\mathrm{P}^{X\times Y}(x, y) = \begin{cases} \frac{1}{8} & \text{für } (x, y) \in \{(0, 0), (1, 0)\}, \\ \frac{3}{8} & \text{für } (x, y) \in \{(0, 1), (1, 1)\}. \end{cases}$$

Beweis.

(a) Für $(x_1, x_2) \in X \times X$ gilt

$$\mathrm{P}^{X\times X}(x_1, x_2) = \mathrm{P}^X(x_1)\,\mathrm{P}^X(x_2) = \frac{1}{|X|} \cdot \frac{1}{|X|} = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} = \frac{1}{|X \times X|}.$$

Nach Bemerkung (19.14) ist daher $X \times X$ ein Laplaceraum.

(b) Für $(y_1, y_2) \in Y \times Y$ gilt

$$\mathrm{P}^{Y\times Y}(y_1, y_2) = \mathrm{P}^Y(y_1)\,\mathrm{P}^Y(y_2) = \left\{\begin{array}{ll} \frac{1}{4}\cdot\frac{1}{4}, & \text{falls } (y_1, y_2) = (0,0), \\ \frac{3}{4}\cdot\frac{1}{4}, & \text{falls } (y_1, y_2) = (1,0), \\ \frac{1}{4}\cdot\frac{3}{4}, & \text{falls } (y_1, y_2) = (0,1), \\ \frac{3}{4}\cdot\frac{3}{4}, & \text{falls } (y_1, y_2) = (1,1) \end{array}\right\}$$

$$= \begin{cases} \frac{1}{16}, & \text{falls } (y_1, y_2) = (0,0), \\ \frac{3}{16}, & \text{falls } (y_1, y_2) \in \{(1,0),(0,1)\}, \\ \frac{9}{16}, & \text{falls } (y_1, y_2) = (1,1). \end{cases}$$

(c) Für $(x, y) \in X \times Y$ gilt

$$\mathrm{P}^{X\times Y}(x, y) = \mathrm{P}^X(x)\,\mathrm{P}^Y(y) = \left\{\begin{array}{ll} \frac{1}{2}\cdot\frac{1}{4}, & \text{falls } (x, y) = (0,0), \\ \frac{1}{2}\cdot\frac{1}{4}, & \text{falls } (x, y) = (1,0), \\ \frac{1}{2}\cdot\frac{3}{4}, & \text{falls } (x, y) = (0,1), \\ \frac{1}{2}\cdot\frac{3}{4}, & \text{falls } (x, y) = (1,1) \end{array}\right\}$$

$$= \begin{cases} \frac{1}{8}, & \text{falls } (x, y) \in \{(0,0),(1,0)\}, \\ \frac{3}{8}, & \text{falls } (y_1, y_2) \in \{(0,1),(1,1)\}. \end{cases}$$

□

(19.32) Bemerkung. Es seien eine endliche Menge I und eine Familie von Laplaceräumen $(X_i)_{i\in I}$ über I gegeben. Dann ist $\times_{i\in I} X_i$ ebenfalls ein Laplaceraum und für jedes Ereignis A von $\times_{i\in I} X_i$ gilt

$$\mathrm{P}(A) = \frac{|A|}{\prod_{i\in I} |X_i|}$$

Beweis. Für jedes Ergebnis x von $\times_{i\in I} X_i$ gilt

$$\mathrm{P}(x) = \prod_{i\in I} \mathrm{P}(x_i) = \prod_{i\in I} \frac{1}{|X_i|} = \frac{1}{\prod_{i\in I} |X_i|} = \frac{1}{|\times_{i\in I} X_i|}.$$

Nach Bemerkung (19.14) ist daher $\times_{i\in I} X_i$ ein Laplaceraum. Für jedes Ereignis A von $\times_{i\in I} X_i$ gilt somit

$$\mathrm{P}(A) = \frac{|A|}{|\times_{i\in I} X_i|} = \frac{|A|}{\prod_{i\in I} |X_i|}.$$

□

(19.33) Anwendungsbeispiel. Die möglichen (realen) Ergebnisse eines Würfelwurfs mit zwei gewöhnlichen Würfeln seien als (formale) Ergebnisse des Produktraums $[1,6] \times [1,6]$ modelliert.
Das (reale) Ereignis, dass die Würfel nach dem Wurf einen Pasch zeigen, entspricht dem (formalen) Ereignis

$$A = \{(x, x) \mid x \in [1,6]\} = \{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6)\}$$

von $[1,6] \times [1,6]$. Seine Wahrscheinlichkeit ist nach Bemerkung (19.32) gleich

$$\mathrm{P}(A) = \frac{|A|}{|[1,6]| \cdot |[1,6]|} = \frac{6}{6\cdot 6} = \frac{1}{6}.$$

Bedingte Wahrscheinlichkeit

Wissen wir, dass bei einem Zufallsexperiment ein gewisses Ereignis eintritt, so legen wir die Wahrscheinlichkeiten für die unter dieser Annahme noch möglichen Ereignisse durch geeignete Einschränkung auf das eintretende Ereignis fest, d.h. wir „normieren“ mit der Wahrscheinlichkeit des eintretenden Ereignisses:

(19.34) Proposition. Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und ein Ereignis B von X mit $\mathrm{P}^X(B) > 0$ gegeben. Dann wird B ein quasiendlicher Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsverteilung gegeben durch

$$\mathrm{P}^B(A) = \frac{\mathrm{P}^X(A)}{\mathrm{P}^X(B)}$$

für jedes Ereignis A in B.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(19.35) Definition (durch Einschränkung gegebener Wahrscheinlichkeitsraum)**.** Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und ein Ereignis B von X mit $\mathrm{P}^X(B) > 0$ gegeben. Der Wahrscheinlichkeitsraum B aus Proposition (19.34) wird der durch *Restriktion* (oder durch *Einschränkung*) auf B gegebene *Wahrscheinlichkeitsraum* genannt. Die Wahrscheinlichkeitsverteilung von B wird auch durch *Restriktion* (oder durch *Einschränkung*) auf B gegebene *Wahrscheinlichkeitsverteilung* genannt.

(19.36) Beispiel. Es sei X der Laplaceraum mit Ergebnismenge $[1, 5]$ und es sei B das Ereignis von X gegeben durch

$$B = \{x \in X \mid x \text{ ist ungerade}\}.$$

Dann ist die Wahrscheinlichkeit des Ergebnisses 3 im durch Einschränkung gegebenen Wahrscheinlichkeitsraum B gleich

$$\mathrm{P}^B(3) = \frac{1}{3}.$$

Beweis. Die Anzahl der Ergebnisse von X ist gleich $|X| = 5$. Wegen $B = \{1, 3, 5\}$ ist $|B| = 3$, die Wahrscheinlichkeit von B in X also gleich

$$\mathrm{P}^X(B) = \frac{|B|}{|X|} = \frac{3}{5}.$$

Folglich ist die Wahrscheinlichkeit von 3 in B gleich

$$\mathrm{P}^B(3) = \frac{\mathrm{P}^X(3)}{\mathrm{P}^X(B)} = \frac{\frac{1}{5}}{\frac{3}{5}} = \frac{1}{3}.$$ □

(19.37) Bemerkung. Es seien ein Laplaceraum X und ein Ereignis B von X mit $\mathrm{P}^X(B) > 0$ gegeben. Dann ist der durch Einschränkung gegebene Wahrscheinlichkeitsraum B ein Laplaceraum.

Beweis. Für jedes Ereignis A in B gilt

$$\mathrm{P}^B(A) = \frac{\mathrm{P}^X(A)}{\mathrm{P}^X(B)} = \frac{\frac{|A|}{|X|}}{\frac{|B|}{|X|}} = \frac{|A|}{|B|}.$$

Folglich ist B ein Laplaceraum. □

Alternativer Beweis von Beispiel (19.36). Wegen $B = \{1, 3, 5\}$ ist

$$\mathrm{P}^B(3) = \frac{1}{|B|} = \frac{1}{3}$$

nach Bemerkung (19.37). □

(19.38) Anwendungsbeispiel. Die möglichen (realen) Ergebnisse eines Würfelwurfs mit zwei gewöhnlichen Würfeln seien als (formale) Ergebnisse des Produktraums $[1, 6]_{\text{Laplace}} \times [1, 6]_{\text{Laplace}}$ modelliert. Das (reale) Ereignis, dass die Würfel nach dem Wurf einen Pasch zeigen, entspricht dem (formalen) Ereignis

$$B = \{(x, x) \mid x \in [1, 6]\} = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\}$$

von X. Das (reale) Ergebnis, dass die Würfel nach dem Wurf einen Sechserpasch zeigen, entspricht dem (formalen) Ergebnis $(6, 6)$ von X. Unter der Bedingung, dass die Würfel nach dem Wurf einen Pasch zeigen, ist die Wahrscheinlichkeit dafür, dass sie einen Sechserpasch zeigen, nach Bemerkung (19.37) gleich

$$\mathrm{P}^B(6, 6) = \frac{1}{|B|} = \frac{1}{6}.$$

Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und ein Ereignis B von X mit $\mathrm{P}(B) > 0$ gegeben, so dass B durch Restriktion zu einem Wahrscheinlichkeitsraum wird. Die Inklusion $\mathrm{inc}\colon B \to X$ ist dann eine Zufallsgröße auf B mit Werten in X, induziert ihrerseits also eine Wahrscheinlichkeitsverteilung auf X:

(19.39) Definition (bedingte Wahrscheinlichkeit)**.** Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und ein Ereignis B von X mit $\mathrm{P}(B) > 0$ gegeben, und es bezeichne $\mathrm{inc}\colon B \to X$ die Inklusion von B in X. Der durch die Inklusion $\mathrm{inc}\colon B \to X$, aufgefasst als Zufallsgröße auf dem durch Restriktion gegebenen Wahrscheinlichkeitsraum B mit Werten in X, induzierte Wahrscheinlichkeitsraum $X_B := X_{\mathrm{inc}}$ wird der durch B *induzierte Wahrscheinlichkeitsraum* genannt. Die Wahrscheinlichkeitsverteilung von X_B wird auch *bedingte Wahrscheinlichkeitsverteilung* von X unter (der *Bedingung*) B genannt und als $\mathrm{P}(- \mid B) = \mathrm{P}^X(- \mid B) := \mathrm{P}^{X_B}$ notiert. Für jedes Ereignis A von X wird $\mathrm{P}(A \mid B)$ die *bedingte Wahrscheinlichkeit* von A in X unter (der *Bedingung*) B genannt.

Die bedingte Wahrscheinlichkeitsverteilung $\mathrm{P}^X(- \mid B)\colon \mathrm{Pot}(X) \to \mathbb{R}$ auf einem quasiendlichen Wahrscheinlichkeitsraum X unter einem bedingenden Ereignis B von X mit $\mathrm{P}(B) > 0$ entspricht einer Erweiterung der durch Restriktion gegebenen Wahrscheinlichkeitsverteilung $\mathrm{P}^B\colon \mathrm{Pot}(B) \to \mathbb{R}$ auf beliebige Ereignisse von X:

(19.40) Bemerkung. Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und ein Ereignis B von X mit $\mathrm{P}(B) > 0$ gegeben. Für jedes Ereignis A in X ist

$$\mathrm{P}(A \mid B) = \frac{\mathrm{P}(A \cap B)}{\mathrm{P}(B)}.$$

Beweis. Es bezeichne $\mathrm{inc}\colon B \to X$ die Inklusion. Für jedes Ereignis A von X ist dann

$$\mathrm{inc}^{-1}(A) = \{x \in B \mid \mathrm{inc}(x) \in A\} = \{x \in B \mid x \in A\} = A \cap B,$$

also

$$\mathrm{P}^X(A \mid B) = \mathrm{P}^{X_B}(A) = \mathrm{P}^{X_{\mathrm{inc}_B}}(A) = \mathrm{P}^B(\mathrm{inc}^{-1}(A)) = \mathrm{P}^B(A \cap B) = \frac{\mathrm{P}^X(A \cap B)}{\mathrm{P}^X(B)}.$$ □

(19.41) Korollar. Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und ein Ereignis B von X mit $\mathrm{P}(B) > 0$ gegeben. Jedes Ereignis A in B ist ein Ereignis in X und es gilt

$$\mathrm{P}^B(A) = \mathrm{P}^X(A \mid B).$$

Beweis. Es sei ein Ereignis A in B gegeben. Dann ist A eine Teilmenge von B und B eine Teilmenge von X, also auch A eine Teilmenge von X, d.h. A ist ein Ereignis in X. Nach Bemerkung (19.40) gilt ferner

$$\mathrm{P}^X(A \mid B) = \frac{\mathrm{P}^X(A \cap B)}{\mathrm{P}^X(B)} = \frac{\mathrm{P}^X(A)}{\mathrm{P}^X(B)} = \mathrm{P}^B(A).$$ □

(19.42) Beispiel. Es seien Ereignisse A und B des Laplaceraums $[1, 5]$ gegeben durch

$$A = \{x \in X \mid x \geq 3\},$$
$$B = \{x \in X \mid x \text{ ist ungerade}\}.$$

Dann ist die bedingte Wahrscheinlichkeit von A unter der Bedingung B gleich

$$\mathrm{P}(A \mid B) = \frac{2}{3}.$$

Beweis. Die Anzahl der Ergebnisse von X ist gleich $|X| = 5$. Wegen $B = \{1, 3, 5\}$ ist

$$\mathrm{P}(B) = \frac{|B|}{|X|} = \frac{3}{5}$$

und wegen $A \cap B = \{x \in B \mid x \geq 3\} = \{3, 5\}$ ist

$$\mathrm{P}(A \cap B) = \frac{|A \cap B|}{|X|} = \frac{2}{5}.$$

Nach Bemerkung (19.40) folgt

$$\mathrm{P}(A \mid B) = \frac{\mathrm{P}(A \cap B)}{\mathrm{P}(B)} = \frac{\frac{2}{5}}{\frac{3}{5}} = \frac{2}{3}.$$ □

(19.43) Bemerkung. Es seien ein Laplaceraum X und ein Ereignis B von X mit $\mathrm{P}^X(B) > 0$ gegeben. Für jedes Ereignis A in X gilt

$$\mathrm{P}(A \mid B) = \frac{|A \cap B|}{|B|}.$$

Beweis. Für jedes Ereignis A in X gilt

$$\mathrm{P}(A \mid B) = \frac{\mathrm{P}(A \cap B)}{\mathrm{P}(B)} = \frac{\frac{|A \cap B|}{|X|}}{\frac{|B|}{|X|}} = \frac{|A \cap B|}{|B|}.$$ □

Alternativer Beweis von Beispiel (19.42). Wegen $B = \{1, 3, 5\}$ und $A \cap B = \{x \in B \mid x \geq 3\} = \{3, 5\}$ ist

$$\mathrm{P}(A \mid B) = \frac{|A \cap B|}{|B|} = \frac{2}{3}$$

nach Bemerkung (19.43). □

(19.44) Anwendungsbeispiel. Die möglichen (realen) Ergebnisse eines Würfelwurfs mit zwei gewöhnlichen Würfeln seien als (formale) Ergebnisse des Produktraums

$$X = [1, 6]_{\mathrm{Laplace}} \times [1, 6]_{\mathrm{Laplace}}$$

modelliert. Das (reale) Ereignis, dass die Würfel nach dem Wurf einen Pasch zeigen, entspricht dem (formalen) Ereignis

$$B = \{(x, x) \mid x \in [1, 6]\} = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\}$$

von X. Das (reale) Ereignis, dass (mindestens) einer der beiden Würfel eine gerade Augenzahl zeigt, entspricht dem formalen Ereignis

$$\begin{aligned} A &= (\{x \in [1, 6] \mid x \text{ ist gerade}\} \times [1, 6]) \cup ([1, 6] \times \{y \in [1, 6] \mid y \text{ ist gerade}\}) \\ &= (\{2, 4, 6\} \times [1, 6]) \cup ([1, 6] \times \{2, 4, 6\}) \end{aligned}$$

von X. Wegen

$$A \cap B = \{(2, 2), (4, 4), (6, 6)\}$$

ist

$$\mathrm{P}(A \mid B) = \frac{|A \cap B|}{|B|} = \frac{3}{6} = \frac{1}{2}$$

nach Bemerkung (19.32) und Bemerkung (19.43).

(19.45) Bemerkung (Satz von Bayes)**.** Es sei ein quasiendlicher Wahrscheinlichkeitsraum X gegeben. Für alle Ereignisse A und B von X mit $\mathrm{P}(A) > 0$ und $\mathrm{P}(B) > 0$ gilt

$$\mathrm{P}(A)\,\mathrm{P}(B \mid A) = \mathrm{P}(A \mid B)\,\mathrm{P}(B).$$

Beweis. Für alle Ereignisse A und B von X mit $\mathrm{P}(A) > 0$ und $\mathrm{P}(B) > 0$ gilt

$$\mathrm{P}(A)\,\mathrm{P}(B \mid A) = \mathrm{P}(B \cap A) = \mathrm{P}(A \cap B) = \mathrm{P}(A \mid B)\,\mathrm{P}(B)$$

nach Bemerkung (19.40). □

Auswahlmodelle als Wahrscheinlichkeitsräume

Wir wenden unsere bisherigen Konzepte an, um die kombinatorischen Auswahlmodelle aus Abschnitt 18 als Wahrscheinlichkeitsräume aufzufassen:

(19.46) Konvention. Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und eine endliche Menge I gegeben.

(a) Wir fassen $\mathrm{Var}_I(X) = X^I = \times_{i\in I} X$ als Produktwahrscheinlichkeitsraum von $(X)_{i\in I}$ auf.

(b) Es sei $\mathrm{P}^{\mathrm{Var}_I(X)}(\mathrm{Perm}_I(X)) > 0$. Wir fassen $\mathrm{Perm}_I(X)$ als durch Restriktion gegebenen Wahrscheinlichkeitsraum auf.

(c) Wir fassen $\mathrm{MComb}_I(X)$ als durch $\mathrm{quo}\colon \mathrm{Var}_I(X) \to \mathrm{MComb}_I(X)$, $x \mapsto [x]$ induzierten Wahrscheinlichkeitsraum auf.

(d) Es sei $\mathrm{P}^{\mathrm{Var}_I(X)}(\mathrm{Perm}_I(X)) > 0$. Wir fassen $\mathrm{Comb}_I(X)$ als durch $\mathrm{quo}\colon \mathrm{Perm}_I(X) \to \mathrm{Comb}_I(X)$, $x \mapsto [x]$ induzierten Wahrscheinlichkeitsraum auf.

(19.47) Bemerkung. Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und eine endliche Menge I gegeben.

(a) Für jedes Ereignis A von $\mathrm{Var}_I(X)$ ist

$$\mathrm{P}^{\mathrm{Var}_I(X)}(A) = \sum_{x\in A}\prod_{i\in I}\mathrm{P}^X(x_i) = \sum_{x\in A}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_x(y)}.$$

(b) Es gebe ein $x \in \mathrm{Perm}_I(X)$ mit $\prod_{i\in I}\mathrm{P}^X(x_i) > 0$. Für jedes Ereignis A von $\mathrm{Perm}_I(X)$ ist

$$\mathrm{P}^{\mathrm{Perm}_I(X)}(A) = \frac{\sum_{x\in A}\prod_{i\in I}\mathrm{P}^X(x_i)}{\sum_{x\in\mathrm{Perm}_I(X)}\prod_{i\in I}\mathrm{P}^X(x_i)} = \frac{\sum_{x\in A}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_x(y)}}{\sum_{x\in\mathrm{Perm}_I(X)}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_x(y)}}.$$

(c) Für jedes Ereignis B von $\mathrm{MComb}_I(X)$ ist

$$\mathrm{P}^{\mathrm{MComb}_I(X)}(B) = \sum_{C\in B}\sum_{x\in C}\prod_{i\in I}\mathrm{P}^X(x_i) = \sum_{C\in B}|C|\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)}.$$

(d) Es gebe ein $x \in \mathrm{Perm}_I(X)$ mit $\prod_{i\in I}\mathrm{P}^X(x_i) > 0$. Für jedes Ereignis B von $\mathrm{Comb}_I(X)$ ist

$$\mathrm{P}^{\mathrm{Comb}_I(X)}(B) = \frac{\sum_{C\in B}\sum_{x\in C}\prod_{i\in I}\mathrm{P}^X(x_i)}{\sum_{C\in\mathrm{Comb}_I(X)}\sum_{x\in C}\prod_{i\in I}\mathrm{P}^X(x_i)} = \frac{\sum_{C\in B}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)}}{\sum_{C\in\mathrm{Comb}_I(X)}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)}}.$$

Beweis.

(a) Die Wahrscheinlichkeitsverteilung von $\mathrm{Var}_I(X) = X^I = \times_{i\in I} X$ ist nach Proposition (19.29) gegeben durch

$$\mathrm{P}^{\mathrm{Var}_I(X)}(A) = \mathrm{P}^{\times_{i\in I}X}(A) = \sum_{x\in A}\prod_{i\in I}\mathrm{P}^X(x_i) = \sum_{x\in A}\prod_{y\in X}\prod_{\substack{i\in I\\ x_i=y}}\mathrm{P}^X(y) = \sum_{x\in A}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_x(y)}$$

für jedes Ereignis A von $\mathrm{Var}_I(X)$.

(b) Nach Proposition (19.9) und (a) ist

$$\mathrm{P}^{\mathrm{Var}_I(X)}(\mathrm{Perm}_I(X)) = \sum_{x\in\mathrm{Perm}_I(X)}\mathrm{P}^{\mathrm{Var}_I(X)}(x) = \sum_{x\in\mathrm{Perm}_I(X)}\prod_{i\in I}\mathrm{P}^X(x_i) > 0.$$

Nach Proposition (19.34) und (a) folgt

$$\mathrm{P}^{\mathrm{Perm}_I(X)}(A) = \frac{\mathrm{P}^{\mathrm{Var}_I(X)}(A)}{\mathrm{P}^{\mathrm{Var}_I(X)}(\mathrm{Perm}_I(X))} = \frac{\sum_{x\in A}\prod_{i\in I}\mathrm{P}^X(x_i)}{\sum_{x\in\mathrm{Perm}_I(X)}\prod_{i\in I}\mathrm{P}^X(x_i)}$$

$$= \frac{\sum_{x\in A}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_x(y)}}{\sum_{x\in \mathrm{Perm}_I(X)}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_x(y)}}$$

für jedes Ereignis A von $\mathrm{Perm}_I(X)$.

(c) Nach Proposition (19.23) und (a) gilt

$$\begin{aligned}\mathrm{P}^{\mathrm{MComb}_I(X)}(B) &= \sum_{\substack{x\in\mathrm{Var}_I(X)\\ \mathrm{quo}(x)\in B}} \mathrm{P}^{\mathrm{Var}_I(X)}(x) = \sum_{\substack{x\in\mathrm{Var}_I(X)\\ [x]\in B}} \mathrm{P}^{\mathrm{Var}_I(X)}(x) = \sum_{C\in B}\sum_{\substack{x\in\mathrm{Var}_I(X)\\ [x]=C}} \mathrm{P}^{\mathrm{Var}_I(X)}(x)\\ &= \sum_{C\in B}\sum_{x\in C}\mathrm{P}^{\mathrm{Var}_I(X)}(x) = \sum_{C\in B}\sum_{x\in C}\prod_{i\in I}\mathrm{P}^X(x_i) = \sum_{C\in B}\sum_{x\in C}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_x(y)}\\ &= \sum_{C\in B}\sum_{x\in C}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)} = \sum_{C\in B}|C|\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)}\end{aligned}$$

(d) Nach Proposition (19.23), (b) und (a) und Korollar (18.61) gilt

$$\begin{aligned}\mathrm{P}^{\mathrm{Comb}_I(X)}(B) &= \sum_{\substack{x\in\mathrm{Perm}_I(X)\\ \mathrm{quo}(x)\in B}} \mathrm{P}^{\mathrm{Perm}_I(X)}(x) = \sum_{\substack{x\in\mathrm{Perm}_I(X)\\ [x]\in B}} \mathrm{P}^{\mathrm{Perm}_I(X)}(x) = \sum_{C\in B}\sum_{\substack{x\in\mathrm{Perm}_I(X)\\ [x]=C}} \mathrm{P}^{\mathrm{Perm}_I(X)}(x)\\ &= \sum_{C\in B}\sum_{x\in C}\mathrm{P}^{\mathrm{Perm}_I(X)}(x) = \sum_{C\in B}\sum_{x\in C}\frac{\prod_{i\in I}\mathrm{P}^X(x_i)}{\sum_{y\in\mathrm{Perm}_I(X)}\prod_{i\in I}\mathrm{P}^X(y_i)}\\ &= \frac{\sum_{C\in B}\sum_{x\in C}\prod_{i\in I}\mathrm{P}^X(x_i)}{\sum_{C\in\mathrm{Comb}_I(X)}\sum_{x\in C}\prod_{i\in I}\mathrm{P}^X(x_i)} = \frac{\sum_{C\in B}\sum_{x\in C}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_x(y)}}{\sum_{C\in\mathrm{Comb}_I(X)}\sum_{x\in C}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_x(y)}}\\ &= \frac{\sum_{C\in B}\sum_{x\in C}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)}}{\sum_{C\in\mathrm{Comb}_I(X)}\sum_{x\in C}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)}} = \frac{\sum_{C\in B}|C|\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)}}{\sum_{C\in\mathrm{Comb}_I(X)}|C|\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)}}\\ &= \frac{\sum_{C\in B}|I|!\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)}}{\sum_{C\in\mathrm{Comb}_I(X)}|I|!\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)}} = \frac{|I|!\sum_{C\in B}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)}}{|I|!\sum_{C\in\mathrm{Comb}_I(X)}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)}}\\ &= \frac{\sum_{C\in B}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)}}{\sum_{C\in\mathrm{Comb}_I(X)}\prod_{y\in X}(\mathrm{P}^X(y))^{\mu_C(y)}}\end{aligned}$$

für jedes Ereignis B von $\mathrm{Comb}_I(X)$. □

(19.48) Beispiel.

(a) Es sei X der Laplaceraum mit Ergebnismenge $\{0,1\}$.

(i) Für $x\in\mathrm{Var}_3(X)$ ist

$$\mathrm{P}^{\mathrm{Var}_3(X)}(x) = \frac{1}{8}.$$

(ii) Für $C\in\mathrm{MComb}_3(X)$ ist

$$\mathrm{P}^{\mathrm{MComb}_3(X)}(C) = \begin{cases}\frac{1}{8}, & \text{falls } C\in\{[0,0,0],[1,1,1]\},\\ \frac{3}{8}, & \text{falls } C\in\{[0,0,1],[0,1,1]\}.\end{cases}$$

(b) Es sei X der endliche Wahrscheinlichkeitsraum mit Ergebnismenge $\{0,1\}$ und

$$\mathrm{P}(y) = \begin{cases}\frac{1}{4} & \text{für } y=0,\\ \frac{3}{4} & \text{für } y=1.\end{cases}$$

(i) Für $x\in\mathrm{Var}_3(X)$ ist

$$\mathrm{P}^{\mathrm{Var}_3(X)}(x) = \begin{cases}\frac{1}{64}, & \text{falls } x\in\{(0,0,0)\},\\ \frac{3}{64}, & \text{falls } x\in\{(1,0,0),(0,1,0),(0,0,1)\},\\ \frac{9}{64}, & \text{falls } x\in\{(1,1,0),(1,0,1),(0,1,1)\},\\ \frac{27}{64}, & \text{falls } x\in\{(1,1,1)\}.\end{cases}$$

(ii) Für $C \in \mathrm{MComb}_3(X)$ ist

$$\mathrm{P}^{\mathrm{MComb}_3(X)}(C) = \begin{cases} \frac{1}{64}, & \text{falls } C \in \{[0,0,0]\}, \\ \frac{9}{64}, & \text{falls } C \in \{[0,0,1]\}, \\ \frac{27}{64}, & \text{falls } C \in \{[0,1,1],[1,1,1]\}. \end{cases}$$

Beweis.

(a) (i) Nach Bemerkung (19.47)(a) ist

$$\mathrm{P}^{\mathrm{Var}_3(X)}(x) = \prod_{i\in[1,3]} \mathrm{P}^X(x_i) = \prod_{i\in[1,3]} \frac{1}{2} = \frac{1}{8}.$$

für $x \in \mathrm{Var}_3(X)$.

(ii) Nach Proposition (19.23) und (i) ist

$$\mathrm{P}^{\mathrm{MComb}_3(X)}(C) = \sum_{\substack{x\in\mathrm{Var}_I(X)\\ [x]=C}} \mathrm{P}^{\mathrm{Var}_3(X)}(x) = \sum_{x\in C} \frac{1}{8} = \frac{|C|}{8} = \begin{cases} \frac{1}{8}, & \text{falls } C \in \{[0,0,0],[1,1,1]\}, \\ \frac{3}{8}, & \text{falls } C \in \{[0,0,1],[0,1,1]\}, \end{cases}$$

für $C \in \mathrm{MComb}_3(X)$.

(b) (i) Nach Bemerkung (19.47)(a) ist

$$\begin{aligned} \mathrm{P}^{\mathrm{Var}_3(X)}(x) &= \prod_{y\in X} (\mathrm{P}^X(y))^{\mu_x(y)} = (\mathrm{P}^X(0))^{\mu_x(0)} (\mathrm{P}^X(1))^{\mu_x(1)} = (\frac{1}{4})^{\mu_x(0)} (\frac{3}{4})^{\mu_x(1)} \\ &= \left.\begin{cases} (\frac{1}{4})^3 (\frac{3}{4})^0, & \text{falls } \mu_x(0)=3,\ \mu_x(1)=0, \\ (\frac{1}{4})^2 (\frac{3}{4})^1, & \text{falls } \mu_x(0)=2,\ \mu_x(1)=1, \\ (\frac{1}{4})^1 (\frac{3}{4})^2, & \text{falls } \mu_x(0)=1,\ \mu_x(1)=2, \\ (\frac{1}{4})^0 (\frac{3}{4})^3, & \text{falls } \mu_x(0)=0,\ \mu_x(1)=3 \end{cases}\right\} \\ &= \begin{cases} \frac{1}{64}, & \text{falls } x \in \{(0,0,0)\}, \\ \frac{3}{64}, & \text{falls } x \in \{(1,0,0),(0,1,0),(0,0,1)\}, \\ \frac{9}{64}, & \text{falls } x \in \{(1,1,0),(1,0,1),(0,1,1)\}, \\ \frac{27}{64}, & \text{falls } x \in \{(1,1,1)\}, \end{cases} \end{aligned}$$

für $x \in \mathrm{Var}_3(X)$.

(ii) Nach Proposition (19.23) und (i) ist

$$\begin{aligned} \mathrm{P}^{\mathrm{MComb}_3(X)}(C) &= \sum_{\substack{x\in\mathrm{Var}_I(X)\\ [x]=C}} \mathrm{P}^{\mathrm{Var}_3(X)}(x) = \sum_{x\in C} \mathrm{P}^{\mathrm{Var}_3(X)}(x) = \left.\begin{cases} \frac{1}{64}, & \text{falls } C=[0,0,0], \\ 3\cdot\frac{3}{64}, & \text{falls } C=[0,0,1], \\ 3\cdot\frac{9}{64}, & \text{falls } C=[0,1,1], \\ \frac{27}{64}, & \text{falls } C=[1,1,1] \end{cases}\right\} \\ &= \begin{cases} \frac{1}{64}, & \text{falls } C \in \{[0,0,0]\}, \\ \frac{9}{64}, & \text{falls } C \in \{[0,0,1]\}, \\ \frac{27}{64}, & \text{falls } C \in \{[0,1,1],[1,1,1]\}, \end{cases} \end{aligned}$$

für $C \in \mathrm{MComb}_3(X)$. □

(19.49) Bemerkung. Es seien $n \in \mathbb{N}$, $k \in \mathbb{N}_0$, ein Laplaceraum X mit $|X| = n$ und eine k-elementige Menge I gegeben.

(a) Der endliche Wahrscheinlichkeitsraum $\mathrm{Var}_I(X)$ ist ein Laplaceraum.

(b) Es gelte $k \leq n$. Dann ist $\mathrm{Perm}_I(X)$ ein Laplaceraum.

(c) Es gelte $k \leq n$. Dann ist $\mathrm{Comb}_I(X)$ ein Laplaceraum.

Beweis.

(a) Dies folgt aus Bemerkung (19.32).

(b) Wegen $k \leq n$ ist $\mathrm{Perm}_I(X) \neq \emptyset$, nach (a) gilt also $\mathrm{P}^{\mathrm{Var}_I(X)}(\mathrm{Perm}_I(X)) = \frac{|\mathrm{Perm}_I(X)|}{|\mathrm{Var}_I(X)|} > 0$. Nach Bemerkung (19.37) und (a) ist $\mathrm{Perm}_I(X)$ ein Laplaceraum.

(c) Für alle $C \in \mathrm{Comb}_I(X)$ gilt

$$\prod_{y \in X} (\mathrm{P}^X(y))^{\mu_C(y)} = \prod_{y \in X} (\frac{1}{n})^{\mu_C(y)} = (\frac{1}{n})^{\sum_{y \in X} \mu_C(y)} = (\frac{1}{n})^k = \frac{1}{n^k}.$$

Nach Bemerkung (19.47)(d) ist also

$$\begin{aligned} \mathrm{P}^{\mathrm{Comb}_I(X)}(B) &= \frac{\sum_{C \in B} \prod_{y \in X} (\mathrm{P}^X(y))^{\mu_C(y)}}{\sum_{C \in \mathrm{Comb}_I(X)} \prod_{y \in X} (\mathrm{P}^X(y))^{\mu_C(y)}} = \frac{\sum_{C \in B} \frac{1}{n^k}}{\sum_{C \in \mathrm{Comb}_I(X)} \frac{1}{n^k}} = \frac{|B| \frac{1}{n^k}}{|\mathrm{Comb}_I(X)| \frac{1}{n^k}} \\ &= \frac{|B|}{|\mathrm{Comb}_I(X)|} \end{aligned}$$

für jedes Ereignis B von $\mathrm{Comb}_I(X)$. Folglich ist $\mathrm{Comb}_I(X)$ ein Laplaceraum. □

Alternativer Beweis.

(c) Für jedes Ergebnis C von $\mathrm{Comb}_I(X)$ gilt

$$\begin{aligned} \mathrm{P}^{\mathrm{Comb}_I(X)}(C) &= \sum_{\substack{x \in \mathrm{Perm}_I(X) \\ \mathrm{quo}(x) = C}} \mathrm{P}^{\mathrm{Perm}_I(X)}(x) = \sum_{\substack{x \in \mathrm{Perm}_I(X) \\ [x] = C}} \frac{1}{|\mathrm{Perm}_I(X)|} = \sum_{x \in C} \frac{1}{|\mathrm{Perm}_I(X)|} \\ &= \frac{|C|}{|\mathrm{Perm}_I(X)|} = \frac{k!}{\prod_{i \in [1,k]} (n - i + 1)} = \frac{1}{|\mathrm{Comb}_I(X)|} \end{aligned}$$

nach Proposition (19.23) und (b), Korollar (18.61), Korollar (18.31) und Korollar (18.62). Nach Bemerkung (19.14) ist daher $\mathrm{Comb}_I(X)$ ein Laplaceraum. □

Nach Beispiel (19.48)(a)(ii) ist $\mathrm{MComb}_I(X)$ für einen Laplaceraum X und eine endliche Menge I im Allgemeinen kein Laplaceraum. Stattdessen erhalten wir:

(19.50) Bemerkung. Es sei $n, k \in \mathbb{N}_0$, ein Laplaceraum X mit $|X| = n$ und eine k-elementige Menge I gegeben. Für jedes Ereignis B in $\mathrm{MComb}_I(X)$ gilt

$$\mathrm{P}^{\mathrm{MComb}_I(X)}(B) = \frac{1}{n^k} \sum_{C \in B} |C|.$$

Beweis. Für alle $C \in \mathrm{MComb}_I(X)$ gilt

$$\prod_{y \in X} (\mathrm{P}^X(y))^{\mu_C(y)} = \prod_{y \in X} (\frac{1}{n})^{\mu_C(y)} = (\frac{1}{n})^{\sum_{y \in X} \mu_C(y)} = (\frac{1}{n})^k = \frac{1}{n^k}.$$

Nach Bemerkung (19.47)(c) folgt

$$\mathrm{P}^{\mathrm{MComb}_I(X)}(B) = \sum_{C \in B} |C| \prod_{y \in X} (\mathrm{P}^X(y))^{\mu_C(y)} = \sum_{C \in B} |C| \frac{1}{n^k} = \sum_{C \in B} |C| (\frac{1}{n})^k = \frac{1}{n^k} \sum_{C \in B} |C|$$

für jedes Ereignis B in $\mathrm{MComb}_I(X)$. □

Alternativer Beweis. Nach Proposition (19.23), Bemerkung (a) und Bemerkung (18.18) gilt

$$\begin{aligned}\mathrm{P}^{\mathrm{MComb}_I(X)}(B) &= \sum_{\substack{x\in\mathrm{Var}_I(X)\\ \mathrm{quo}(x)\in B}} \mathrm{P}^{\mathrm{Var}_I(X)}(x) = \sum_{\substack{x\in\mathrm{Var}_I(X)\\ [x]\in B}} \frac{1}{|\mathrm{Var}_I(X)|} = \sum_{C\in B}\sum_{\substack{x\in\mathrm{Var}_I(X)\\ [x]=C}} \frac{1}{n^k} = \sum_{C\in B}\frac{|C|}{n^k}\\ &= \frac{1}{n^k}\sum_{C\in B}|C|\end{aligned}$$

für jedes Ereignis B von $\mathrm{MComb}_I(X)$. □

(19.51) Anwendungsbeispiel.

(a) (i) Die möglichen (realen) Ergebnisse eines Würfelwurfs mit drei gewöhnlichen Würfeln seien als (formale) Ergebnisse des endlichen Wahrscheinlichkeitsraums $\mathrm{Var}_3([1,6])$ modelliert. Nach Bemerkung (19.49)(a) ist $\mathrm{Var}_3([1,6])$ ein Laplaceraum. Die Anzahl der Ergebnisse ist nach Bemerkung (18.18) gleich

$$|\mathrm{Var}_3([1,6])| = 6^3.$$

Das (reale) Ereignis, dass die Würfel nach dem Wurf dreimal eine 6 zeigen, entspricht dem (formalen) Ereignis

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

von $\mathrm{Var}_3([1,6])$. Seine Wahrscheinlichkeit ist gleich

$$\mathrm{P}(A) = \frac{|A|}{|\mathrm{Var}_3([1,6])|} = \frac{1}{6^3} = \frac{1}{216} \approx 0{,}0046.$$

Das (reale) Ereignis, dass die Würfel nach dem Wurf genau zweimal eine 6 zeigen, entspricht dem (formalen) Ereignis

$$A' = \{6\}\times\{6\}\times[1,5] \,\dot\cup\, \{6\}\times[1,5]\times\{6\} \,\dot\cup\, [1,5]\times\{6\}\times\{6\}$$

von $\mathrm{Var}_3([1,6])$. Die Anzahl der Ergebnisse von A' ist nach der Summenregel (18.4) und der Produktregel (18.8) gleich

$$\begin{aligned}|A'| &= |\{6\}\times\{6\}\times[1,5] \,\dot\cup\, \{6\}\times[1,5]\times\{6\} \,\dot\cup\, [1,5]\times\{6\}\times\{6\}|\\ &= |\{6\}\times\{6\}\times[1,5]| + |\{6\}\times[1,5]\times\{6\}| + |[1,5]\times\{6\}\times\{6\}| = 5+5+5 = 15.\end{aligned}$$

Die Wahrscheinlichkeit von A' ist folglich gleich

$$\mathrm{P}(A') = \frac{|A'|}{|\mathrm{Var}_3([1,6])|} = \frac{15}{6^3} = \frac{5}{72} \approx 0{,}0694.$$

Das (reale) Ereignis, dass die Würfel nach dem Wurf mindestens zweimal eine 6 zeigen, entspricht dem (formalen) Ereignis $A \,\dot\cup\, A'$ von $\mathrm{Var}_3([1,6])$. Seine Wahrscheinlichkeit ist gleich

$$\mathrm{P}(A \,\dot\cup\, A') = \mathrm{P}(A) + \mathrm{P}(A') = \frac{1}{6^3} + \frac{15}{6^3} = \frac{16}{6^3} = \frac{2}{3^3} = \frac{2}{27} \approx 0{,}0741.$$

(ii) Die möglichen (realen) Ergebnisse eines Würfelwurfs mit drei gewöhnlichen Würfeln seien als (formale) Ergebnisse des endlichen Wahrscheinlichkeitsraums $\mathrm{MComb}_3([1,6])$ modelliert.
Das (reale) Ereignis, dass die Würfel nach dem Wurf dreimal eine 6 zeigen, entspricht dem (formalen) Ereignis

$$B = \{[6,6,6]\}$$

von $\mathrm{MComb}_3([1,6])$. Wegen

$$|[6,6,6]| = |\{(6,6,6)\}| = 1$$

ist seine Wahrscheinlichkeit nach obiger Bemerkung gleich

$$\mathrm{P}(B) = \frac{|[6,6,6]|}{6^3} = \frac{1}{216} \approx 0{,}0046.$$

Das (reale) Ereignis, dass die Würfel nach dem Wurf genau zweimal eine 6 zeigen, entspricht dem (formalen) Ereignis

$$B' = \{C \in \mathrm{MComb}_3([1,6]) \mid \mu_C(6) = 2\}$$

von $\mathrm{MComb}_3([1,6])$. Die Abbildung

$$[1,5] \to B',\ x \mapsto [x,6,6]$$

ist eine Bijektion. Wegen

$$|[x,6,6]| = |\{(x,6,6),(6,x,6),(6,6,x)\}| = 3$$

für $x \in [1,5]$ ist die Wahrscheinlichkeit von B' nach obiger Bemerkung gleich

$$\mathrm{P}(B') = \frac{1}{6^3} \sum_{C \in B'} |C| = \frac{1}{6^3} \sum_{x \in [1,5]} |[x,6,6]| = \frac{1}{6^3} \sum_{x \in [1,5]} 3 = \frac{5 \cdot 3}{6^3} = \frac{5}{72} \approx 0{,}0694.$$

Das (reale) Ereignis, dass die Würfel nach dem Wurf mindestens zweimal eine 6 zeigen, entspricht dem (formalen) Ereignis $B \,\dot\cup\, B'$ von $\mathrm{MComb}_3([1,6])$. Seine Wahrscheinlichkeit ist gleich

$$\mathrm{P}(B \,\dot\cup\, B') = \mathrm{P}(B) + \mathrm{P}(B') = \frac{1}{6^3} + \frac{15}{6^3} = \frac{16}{6^3} = \frac{2}{3^3} = \frac{2}{27} \approx 0{,}0741.$$

(b) (i) Pokerhände (in der Variante Texas Hold'em) nach dem Austeilen seien als 2-Kombinationen in

$$K = \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \times \{2,3,4,5,6,7,8,9,10,\mathrm{B},\mathrm{D},\mathrm{K},\mathrm{A}\},$$

d.h. als Ergebnisse des endlichen Wahrscheinlichkeitsraums $\mathrm{Comb}_2(K)$ modelliert. Nach Bemerkung (19.49)(c) ist $\mathrm{Comb}_2(K)$ ein Laplaceraum. Die Anzahl der Ergebnisse ist nach der Produktregel (18.8) und Korollar (18.62) gleich

$$|\mathrm{Comb}_2(K)| = \binom{4 \cdot 13}{2} = \binom{52}{2} = \frac{52 \cdot 51}{1 \cdot 2} = 26 \cdot 51.$$

Das (reale) Ereignis, dass eine Pokerhand nach dem Austeilen zwei Asse enthält, entspricht dem (formalen) Ereignis

$$\begin{aligned} A &= \{[(f_1,\mathrm{A}),(f_2,\mathrm{A})] \mid f_1, f_2 \in \{\heartsuit,\diamondsuit,\spadesuit,\clubsuit\} \text{ mit } f_1 \neq f_2\} \\ &= \{[x_1,x_2] \mid x_1, x_2 \in \{\heartsuit,\diamondsuit,\spadesuit,\clubsuit\} \times \{\mathrm{A}\} \text{ mit } x_1 \neq x_2\} = \mathrm{Comb}_2(\{\heartsuit,\diamondsuit,\spadesuit,\clubsuit\} \times \{\mathrm{A}\}) \end{aligned}$$

von $\mathrm{Comb}_2(K)$. Die Anzahl der Ergebnisse von A ist nach Korollar (18.62) gleich

$$|A| = |\mathrm{Comb}_2(\{\heartsuit,\diamondsuit,\spadesuit,\clubsuit\} \times \{\mathrm{A}\})| = \binom{4}{2} = \frac{4 \cdot 3}{1 \cdot 2} = 2 \cdot 3.$$

Die Wahrscheinlichkeit von A ist folglich gleich

$$\mathrm{P}(A) = \frac{|A|}{|\mathrm{Comb}_2(K)|} = \frac{2 \cdot 3}{26 \cdot 51} = \frac{1}{13 \cdot 17} = \frac{1}{221} \approx 0{,}0045.$$

Das (reale) Ereignis, dass eine Pokerhand nach dem Austeilen eine 2 und eine 7 in unterschiedlichen Kartenfarben enthält, entspricht dem (formalen) Ereignis

$$B = \{[(f_1,2),(f_2,7)] \mid f_1, f_2 \in \{\heartsuit,\diamondsuit,\spadesuit,\clubsuit\} \text{ mit } f_1 \neq f_2\}$$

$$= \{[(f_1, 2), (f_2, 7)] \mid f \in \mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\})\}$$

von $\mathrm{Comb}_2(K)$. Die Abbildung

$$\mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}) \to B,\ f \mapsto [(f_1, 2), (f_2, 7)]$$

ist eine Bijektion. Nach der Gleichheitsregel (18.1) und Korollar (18.31) ist die Anzahl der Ergebnisse von B folglich gleich

$$|B| = |\mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\})| = 4 \cdot 3 = 12.$$

Somit ist die Wahrscheinlichkeit von B gleich

$$\mathrm{P}(B) = \frac{|B|}{|\mathrm{Comb}_2(K)|} = \frac{12}{26 \cdot 51} = \frac{2}{13 \cdot 17} = \frac{2}{221} \approx 0{,}0090.$$

(ii) Pokerhände (in der Variante Texas Hold'em) nach dem Austeilen seien als 2-Permutationen in

$$K = \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \times \{2, 3, 4, 5, 6, 7, 8, 9, 10, \mathrm{B}, \mathrm{D}, \mathrm{K}, \mathrm{A}\},$$

d.h. als Ergebnisse des endlichen Wahrscheinlichkeitsraums $\mathrm{Perm}_2(K)$ modelliert. Nach Bemerkung (19.49)(b) ist $\mathrm{Perm}_2(K)$ ein Laplaceraum. Die Anzahl der Ergebnisse ist nach der Produktregel (18.8) und Korollar (18.31) gleich

$$|\mathrm{Perm}_2(K)| = 52 \cdot 51.$$

Das (reale) Ereignis, dass eine Pokerhand nach dem Austeilen zwei Asse enthält, entspricht dem (formalen) Ereignis

$$\begin{aligned} A &= \{((f_1, \mathrm{A}), (f_2, \mathrm{A})) \mid f_1, f_2 \in \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \text{ mit } f_1 \neq f_2\} \\ &= \{(x_1, x_2) \mid x_1, x_2 \in \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \times \{\mathrm{A}\} \text{ mit } x_1 \neq x_2\} = \mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \times \{\mathrm{A}\}) \end{aligned}$$

von $\mathrm{Perm}_2(K)$. Die Anzahl der Ergebnisse von A ist nach Korollar (18.31) gleich

$$|A| = |\mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \times \{\mathrm{A}\})| = 4 \cdot 3.$$

Die Wahrscheinlichkeit von A ist folglich gleich

$$\mathrm{P}(A) = \frac{|A|}{|\mathrm{Perm}_2(K)|} = \frac{4 \cdot 3}{52 \cdot 51} = \frac{1}{13 \cdot 17} = \frac{1}{221} \approx 0{,}0045.$$

Das (reale) Ereignis, dass eine Pokerhand nach dem Austeilen eine 2 und eine 7 in unterschiedlichen Kartenfarben enthält, entspricht dem (formalen) Ereignis

$$\begin{aligned} B &= \{((f_1, 2), (f_2, 7)) \mid f_1, f_2 \in \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \text{ mit } f_1 \neq f_2\} \\ &\quad \dot\cup \{((f_1, 7), (f_2, 2)) \mid f_1, f_2 \in \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\} \text{ mit } f_1 \neq f_2\} \\ &= \{((f_1, 2), (f_2, 7)) \mid f \in \mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\})\} \\ &\quad \dot\cup \{((f_1, 7), (f_2, 2)) \mid f \in \mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\})\} \end{aligned}$$

von $\mathrm{Perm}_2(K)$. Die Abbildungen

$$\begin{aligned} &\mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}) \to \{((f_1, 2), (f_2, 7)) \mid f \in \mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\})\},\ f \mapsto ((f_1, 2), (f_2, 7)), \\ &\mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}) \to \{((f_1, 7), (f_2, 2)) \mid f \in \mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\})\},\ f \mapsto ((f_1, 7), (f_2, 2)), \end{aligned}$$

sind Bijektionen. Nach der Summenregel (18.1), der Gleichheitsregel (18.1) und Korollar (18.31) ist die Anzahl der Ergebnisse von B folglich gleich

$$\begin{aligned} |B| &= |\{((f_1, 2), (f_2, 7)) \mid f \in \mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\})\} \\ &\qquad \dot\cup \{((f_1, 7), (f_2, 2)) \mid f \in \mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\})\}| \\ &= |\{((f_1, 2), (f_2, 7)) \mid f \in \mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\})\}| \\ &\qquad + |\{((f_1, 7), (f_2, 2)) \mid f \in \mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\})\}| \\ &= |\mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\})| + |\mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\})| = 2|\mathrm{Perm}_2(\{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\})| = 2 \cdot 4 \cdot 3. \end{aligned}$$

Somit ist die Wahrscheinlichkeit von B gleich

$$\mathrm{P}(B) = \frac{|B|}{|\mathrm{Perm}_2(K)|} = \frac{2 \cdot 4 \cdot 3}{52 \cdot 51} = \frac{2}{13 \cdot 17} = \frac{2}{221} \approx 0{,}0090.$$

Stochastische Unabhängigkeit

Es sei ein quasiendlicher Wahrscheinlichkeitsraum X gegeben. Der Produktwahrscheinlichkeitsraum $X \times X$ dient zur Modellierung eines doppelt durchgeführten Zufallsexperiments, deren einzelne Durchführungen unabhängig voneinander geschehen.
Für alle Ereignisse A und B von X gilt

$$\begin{aligned}\mathrm{P}^{X\times X}(A \times B) &= \sum_{(x,y)\in A\times B} \mathrm{P}^X(x)\,\mathrm{P}^X(y) = \sum_{x\in A}\sum_{y\in B} \mathrm{P}^X(x)\,\mathrm{P}^X(y) = \sum_{x\in A} \mathrm{P}^X(x) \sum_{y\in B} \mathrm{P}^X(y)\\ &= \mathrm{P}^X(A)\,\mathrm{P}^X(B).\end{aligned}$$

Daher ist insbesondere

$$\begin{aligned}&\mathrm{P}^{X\times X}(A \times X) = \mathrm{P}^X(A)\,\mathrm{P}^X(X) = \mathrm{P}^X(A),\\ &\mathrm{P}^{X\times X}(X \times B) = \mathrm{P}^X(X)\,\mathrm{P}^X(B) = \mathrm{P}^X(B)\end{aligned}$$

und damit

$$\mathrm{P}^{X\times X}((A \times X) \cap (X \times B)) = \mathrm{P}^{X\times X}(A \times B) = \mathrm{P}^X(A)\,\mathrm{P}^X(B) = \mathrm{P}^{X\times X}(A \times X)\,\mathrm{P}^{X\times X}(X \times B)$$

für alle Ereignisse A und B von X.
Wir wollen Ereignisse A und B von X unabhängig nennen, wenn Sie sich so verhalten wie ihre entsprechenden Ereignisse $A \times X$ und $X \times B$ im Produktwahrscheinlichkeitsraum $X \times X$:

(19.52) Definition (stochastische (Un)abhängigkeit)**.** Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und Ereignisse A und B von X gegeben. Wir nennen A und B *stochastisch unabhängig*, falls

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

gilt; ansonsten *stochastisch abhängig*.

(19.53) Beispiel. Es seien verschiedene Objekte a, b, c, d gegeben und es sei X der Wahrscheinlichkeitsraum mit Ergebnismenge $\{a, b, c, d\}$ und mit

$$\mathrm{P}(x) = \begin{cases} \frac{1}{3} & \text{für } x \in \{a, b\},\\ \frac{1}{6} & \text{für } x \in \{c, d\}.\end{cases}$$

(a) Die Ereignisse $\{a, b\}$ und $\{a, c\}$ sind stochastisch unabhängig.

(b) Die Ereignisse $\{a, b\}$ und $\{c, d\}$ sind stochastisch abhängig.

Beweis.

(a) Es ist

$$\begin{aligned}\mathrm{P}(\{a, b\}) &= \mathrm{P}(a) + \mathrm{P}(b) = \frac{1}{3} + \frac{1}{3} = \frac{2}{3},\\ \mathrm{P}(\{a, c\}) &= \mathrm{P}(a) + \mathrm{P}(c) = \frac{1}{3} + \frac{1}{6} = \frac{1}{2},\\ \mathrm{P}(\{a, b\} \cap \{a, c\}) &= \mathrm{P}(a) = \frac{1}{3},\end{aligned}$$

also

$$\mathrm{P}(\{a, b\} \cap \{a, c\}) = \frac{1}{3} = \frac{2}{3} \cdot \frac{1}{2} = \mathrm{P}(\{a, b\})\,\mathrm{P}(\{a, c\}).$$

Folglich sind $\{a, b\}$ und $\{a, c\}$ stochastisch unabhängig.

(b) Es ist

$$\begin{aligned}
\mathrm{P}(\{a,b\}) &= \mathrm{P}(a) + \mathrm{P}(b) = \frac{1}{3} + \frac{1}{3} = \frac{2}{3},\\
\mathrm{P}(\{c,d\}) &= \mathrm{P}(c) + \mathrm{P}(d) = \frac{1}{6} + \frac{1}{6} = \frac{1}{3},\\
\mathrm{P}(\{a,b\} \cap \{c,d\}) &= \mathrm{P}(\emptyset) = 0,
\end{aligned}$$

also

$$\mathrm{P}(\{a,b\} \cap \{c,d\}) = 0 \neq \frac{2}{9} = \frac{2}{3} \cdot \frac{1}{3} = \mathrm{P}(\{a,b\})\,\mathrm{P}(\{c,d\}).$$

Folglich sind $\{a,b\}$ und $\{c,d\}$ stochastisch abhängig. □

(19.54) Anwendungsbeispiel. In einer Urne befinden sich zehn rote und 20 schwarze Kugeln. Die möglichen (realen) Ergebnisse einer einfachen Entnahme einer Kugel seien als (formale) Ergebnisse des Laplaceraums $U = R \dot\cup S$ mit $R = [1,10] \times \{\text{rot}\}$ und $S = [1,20] \times \{\text{schwarz}\}$ modelliert.

(a) Es wird blind eine Kugel entnommen, zurückgelegt, und eine zweite Kugel blind entnommen. Die möglichen (realen) Ergebnisse dieser zweifachen Entnahme seien als (formale) Ergebnisse des endlichen Wahrscheinlichkeitsraums $\mathrm{Var}_2(U)$ modelliert. Nach Bemerkung (19.49)(a) ist $\mathrm{Var}_2(U)$ ein Laplaceraum. Die Anzahl der Ergebnisse ist nach Bemerkung (18.18) und Anwendungsbeispiel (19.19) gleich

$$|\mathrm{Var}_2(U)| = 30^2 = 900.$$

Das (reale) Ereignis, dass die erste gezogene Kugel rot ist, entspricht dem (formalen) Ereignis $A = R \times U$ von $\mathrm{Var}_2(U)$. Die Anzahl der Ergebnisse von A ist nach der Produktregel (18.8) gleich

$$|A| = |R \times U| = |R| \cdot |U| = 10 \cdot 30 = 300.$$

Seine Wahrscheinlichkeit ist somit gleich

$$\mathrm{P}(A) = \frac{|A|}{|\mathrm{Var}_2(U)|} = \frac{300}{900} = \frac{1}{3}.$$

Das (reale) Ereignis, dass die zweite gezogene Kugel rot ist, entspricht dem (formalen) Ereignis

$$B = U \times R$$

von $\mathrm{Var}_2(U)$. Seine Wahrscheinlichkeit ist ebenfalls gleich

$$\mathrm{P}(B) = \frac{1}{3},$$

wie man durch eine analoge Rechnung erkennt.

Das (reale) Ereignis, dass beide gezogenen Kugeln rot sind, entspricht dem (formalen) Ereignis

$$A \cap B = R \times R = \mathrm{Var}_2(R)$$

von $\mathrm{Var}_2(U)$. Die Anzahl der Ergebnisse von $A \cap B$ ist nach Bemerkung (18.18) gleich

$$|A \cap B| = |\mathrm{Var}_2(R)| = 10^2 = 100.$$

Seine Wahrscheinlichkeit ist somit gleich

$$\mathrm{P}(A \cap B) = \frac{|A \cap B|}{|\mathrm{Var}_2(U)|} = \frac{100}{900} = \frac{1}{9}.$$

Wegen

$$\mathrm{P}(A \cap B) = \frac{1}{9} = \frac{1}{3} \cdot \frac{1}{3} = \mathrm{P}(A)\,\mathrm{P}(B)$$

sind A und B stochastisch unabhängig.

(b) Es wird blind eine Kugel entnommen, beiseite gelegt, und eine zweite Kugel blind entnommen. Die möglichen (realen) Ergebnisse dieser zweifachen Entnahme seien als (formale) Ergebnisse des endlichen Wahrscheinlichkeitsraums $\mathrm{Perm}_2(U)$ modelliert. Nach Bemerkung (19.49)(b) ist $\mathrm{Perm}_2(U)$ ein Laplaceraum. Die Anzahl der Ergebnisse ist nach Korollar (18.31) und Anwendungsbeispiel (19.19) gleich

$$|\mathrm{Perm}_2(U)| = \prod_{i\in[1,2]} (30 - i + 1) = 30 \cdot 29 = 870.$$

Das (reale) Ereignis, dass die erste gezogene Kugel rot ist, entspricht dem (formalen) Ereignis

$$\begin{aligned} A &= \{x \in \mathrm{Perm}_2(U) \mid x_1 \in R\} = \{(x_1, x_2) \mid x_1 \in R,\, x_2 \in U \setminus \{x_1\}\} \\ &= \dot{\bigcup_{x_1\in R}} \{(x_1, x_2) \mid x_2 \in U \setminus \{x_1\}\} \end{aligned}$$

von $\mathrm{Perm}_2(U)$. Für jedes $x_1 \in R$ ist

$$U \setminus \{x_1\} \to \{(x_1, x_2) \mid x_2 \in U \setminus \{x_1\}\},\ x_2 \mapsto (x_1, x_2)$$

eine Bijektion. Die Anzahl der Ergebnisse von A ist nach der Summenregel (18.4), der Gleichheitsregel (18.1) und der Differenzregel (18.6) gleich

$$\begin{aligned} |A| &= |\dot{\bigcup_{x_1\in R}} \{(x_1, x_2) \mid x_2 \in U \setminus \{x_1\}\}| = \sum_{x_1\in R} |\{(x_1, x_2) \mid x_2 \in U \setminus \{x_1\}\}| = \sum_{x_1\in R} |U \setminus \{x_1\}| \\ &= \sum_{x_1\in R} 29 = 10 \cdot 29 = 290. \end{aligned}$$

Seine Wahrscheinlichkeit ist somit gleich

$$\mathrm{P}(A) = \frac{|A|}{|\mathrm{Perm}_2(U)|} = \frac{290}{870} = \frac{1}{3}.$$

Das (reale) Ereignis, dass die zweite gezogene Kugel rot ist, entspricht dem (formalen) Ereignis

$$B = \{x \in \mathrm{Perm}_2(U) \mid x_2 \in R\}$$

von $\mathrm{Perm}_2(U)$. Seine Wahrscheinlichkeit ist ebenfalls gleich

$$\mathrm{P}(B) = \frac{1}{3},$$

wie man durch eine analoge Rechnung erkennt.

Das (reale) Ereignis, dass beide gezogenen Kugeln rot sind, entspricht dem (formalen) Ereignis

$$A \cap B = \{x \in \mathrm{Perm}_2(U) \mid x_1 \in R,\, x_2 \in R\} = \mathrm{Perm}_2(R)$$

von $\mathrm{Perm}_2(U)$. Die Anzahl der Ergebnisse von $A \cap B$ ist nach Korollar (18.31) gleich

$$|A \cap B| = |\mathrm{Perm}_2(R)| = \prod_{i\in[1,2]} (10 - i + 1) = 10 \cdot 9 = 90.$$

Seine Wahrscheinlichkeit ist somit gleich

$$\mathrm{P}(A \cap B) = \frac{|A \cap B|}{|\mathrm{Perm}_2(U)|} = \frac{90}{870} = \frac{1}{29}.$$

Wegen

$$\mathrm{P}(A \cap B) = \frac{1}{29} \neq \frac{1}{9} = \frac{1}{3} \cdot \frac{1}{3} = \mathrm{P}(A)\,\mathrm{P}(B)$$

sind A und B stochastisch abhängig.

(19.55) Bemerkung. Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und Ereignisse A und B von X mit $\mathrm{P}(B) > 0$ gegeben. Genau dann sind A und B stochastisch unabhängig, wenn

$$\mathrm{P}(A \mid B) = \mathrm{P}(A)$$

gilt.

Beweis. Nach Bemerkung (19.40) gilt $\mathrm{P}(A \cap B) = \mathrm{P}(B)\,\mathrm{P}(A \mid B)$. Folglich ist $\mathrm{P}(A \cap B) = \mathrm{P}(A)\,\mathrm{P}(B)$ äquivalent zu $\mathrm{P}(B)\,\mathrm{P}(A \mid B) = \mathrm{P}(A)\,\mathrm{P}(B)$. Wegen $\mathrm{P}(B) > 0$ sind daher A und B genau dann stochastisch unabhängig, wenn $\mathrm{P}(A \mid B) = \mathrm{P}(A)$ gilt. □

Erwartungswert und Varianz

Zum Abschluss dieser Einführung in die Wahrscheinlichkeitstheorie betrachten wir noch zwei Kennzahlen zur Beschreibung reellwertiger Zufallsgrößen.
Die erste Kennzahl ist der Erwartungswert, ein mit den Wahrscheinlichkeiten gewichteter Mittelwert:

(19.56) Definition (Erwartungswert)**.** Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und eine Zufallsgröße f auf X mit Werten in $\mathbb{R}$ gegeben. Der *Erwartungswert* von f ist definiert durch

$$\mathrm{E}(f) := \sum_{x \in X} \mathrm{P}(x)\, f(x).$$

(19.57) Beispiel. Es sei X der endliche Wahrscheinlichkeitsraum mit Ergebnismenge $[1, 5]$ und $P(x) = \frac{x}{15}$ für $x \in X$. Der Erwartungswert der Inklusion $\mathrm{inc}\colon X \to \mathbb{R}$ ist gegeben durch

$$\mathrm{E}(\mathrm{inc}) = \frac{11}{3}.$$

Beweis. Es ist

$$\mathrm{E}(\mathrm{inc}) = \sum_{x \in X} \mathrm{P}(x)\,\mathrm{inc}(x) = \sum_{x \in X} \frac{x}{15} \cdot x = \frac{1}{15} \sum_{x \in X} x^2 = \frac{1}{15}(1^2 + 2^2 + 3^2 + 4^2 + 5^2) = \frac{55}{15} = \frac{11}{3}. \qquad \square$$

(19.58) Anwendungsbeispiel. Die möglichen (realen) Ergebnisse eines Würfelwurfs mit zwei gewöhnlichen Würfeln seien als (formale) Ergebnisse des Produktraums $[1, 6] \times [1, 6]$ modelliert. Nach Bemerkung (19.32) ist $[1, 6] \times [1, 6]$ ein Laplaceraum. Die Zuordnung der Augensumme zu jedem Ergebnis sei als Zufallsgröße $s\colon [1, 6] \times [1, 6] \to \mathbb{R}$, $(x, y) \mapsto x + y$ modelliert.
Der Erwartungswert von s ist gleich

$$\begin{aligned}\mathrm{E}(s) &= \sum_{(x,y) \in [1,6] \times [1,6]} \mathrm{P}(x, y)\, s(x, y) = \sum_{x \in [1,6]} \sum_{y \in [1,6]} \frac{1}{36}(x + y) = \frac{1}{36}\Big(\sum_{x \in [1,6]} \sum_{y \in [1,6]} x + \sum_{x \in [1,6]} \sum_{y \in [1,6]} y \Big) \\ &= \frac{1}{36}\Big(\sum_{y \in [1,6]} \sum_{x \in [1,6]} x + \sum_{x \in [1,6]} \sum_{y \in [1,6]} y \Big) = \frac{1}{36}\Big(6 \cdot \frac{6 \cdot 7}{2} + 6 \cdot \frac{6 \cdot 7}{2}\Big) = 7.\end{aligned}$$

Der Erwartungswert einer reellwertigen Zufallsgröße hängt nur von ihren Werten ab:

(19.59) Bemerkung. Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und eine Zufallsgröße f auf X mit Werten in $\mathbb{R}$ gegeben. Dann ist

$$\mathrm{E}(f) = \sum_{y \in \mathbb{R}} \mathrm{P}(y)\, y = \sum_{y \in \operatorname{Im} f} \mathrm{P}(y)\, y.$$

Beweis. Nach Proposition (19.23) und Bemerkung (19.28) ist

$$\mathrm{E}(f) = \sum_{x \in X} \mathrm{P}(x)\, f(x) = \sum_{y \in \mathbb{R}} \sum_{\substack{x \in X \\ f(x) = y}} \mathrm{P}(x)\, f(x) = \sum_{y \in \mathbb{R}} \sum_{\substack{x \in X \\ f(x) = y}} \mathrm{P}(x)\, y = \sum_{y \in \mathbb{R}} \mathrm{P}(y)\, y = \sum_{y \in \operatorname{Im} f} \mathrm{P}(y)\, y. \qquad \square$$

(19.60) Anwendungsbeispiel. Die möglichen (realen) Ergebnisse eines Würfelwurfs mit zwei gewöhnlichen Würfeln seien als (formale) Ergebnisse des Produktraums $[1,6] \times [1,6]$ modelliert. Nach Bemerkung (19.32) ist $[1,6] \times [1,6]$ ein Laplaceraum. Die Zuordnung der Augensumme zu jedem Ergebnis sei als Zufallsgröße $s\colon [1,6] \times [1,6] \to \mathbb{R}$, $(x,y) \mapsto x+y$ modelliert.
Dann ist

$$\operatorname{Im} s = \{s(x,y) \mid (x,y) \in [1,6] \times [1,6]\} = \{x+y \mid (x,y) \in [1,6] \times [1,6]\} = [2,12]$$

und die Wahrscheinlichkeitsverteilung von s erfüllt

$$\mathrm{P}(z) = \sum_{\substack{(x,y)\in[1,6]\times[1,6]\\ s(x,y)=z}} \mathrm{P}(x,y) = \sum_{\substack{(x,y)\in[1,6]\times[1,6]\\ x+y=z}} \frac{1}{36} = \begin{cases} \frac{1}{36} & \text{für } z \in \{2,12\}, \\ \frac{2}{36} & \text{für } z \in \{3,11\}, \\ \frac{3}{36} & \text{für } z \in \{4,10\}, \\ \frac{4}{36} & \text{für } z \in \{5,9\}, \\ \frac{5}{36} & \text{für } z \in \{6,8\}, \\ \frac{6}{36} & \text{für } z \in \{7\}. \end{cases}$$

Nach Bemerkung (19.59) ist der Erwartungswert von s gleich

$$\begin{aligned} \mathrm{E}(s) &= \sum_{z \in \operatorname{Im} s} \mathrm{P}(z)\, z \\ &= \frac{1}{36}\cdot 2 + \frac{2}{36}\cdot 3 + \frac{3}{36}\cdot 4 + \frac{4}{36}\cdot 5 + \frac{5}{36}\cdot 6 + \frac{6}{36}\cdot 7 + \frac{5}{36}\cdot 8 + \frac{4}{36}\cdot 9 + \frac{3}{36}\cdot 10 + \frac{2}{36}\cdot 11 + \frac{1}{36}\cdot 12 \\ &= \frac{1}{36}(2+12) + \frac{2}{36}(3+11) + \frac{3}{36}(4+10) + \frac{4}{36}(5+9) + \frac{5}{36}(6+8) + \frac{6}{36}\cdot 7 \\ &= \frac{(1+2+3+4+5)\cdot 14 + 6\cdot 7}{36} = 7. \end{aligned}$$

Als ein Maß für die Streuung der Wahrscheinlichkeitsverteilung einer Zufallsgröße mit Werten in $\mathbb{R}$, also der Abweichung von ihrem Erwartungswert, führen wir die sogenannte Varianz ein. Hierzu fassen wir die Menge dieser Zufallsgrößen wie folgt auf:

(19.61) Bemerkung. Es sei eine Menge X gegeben.

(a) Die Menge $\mathrm{Map}(X,\mathbb{R})$ wird ein kommutativer Ring mit Addition und Multiplikation gegeben durch

$$\begin{aligned} (f+g)(x) &= f(x) + g(x), \\ (fg)(x) &= f(x)g(x) \end{aligned}$$

für $x \in X$, $f, g \in \mathrm{Map}(X,\mathbb{R})$. Die Null und die Eins von $\mathrm{Map}(X,\mathbb{R})$ sind gegeben durch

$$\begin{aligned} 0(x) &= 0, \\ 1(x) &= 1 \end{aligned}$$

für $x \in R$. Für $f \in \mathrm{Map}(X,\mathbb{R})$ ist das Negative von f in $\mathrm{Map}(X,\mathbb{R})$ gegeben durch

$$(-f)(x) = -f(x)$$

für $x \in \mathbb{R}$. Ein $f \in \mathrm{Map}(X,\mathbb{R})$ ist genau dann invertierbar in $\mathrm{Map}(X,\mathbb{R})$, wenn $f(x)$ für jedes $x \in X$ invertierbar in $\mathrm{Map}(X,\mathbb{R})$ ist, und in diesem Fall ist

$$(f^{-1})(x) = (f(x))^{-1}$$

für $x \in \mathbb{R}$.

(b) Es sei

$$\iota\colon \mathbb{R} \to \mathrm{Map}(X,\mathbb{R}),\ a \mapsto (x \mapsto a).$$

Dann ist ι injektiv und es gilt:

- *Verträglichkeit mit den Additionen.* Für $a, a' \in \mathbb{R}$ ist $\iota(a + a') = \iota(a) + \iota(a')$.
- *Verträglichkeit der Nullen.* Es ist $\iota(0) = 0$.
- *Verträglichkeit der Negative.* Für $a \in \mathbb{R}$ ist $\iota(-a) = -\iota(a)$.
- *Verträglichkeit mit den Multiplikationen.* Für $a, a' \in \mathbb{R}$ ist $\iota(aa') = \iota(a)\,\iota(a')$.
- *Verträglichkeit der Einselemente.* Es ist $\iota(1) = 1$.
- *Verträglichkeit der Inversen.* Für $a \in \mathbb{R}^\times$ ist $\iota(a) \in (\mathrm{Map}(X, \mathbb{R}))^\times$ mit $\iota(a^{-1}) = (\iota(a))^{-1}$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(19.62) Konvention. Es sei eine Menge X gegeben. Sofern keine Missverständnisse entstehen fassen wir von jetzt an $\mathrm{Map}(X, \mathbb{R})$ als kommutativen Ring wie in Bemerkung (19.61)(a) auf und identifizieren $\mathbb{R}$ mit dem Bild der injektiven Abbildung $\iota\colon \mathbb{R} \to \mathrm{Map}(X, \mathbb{R})$, $a \mapsto (x \mapsto a)$ aus Bemerkung (19.61)(b). Das heißt, unter Missbrauch der Notationen schreiben wir $\mathbb{R}$ anstatt $\mathrm{Im}\,\iota$, und für $a \in \mathbb{R}$ notieren wir das Bild $\iota(a)\colon X \to \mathbb{R}$, $x \mapsto a$ von a auch als a.

Die Menge $\mathrm{Map}(\mathbb{R}, \mathbb{R})$ wird auf verschiedene Arten zu einem Monoid: Mit der werteweisen Multiplikation aus Bemerkung (19.61)(a) sowie mit der Komposition wie in Bemerkung (6.22). Sofern aus der jeweiligen Situation nicht klar ist, welche Struktur gemeint ist, sagen wir dies explizit dazu. Insbesondere sei angemerkt, dass die Potenznotation mit der Struktur aus Bemerkung (19.61)(a) eine andere Bedeutung kriegt: Bzgl. der werteweisen Multiplikation gilt etwa $f^2(x) = (f(x))^2$ für $x \in \mathbb{R}$, $f \in \mathrm{Map}(\mathbb{R}, \mathbb{R})$, während bzgl. der Komposition $f^2(x) = f(f(x))$ für $x \in \mathbb{R}$, $f \in \mathrm{Map}(\mathbb{R}, \mathbb{R})$ ist.

(19.63) Definition (Varianz)**.** Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und eine Zufallsgröße f auf X mit Werten in $\mathbb{R}$ gegeben. Die *Varianz* von f ist definiert durch

$$\mathrm{V}(f) := \mathrm{E}((f - \mathrm{E}(f))^2).$$

(19.64) Beispiel. Es sei X der endliche Wahrscheinlichkeitsraum mit Ergebnismenge $[1, 5]$ und $P(x) = \frac{x}{15}$ für $x \in X$. Die Varianz der Inklusion $\mathrm{inc}\colon X \to \mathbb{R}$ ist gegeben durch

$$\mathrm{V}(\mathrm{inc}) = \frac{14}{9}.$$

Beweis. Nach Beispiel (19.57) ist $\mathrm{E}(\mathrm{inc}) = \frac{11}{3}$, also

$$\begin{aligned}
\mathrm{V}(\mathrm{inc}) &= \mathrm{E}((\mathrm{inc} - \mathrm{E}(\mathrm{inc}))^2) = \mathrm{E}((\mathrm{inc} - \tfrac{11}{3})^2) = \sum_{x \in X} \mathrm{P}(x)\,(\mathrm{inc} - \tfrac{11}{3})^2(x) = \sum_{x \in X} \frac{x}{15}(x - \tfrac{11}{3})^2 \\
&= \frac{1}{15} \sum_{x \in X} x\,(x - \tfrac{11}{3})^2 = \frac{1}{15}(1\,(1 - \tfrac{11}{3})^2 + 2\,(2 - \tfrac{11}{3})^2 + 3\,(3 - \tfrac{11}{3})^2 + 4\,(4 - \tfrac{11}{3})^2 + 5\,(5 - \tfrac{11}{3})^2) \\
&= \frac{1}{15}(1\,(-\tfrac{8}{3})^2 + 2\,(-\tfrac{5}{3})^2 + 3\,(-\tfrac{2}{3})^2 + 4\,(\tfrac{1}{3})^2 + 5\,(\tfrac{4}{3})^2) = \frac{1}{15} \cdot \frac{210}{3^2} = \frac{14}{9}.
\end{aligned}$$

□

(19.65) Bemerkung. Es seien ein quasiendlicher Wahrscheinlichkeitsraum X und eine Zufallsgröße f auf X mit Werten in $\mathbb{R}$ gegeben. Dann ist

$$\mathrm{V}(f) = \sum_{y \in \mathbb{R}} \mathrm{P}(y)\,(y - \mathrm{E}(f))^2 = \sum_{y \in \mathrm{Im}\, f} \mathrm{P}(y)\,(y - \mathrm{E}(f))^2.$$

Beweis. Nach Bemerkung (19.59) ist

$$\mathrm{E}(f) = \sum_{y \in \mathbb{R}} \mathrm{P}(y)\, y$$

Nach Proposition (19.23) und Bemerkung (19.28) ist

$$\begin{aligned}
\mathrm{V}(f) &= \mathrm{E}((f - \mathrm{E}(f))^2) = \sum_{x \in X} \mathrm{P}(x)\,(f - \mathrm{E}(f))^2(x) = \sum_{y \in \mathbb{R}} \sum_{\substack{x \in X \\ f(x) = y}} \mathrm{P}(x)\,(f(x) - \mathrm{E}(f))^2 \\
&= \sum_{y \in \mathbb{R}} \sum_{\substack{x \in X \\ f(x) = y}} \mathrm{P}(x)\,(y - \mathrm{E}(f))^2 = \sum_{y \in \mathbb{R}} \mathrm{P}(y)\,(y - \mathrm{E}(f))^2 = \sum_{y \in \mathrm{Im}\, f} \mathrm{P}(y)\,(y - \mathrm{E}(f))^2.
\end{aligned}$$

□

(19.66) Anwendungsbeispiel. Die möglichen (realen) Ergebnisse eines Würfelwurfs mit zwei gewöhnlichen Würfeln seien als (formale) Ergebnisse des Produktraums $[1,6] \times [1,6]$ modelliert. Nach Bemerkung (19.32) ist $[1,6] \times [1,6]$ ein Laplaceraum. Die Zuordnung der Augensumme zu jedem Ergebnis sei als Zufallsgröße $s\colon [1,6] \times [1,6] \to \mathbb{R}$, $(x,y) \mapsto x+y$ modelliert.
Nach Anwendungsbeispiel (19.60) ist $\operatorname{Im} s = [2,12]$, die Wahrscheinlichkeitsverteilung von s erfüllt

$$\mathrm{P}(z) = \begin{cases} \frac{1}{36} & \text{für } z \in \{2,12\}, \\ \frac{2}{36} & \text{für } z \in \{3,11\}, \\ \frac{3}{36} & \text{für } z \in \{4,10\}, \\ \frac{4}{36} & \text{für } z \in \{5,9\}, \\ \frac{5}{36} & \text{für } z \in \{6,8\}, \\ \frac{6}{36} & \text{für } z \in \{7\}, \end{cases}$$

und der Erwartungswert von s ist gleich $\mathrm{E}(s) = 7$. Nach Bemerkung (19.65) ist die Varianz von s gleich

$$\begin{aligned} \mathrm{V}(s) &= \sum_{z \in \mathbb{R}} \mathrm{P}(z)\,(z - \mathrm{E}(s))^2 \\ &= \frac{1}{36} \cdot (2-7)^2 + \frac{2}{36} \cdot (3-7)^2 + \frac{3}{36} \cdot (4-7)^2 + \frac{4}{36} \cdot (5-7)^2 + \frac{5}{36} \cdot (6-7)^2 + \frac{6}{36} \cdot (7-7)^2 \\ &\quad + \frac{5}{36} \cdot (8-7)^2 + \frac{4}{36} \cdot (9-7)^2 + \frac{3}{36} \cdot (10-7)^2 + \frac{2}{36} \cdot (11-7)^2 + \frac{1}{36} \cdot (12-7)^2 \\ &= \frac{1}{36} \cdot 2 \cdot 25 + \frac{2}{36} \cdot 2 \cdot 16 + \frac{3}{36} \cdot 2 \cdot 9 + \frac{4}{36} \cdot 2 \cdot 4 + \frac{5}{36} \cdot 2 \cdot 1 \\ &= \frac{2 \cdot 25 + 2 \cdot 2 \cdot 16 + 3 \cdot 2 \cdot 9 + 4 \cdot 2 \cdot 4 + 5 \cdot 2 \cdot 1}{36} = \frac{35}{6}. \end{aligned}$$

Zusätzliche Konzepte

Im Folgenden geben wir einige zusätzliche Definitionen, deren Studium dem Leser zur Übung überlassen sei.

(19.67) Definition (Binomialverteilung)**.** Es seien $k \in \mathbb{N}_0$ und $p \in [0,1]_{\mathbb{R}}$ gegeben. Ferner sei X der endliche Wahrscheinlichkeitsraum mit Ergebnismenge $\{0,1\}$ und

$$\mathrm{P}(y) = \begin{cases} 1-p & \text{für } y = 0, \\ p & \text{für } y = 1, \end{cases}$$

und es sei

$$f\colon \mathrm{Var}_k(X) \to \mathbb{R},\ x \mapsto \mu_x(1).$$

Die Wahrscheinlichkeitsverteilung des von f induzierten Wahrscheinlichkeitsraums wird *Binomialverteilung* zu den Parametern k und p genannt und als

$$\mathrm{Bin}_{k,p} := \mathrm{P}_f^{\mathbb{R}}\colon \mathbb{R} \to \mathbb{R}$$

notiert.

(19.68) Definition (hypergeometrische Verteilung)**.** Es seien $n, m, k \in \mathbb{N}_0$ mit $m \leq n$ und $k \leq n$ gegeben. Ferner sei

$$f\colon \mathrm{Comb}_k([1,n]) \to \mathbb{R},\ [x] \mapsto |\{i \in [1,k] \mid x_i \in [1,m]\}|.$$

Die Wahrscheinlichkeitsverteilung des von f induzierten Wahrscheinlichkeitsraums wird *hypergeometrische Verteilung* zu den Parametern n, m, k genannt und als

$$\mathrm{Hyp}_{n,m,k} := \mathrm{P}_f^{\mathbb{R}}\colon \mathbb{R} \to \mathbb{R}$$

notiert.

20 Graphen

Graphen bilden mathematische Modelle für Netze aller Art, wie bspw. Straßen- und Schienennetze, Rechnernetze oder auch die Struktur des Internets, und sind deshalb für die Informatik besonders relevant. Im Rahmen dieser Vorlesung beschränken wir uns im Wesentlichen auf einige grundlegende Konzepte zur Beschreibung und Modifikation von Graphen – theoretische Entwicklungen überlassen wir weitgehend weiterführenden Veranstaltungen.
Warnend sei zu Beginn angemerkt, dass insbesondere in der Graphentheorie die Terminologiebildung nicht sehr einheitlich ist – die hier eingeführten Konzepte können in anderen Texten leicht unterschiedliche Bedeutungen haben.

Begriffsbildung

Wir beginnen mit der Definition eines Graphen:

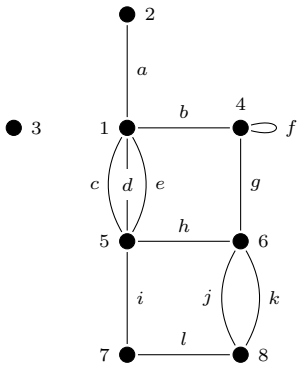
(20.1) Definition (Graph)**.** Ein *Graph* (genauer ein *ungerichteter Graph*) besteht aus Mengen V und E zusammen mit einer Abbildung $W\colon E \to \mathrm{Pot}(V)$ so, dass $W(a)$ für alle $a \in E$ nicht leer und endlich mit $|W(a)| \leq 2$ ist. Die Menge V wird *Eckenmenge* des Graphen und ihre Elemente werden *Ecken* (oder *Eckpunkte* oder *Punkte* oder *Knoten* oder *Objekte*) im Graphen genannt. Die Menge E wird *Kantenmenge* des Graphen und ihre Elemente werden *Kanten* im Graphen genannt. Für $a \in E$ wird $W(a)$ die *Eckenmenge* von a und ihre Elemente werden *Endpunkte* von a genannt.
Für einen Graphen G mit Eckenmenge V, Kantenmenge E und Abbildung $W\colon E \to \mathrm{Pot}(V)$ so, dass $W(a)$ für $a \in E$ die Eckenmenge von a ist, schreiben wir $\mathrm{V}(G) := V$, $\mathrm{E}(G) := E$ und $\mathrm{V}(a) = \mathrm{V}^G(a) := W(a)$ für $a \in E$.

Graphen werden oft durch Skizzen veranschaulicht:

(20.2) Beispiel. Wir haben einen Graphen G gegeben durch

$$\mathrm{V}(G) = \{1,2,3,4,5,6,7,8\},$$
$$\mathrm{E}(G) = \{a,b,c,d,e,f,g,h,i,j,k,l\}$$

sowie $\mathrm{V}(a) = \{1,2\}$, $\mathrm{V}(b) = \{1,4\}$, $\mathrm{V}(c) = \mathrm{V}(d) = \mathrm{V}(e) = \{1,5\}$, $\mathrm{V}(f) = \{4\}$, $\mathrm{V}(g) = \{4,6\}$, $\mathrm{V}(h) = \{5,6\}$, $\mathrm{V}(i) = \{5,7\}$, $\mathrm{V}(j) = \mathrm{V}(k) = \{6,8\}$, $\mathrm{V}(l) = \{7,8\}$.



In Beispielen werden wir im Folgenden einen Graphen G mit endlicher Eckenmenge und endlicher Kantenmenge üblicherweise durch solche Skizzen wie in Beispiel (20.2) „definieren“, da dies knapper und intuitiver ist als die Angabe von $\mathrm{V}(G)$, $\mathrm{E}(G)$ und $\mathrm{V}(a)$ für $a \in \mathrm{E}(G)$. Wegen der Endlichkeit ist dann stets eine vollständige Formalisierung möglich, auch wenn wir diese nicht explizit angeben.

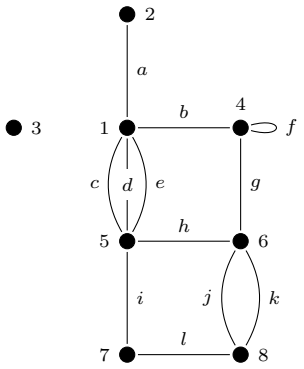
(20.3) Definition (leerer Graph)**.** Der Graph mit Eckenmenge $\emptyset$ heißt *leerer Graph* und wird unter Missbrauch der Notation ebenfalls mit $\emptyset$ bezeichnet.

Untergraphen

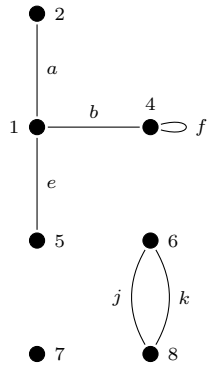
Zur Herausstellung gewisser Teile eines Graphen hat man das Konzept eines Untergraphen:

(20.4) Definition (Untergraph)**.** Es sei ein Graph G gegeben. Ein *Untergraph* von G ist ein Graph U so, dass $\mathrm{V}(U) \subseteq \mathrm{V}(G)$ und $\mathrm{E}(U) \subseteq \mathrm{E}(G)$ gilt, und so, dass für jede Kante a in U die Endpunkte von a in U genau die Endpunkte von a in G sind.

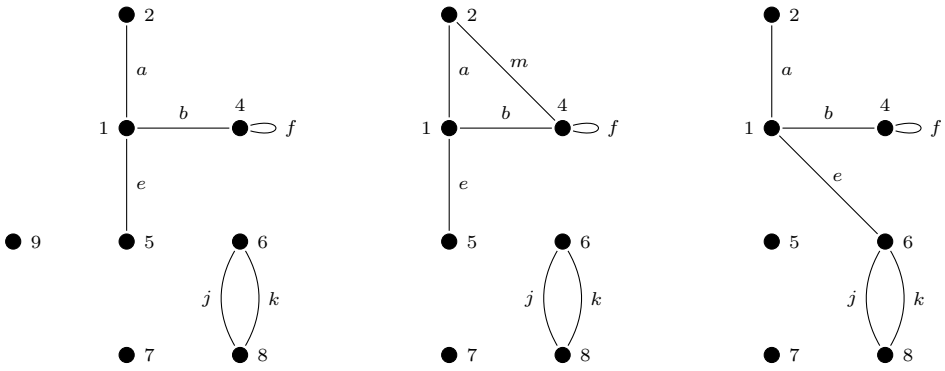
(20.5) Beispiel. Es sei G der folgende Graph.



(a) Der folgende Graph ist ein Untergraph von G.



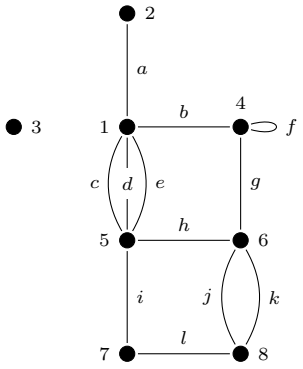
(b) Die folgenden drei Graphen sind keine Untergraphen von G.



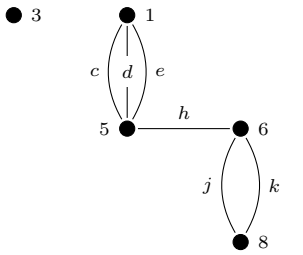
Untergraphen sind durch die Angabe ihrer Ecken- und ihrer Kantenmenge bestimmt.

(20.6) Definition (induzierter Untergraph)**.** Es seien ein Graph G und eine Teilmenge W von $\mathrm{V}(G)$ gegeben. Der Untergraph $G|_W$ von G gegeben durch $\mathrm{V}(G|_W) = W$ und $\mathrm{E}(G|_W) = \{a \in \mathrm{E}(G) \mid \mathrm{V}(a) \subseteq W\}$ heißt der durch W *induzierte Untergraph* von G.

(20.7) Beispiel. Es sei G der folgende Graph.



Dann ist $G|_{\{1,3,5,6,8\}}$ wie folgt gegeben.

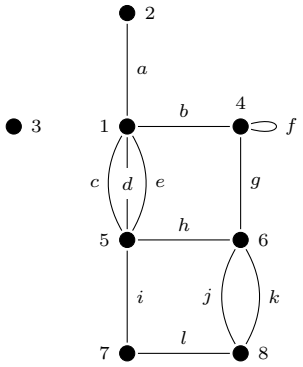


(20.8) Definition (aufspannender Untergraph)**.** Es sei ein Graph G gegeben. Ein Untergraph U von G heißt *aufspannend* (in G), falls

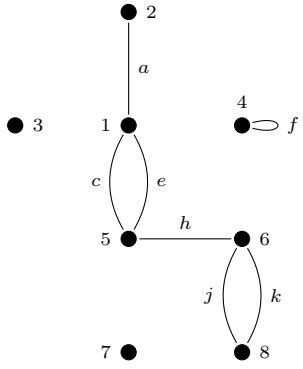
$$\mathrm{V}(U) = \mathrm{V}(G)$$

ist.

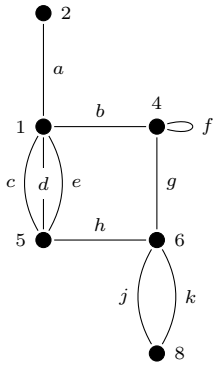
(20.9) Beispiel. Es sei G der folgende Graph.



(a) Der folgende Untergraph von G ist aufspannend.



(b) Der folgende Untergraph von G ist nicht aufspannend.



In Graphalgorithmen werden üblicherweise Untergraphen eines gegebenen Graphen modifiziert. Zur knappen Beschreibung bedienen wir uns folgender Schreibweisen:

(20.10) Notation. Es seien ein Graph G und ein Untergraph U von G gegeben.

(a) Für eine Teilmenge W von $\mathrm{V}(G)$ sei $U \cup W$ der Untergraph von G gegeben durch

$$\mathrm{V}(U \cup W) = \mathrm{V}(U) \cup W,$$
$$\mathrm{E}(U \cup W) = \mathrm{E}(U),$$

und es sei $U \setminus W$ der Untergraph von G gegeben durch

$$\mathrm{V}(U \setminus W) = \mathrm{V}(U) \setminus W,$$
$$\mathrm{E}(U \setminus W) = \{a \in \mathrm{E}(U) \mid \mathrm{V}(a) \subseteq \mathrm{V}(U) \setminus W\}.$$

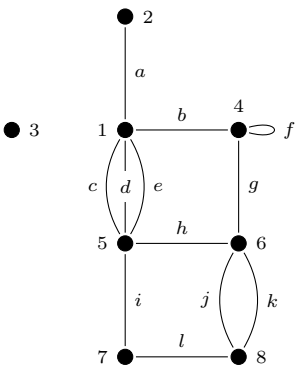
(b) Für eine Teilmenge F von $\mathrm{E}(G)$ sei $U \cup F$ der Untergraph von G gegeben durch

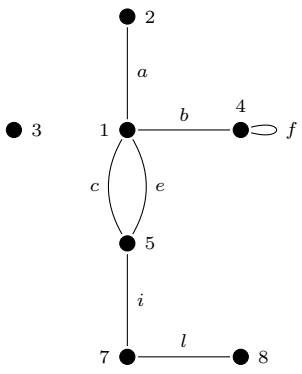
$$\mathrm{V}(U \cup F) = \mathrm{V}(U) \cup \bigcup_{a \in F} \mathrm{V}(a),$$
$$\mathrm{E}(U \cup F) = \mathrm{E}(U) \cup F,$$

und es sei $U \setminus F$ der Untergraph von G gegeben durch

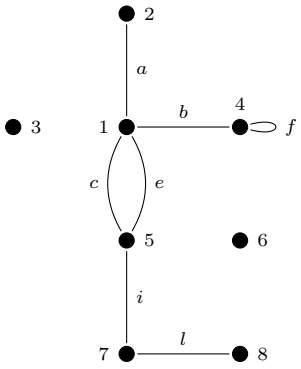
$$\mathrm{V}(U \setminus F) = \mathrm{V}(U),$$
$$\mathrm{E}(U \setminus F) = \mathrm{E}(U) \setminus F.$$

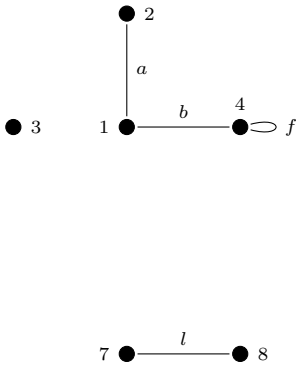
(20.11) Beispiel. Es sei G der im Folgenden links dargestellte Graph und es sei U der im Folgenden rechts dargestellte Untergraph von G.



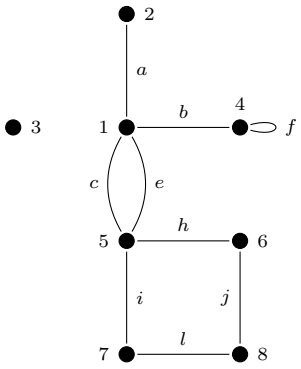


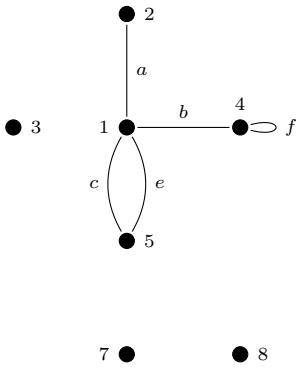
(a) Es ist $U \cup \{5,6\}$ der im Folgenden links dargestellte Untergraph von G und es ist $U \setminus \{5,6\}$ der im Folgenden rechts dargestellte Untergraph von G.





(b) Es ist $U \cup \{h,i,j,l\}$ der im Folgenden links dargestellte Untergraph von G und es ist $U \setminus \{h,i,j,l\}$ der im Folgenden rechts dargestellte Untergraph von G.

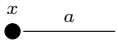




Inzidenz und Adjazenz

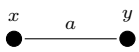
Als nächstes stellen wir einige Begriffe zur Beschreibung der Beziehung von Ecken und Kanten innerhalb von Graphen bereit:

(20.12) Definition (Inzidenz)**.** Es seien ein Graph G, eine Ecke x und eine Kante a in G gegeben. Wir sagen, dass x mit a *inzidiert*, wenn x ein Endpunkt von a ist.



(20.13) Definition (Adjazenz, Nachbarschaft)**.** Es seien ein Graph G und eine Ecke x in G gegeben.

(a) Es seien eine Ecke y in G und eine Kante a in G gegeben. Wir sagen, dass y über a *adjazent* zu x (oder *verbunden* mit x oder *benachbart* zu x) ist, wenn x und y Endpunkte von a sind.

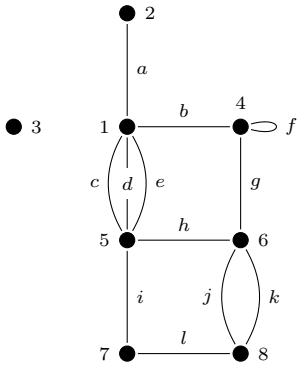


(b) Eine Ecke y in G heißt *adjazent* zu x (oder *verbunden* mit x oder *benachbart* zu x oder ein *Nachbar* von x), wenn es eine Kante a in G so gibt, dass y über a zu x adjazent ist. Die Menge

$$\Gamma(x) = \Gamma^G(x) := \{y \in \mathrm{V}(G) \mid y \text{ ist adjazent zu } x\}.$$

heißt *Nachbarschaft* von x in G.

(20.14) Beispiel. Es sei G der folgende Graph.



(a) Die Ecke 5 inzidiert mit den Kanten c, d, e, h, i und inzidiert nicht mit den Kanten a, b, f, g, j, k, l.

(b) Es ist $\Gamma(5) = \{1, 6, 7\}$.

Beschreibung von Ecken und Kanten

Die folgenden Begriffe dienen der Beschreibung gewisser Phänomene in Graphen.

(20.15) Definition (isolierte Ecke, Schlinge, parallele Kanten)**.** Es sei ein Graph G gegeben.

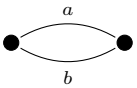
(a) Eine Ecke x in G heißt *isoliert*, falls $\Gamma(x) = \emptyset$ ist.

(b) Eine Kante l in G heißt *Schlinge* (oder *Schleife*), falls sie nur einen Endpunkt hat, und ansonsten eine *Nichtschlinge* (oder *Nichtschleife*).

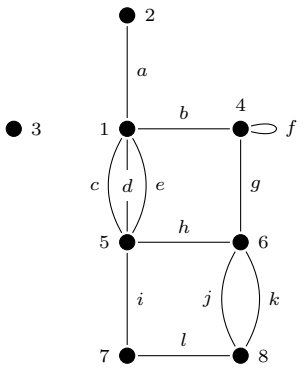
Die *Menge der Schlingen* in G bezeichnen wir mit

$$\mathrm{E}_{\mathrm{loop}}(G) := \{l \in \mathrm{E}(G) \mid l \text{ ist eine Schlinge}\}.$$

(c) Kanten a und b in G heißen *parallel*, falls sie dieselben Endpunkte haben.



(20.16) Beispiel. Es sei G der folgende Graph.



Dann ist 3 eine isolierte Ecke und f eine Schlinge in G. Ferner sind c, d, e sowie j, k jeweils parallel.

Beschreibung von Graphen

Graphen als Ganzes können durch die nachfolgenden Begriffe beschrieben werden:

(20.17) Definition (Mehrfachkanten, schlichter Graph)**.** Es sei ein Graph G gegeben.

(a) Wir sagen, dass es *Mehrfachkanten* in G gibt, falls es parallele Kanten a und b in G mit $a \neq b$ gibt.

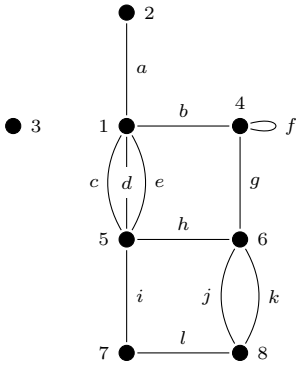
(b) Der Graph G wird *schlicht* (oder *einfach*) genannt, falls es keine Schlingen und keine Mehrfachkanten in G gibt.

In schlichten Graphen sind Kanten durch Angabe ihrer Eckpunkte eindeutig festgelegt. Wir vereinbaren daher:

(20.18) Notation. Es seien ein schlichter Graph G und adjazente Ecken x und y in G gegeben. Wir bezeichnen die eindeutige Kante a in G mit Endpunkten x und y als $(x, y) = (y, x) = xy = yx := a$.

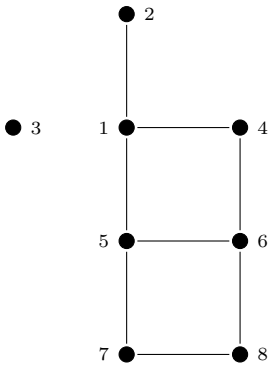
(20.19) Beispiel.

(a) Der Graph



ist nicht schlicht, er hat sowohl Schlingen als auch Mehrfachkanten.

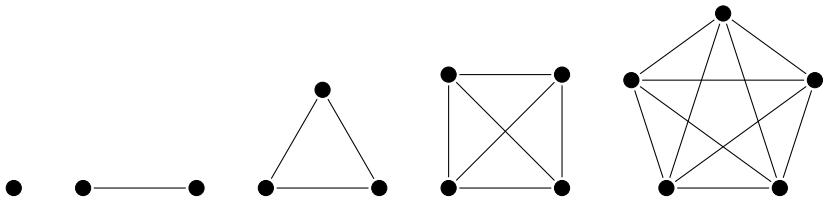
(b) Der Graph



ist schlicht.

(20.20) Definition (vollständiger Graph)**.** Ein Graph G heißt *vollständig*, falls G schlicht ist und je zwei (verschiedene) Ecken in G adjazent sind.

(20.21) Beispiel. Die folgenden fünf Graphen sind vollständig.



Endlichkeit, Ordnung und Größe

In unseren Beispielen haben wir bisher stets endliche Graphen im folgenden Sinn betrachtet:

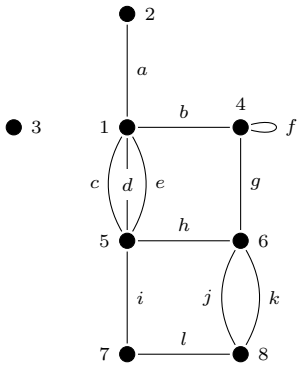
(20.22) Definition (endlicher Graph, Ordnung, Größe)**.**

(a) Ein Graph G heißt *endlich*, wenn seine Eckenmenge $\mathrm{V}(G)$ und seine Kantenmenge $\mathrm{E}(G)$ endlich sind, und ansonsten *unendlich*.

(b) Es sei ein endlicher Graph G gegeben. Wir nennen $|\mathrm{V}(G)|$ die *Ordnung* und $|\mathrm{E}(G)|$ die *Größe* von G.

Im Folgenden werden wir in der Regel endliche Graphen betrachten.

(20.23) Beispiel. Der Graph



ist endlich, er hat die Ordnung 8 und die Größe 12.

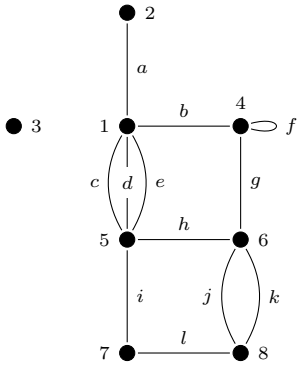
Grad

Der Grad einer Ecke gibt an, mit wievielen Kanten die Ecke inzidiert, wobei Schlingen doppelt gezählt werden.

(20.24) Definition (Eckengrad)**.** Es seien ein endlicher Graph G und eine Ecke x in G gegeben. Der *Grad* (oder *Eckengrad*) von x in G ist definiert als

$$\deg(x) = \deg^G(x) := |\{a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}| + 2\,|\{a \in \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}|.$$

(20.25) Beispiel. Es sei G der folgende Graph.



Dann ist $\deg(1) = 5$, $\deg(2) = 1$, $\deg(3) = 0$, $\deg(4) = 4$, $\deg(5) = 5$, $\deg(6) = 4$, $\deg(7) = 2$, $\deg(8) = 3$.

(20.26) Bemerkung. Es seien ein endlicher Graph G und eine Ecke x in G gegeben. Dann ist

$$\deg(x) = |\{a \in \mathrm{E}(G) \mid x \text{ inzidiert mit } a\}| + |\{a \in \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}|.$$

Beweis. Nach der Summenregel (18.4) gilt

$$\begin{aligned}\deg(x) &= |\{a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}| + 2\,|\{a \in \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}| \\ &= |\{a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}| + |\{a \in \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}| \\ &\quad + |\{a \in \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}| \\ &= |\{a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\} \dot\cup \{a \in \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}| \\ &\quad + |\{a \in \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}| \\ &= |\{a \in \mathrm{E}(G) \mid x \text{ inzidiert mit } a\}| + |\{a \in \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}|.\end{aligned}$$

□

(20.27) Lemma (Handschlaglemma; Euler, 1736)**.** Es sei ein endlicher Graph G gegeben. Dann gilt

$$\sum_{x \in \mathrm{V}(G)} \deg(x) = 2\,|\mathrm{E}(G)|.$$

Beweis. Nach der Summenregel (18.4) gilt einerseits

$$\begin{aligned}&|\{(x,a) \in \mathrm{V}(G) \times (\mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G)) \mid x \text{ inzidiert mit } a\}| \\ &= |\dot{\bigcup_{x \in \mathrm{V}(G)}} \{(x,a) \mid a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G) \text{ so, dass } x \text{ mit } a \text{ inzidiert}\}| \\ &= \sum_{x \in \mathrm{V}(G)} |\{(x,a) \mid a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G) \text{ so, dass } x \text{ mit } a \text{ inzidiert}\}| \\ &= \sum_{x \in \mathrm{V}(G)} |\{a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}|\end{aligned}$$

und andererseits

$$\begin{aligned}&|\{(x,a) \in \mathrm{V}(G) \times (\mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G)) \mid x \text{ inzidiert mit } a\}| \\ &= |\dot{\bigcup_{a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G)}} \{(x,a) \mid x \in \mathrm{V}(G) \text{ so, dass } x \text{ mit } a \text{ inzidiert}\}| \\ &= \sum_{a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G)} |\{(x,a) \mid x \in \mathrm{V}(G) \text{ so, dass } x \text{ mit } a \text{ inzidiert}\}| \\ &= \sum_{a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G)} |\{x \in \mathrm{V}(G) \mid x \text{ inzidiert mit } a\}| = \sum_{a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G)} |\mathrm{V}(a)| = \sum_{a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G)} 2 \\ &= 2\,|\mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G)|.\end{aligned}$$

Analog gilt

$$|\{(x,a) \in \mathrm{V}(G) \times \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}| = \sum_{x \in \mathrm{V}(G)} |\{a \in \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}|$$

sowie

$$\begin{aligned}|\{(x,a) \in \mathrm{V}(G) \times \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}| &= \sum_{a \in \mathrm{E}_{\mathrm{loop}}(G)} |\{x \in \mathrm{V}(G) \mid x \text{ inzidiert mit } a\}| \\ &= \sum_{a \in \mathrm{E}_{\mathrm{loop}}(G)} |\mathrm{V}(a)| = \sum_{a \in \mathrm{E}_{\mathrm{loop}}(G)} 1 = |\mathrm{E}_{\mathrm{loop}}(G)|.\end{aligned}$$

Folglich ist

$$\sum_{x \in \mathrm{V}(G)} |\{a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}| = 2\,|\mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G)|,$$

$$\sum_{x \in \mathrm{V}(G)} |\{a \in \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}| = |\mathrm{E}_{\mathrm{loop}}(G)|.$$

Wir erhalten

$$\begin{aligned}
&\sum_{x\in \mathrm{V}(G)} \deg(x)\\
&= \sum_{x\in \mathrm{V}(G)} \left(|\{a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}| + 2\,|\{a \in \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}|\right)\\
&= \sum_{x\in \mathrm{V}(G)} |\{a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}| + 2 \sum_{x\in \mathrm{V}(G)} |\{a \in \mathrm{E}_{\mathrm{loop}}(G) \mid x \text{ inzidiert mit } a\}|\\
&= 2\,|\mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G)| + 2\,|\mathrm{E}_{\mathrm{loop}}(G)| = 2(|\mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G)| + |\mathrm{E}_{\mathrm{loop}}(G)|) = 2\,|\mathrm{E}(G)|. \qquad \square
\end{aligned}$$

(20.28) Korollar. Es sei ein endlicher Graph G gegeben. Dann ist $|\{x \in \mathrm{V}(G) \mid \deg(x) \text{ ist ungerade}\}|$ gerade.

Beweis. Nach dem Handschlaglemma (20.27) ist

$$\begin{aligned}
0 \equiv_2 \sum_{x\in \mathrm{V}(G)} \deg(x) &= \sum_{\substack{x\in \mathrm{V}(G)\\ \deg(x) \text{ ist gerade}}} \deg(x) + \sum_{\substack{x\in \mathrm{V}(G)\\ \deg(x) \text{ ist ungerade}}} \deg(x)\\
\equiv_2 \sum_{\substack{x\in \mathrm{V}(G)\\ \deg(x) \text{ ist gerade}}} 0 + \sum_{\substack{x\in \mathrm{V}(G)\\ \deg(x) \text{ ist ungerade}}} 1 &= |\{x \in \mathrm{V}(G) \mid \deg(x) \text{ ist ungerade}\}|. \qquad \square
\end{aligned}$$

Kantenfolgen

Dient ein Graph etwa als Modell für ein Straßennetz, so lässt sich ein Abgehen gewisser Straßen in einer bestimmten Reihenfolge mit Hilfe von Kantenfolgen modellieren:

(20.29) Definition (Kantenfolge)**.** Es sei ein Graph G gegeben.

(a) Es seien Ecken x und y in G gegeben. Eine *Kantenfolge* (genauer *endliche Kantenfolge*) von x nach y in G ist ein Tupel $p = (x_0, a_1, x_1, a_2, \ldots, a_k, x_k)$ für ein $k \in \mathbb{N}_0$ bestehend aus Ecken x_i in G für $i \in [0, k]$ und Kanten a_i in G für $i \in [1, k]$ derart, dass $x_0 = x$ und $x_k = y$ ist und x_{i-1} und x_i für $i \in [1, k]$ die Endpunkte von a_i sind. Die Ecken x_i für $i \in [0, k]$ werden *Ecken der Kantenfolge* und die Kanten a_i für $i \in [1, k]$ werden *Kanten der Kantenfolge* genannt. Wir schreiben $\mathrm{V}(p) = \mathrm{V}^G(p) := \{x_0, \ldots, x_k\}$ und $\mathrm{E}(p) = \mathrm{E}^G(p) := \{a_1, \ldots, a_k\}$. Die Ecke x wird *Anfangspunkt*, die Ecke y wird *Endpunkt* und die Ecken x_i für $i \in [1, k-1]$ werden *innere Punkte* der Kantenfolge genannt. Die nicht-negative ganze Zahl k wird *Länge* der Kantenfolge genannt. Eine Kantenfolge der Länge 0 heißt *trivial*, und ansonsten *nicht-trivial*.

Eine *Kantenfolge* in G ist eine Kantenfolge von x nach y in G für gewisse Ecken x und y in G.

Für eine Kantenfolge $p = (x_0, a_1, x_1, a_2, \ldots, a_k, x_k)$ in G schreiben wir auch $p = x_0 a_1 x_1 a_2 \ldots a_k x_k$. Ist G schlicht, so schreiben wir unter Missbrauch der Notation auch $x_0 \ldots x_k = (x_0, \ldots, x_k) := p$.

(b) Eine Kantenfolge in G heißt *geschlossen*, falls ihr Anfangspunkt auch ihr Endpunkt ist, ansonsten *offen*.

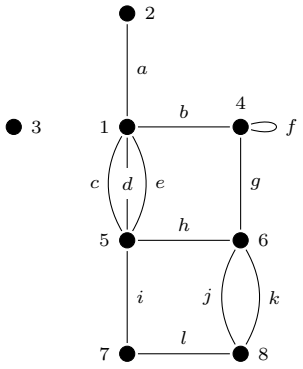
(c) Ein *Kantenzug* in G ist eine Kantenfolge in G, in welcher alle Kanten verschieden sind.

(d) Eine *Tour* (oder ein *Rundgang*) in G ist ein geschlossener Kantenzug in G.

(e) Ein *Weg* in G ist ein Kantenzug in G, in welchem alle Ecken bis auf möglicherweise Anfangs- und Endpunkt verschieden sind.

(f) Ein *Kreis* in G ist ein geschlossener Weg in G.

(20.30) Beispiel. Es sei G der folgende Graph.

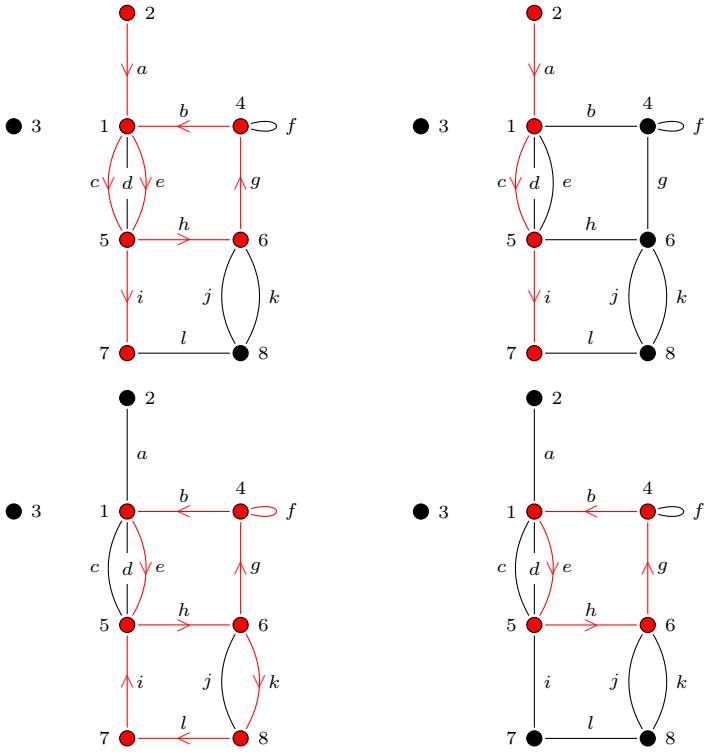


(a) Die Kantenfolge $2a1c5h6g4b1e5i7$ in G ist ein offener Kantenzug, aber kein Weg.

(b) Die Kantenfolge $2a1c5i7$ in G ist ein offener Weg.

(c) Die Kantenfolge $1e5h6k8l7i5h6g4f4b1$ in G ist geschlossen, aber keine Tour.

(d) Die Kantenfolge $1e5h6g4b1$ in G ist ein Kreis.



Kantenfolgen lassen sich stets zu Wegen verkürzen:

(20.31) Bemerkung. Es seien ein Graph G, Ecken x und y in G, ein $k \in \mathbb{N}_0$ sowie eine Kantenfolge $p = x_0 a_1 \dots a_k x_k$ von x nach y in G gegeben. Wenn es $i, j \in [0, k-1]$ mit $i < j$ und $x_i = x_j$ gibt, dann ist $p' := x_0 a_1 \dots a_i x_i a_{j+1} \dots a_k x_k$ eine Kantenfolge von x nach y in G mit $\mathrm{E}(p') \subseteq \mathrm{E}(p)$.

(20.32) Korollar. Es seien ein Graph G, Ecken x und y in G sowie eine Kantenfolge p von x nach y in G gegeben. Ferner sei

$$l := \min \{k \in \mathbb{N}_0 \mid \text{es gibt eine Kantenfolge } p' \text{ der Länge } k \text{ von } x \text{ nach } y \text{ in } G \text{ mit } \mathrm{E}(p') \subseteq \mathrm{E}(p)\}$$

und es sei q eine Kantenfolge der Länge l von x nach y in G mit $\mathrm{E}(q) \subseteq \mathrm{E}(p)$. Dann ist q ein Weg von x nach y in G.

Beweis. Es seien Ecken x_i für $i \in [0,l]$ und Kanten a_i für $i \in [1,l]$ mit $q = x_0 a_1 x_1 a_2 \dots a_l x_l$ gegeben. Wegen der Minimalität von l ist für $i,j \in [0,l-1]$ mit $i<j$ dann $(x_0, a_1, \dots, a_i, x_i, a_{j+1}, \dots, a_l, x_l)$ keine Kantenfolge von x nach y, es gilt also $x_i \neq x_j$. Folglich ist q ein Weg. □

(20.33) Bemerkung. Es sei ein Graph G gegeben.

(a) Für jede Schlinge l mit Endpunkt x in G ist xlx ein Kreis in G.

(b) Für parallele Kanten a und b mit Endpunkten x und y in G ist $xaybx$ ein Kreis in G.

Zusammenhang

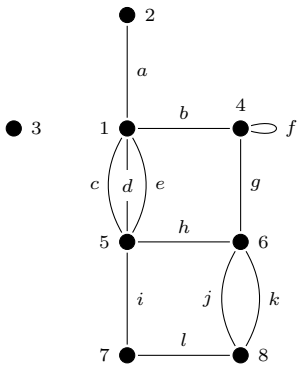
Mit Hilfe von Kantenfolgen lässt sich beschreiben, ob sich ein Graph als „disjunkte Vereinigung“ gewisser induzierter Untergraphen, den Zusammenhangskomponenten, darstellen lässt.

(20.34) Bemerkung. Es sei ein Graph G gegeben. Für $x,y \in \mathrm{V}(G)$ gelte genau dann $x \sim y$, wenn es eine Kantenfolge von x nach y gibt. Dann ist $\sim$ eine Äquivalenzrelation auf $\mathrm{V}(G)$.

Beweis. Es seien $x,y,z \in \mathrm{V}(G)$ mit $x \sim y$ und $y \sim z$ gegeben, so dass es $k,l \in \mathbb{N}_0$ und Kantenfolgen $x_0 a_1 x_1 a_2 \dots a_k x_k$ von $x_0 = x$ nach $x_k = y$ und $y_0 b_1 y_1 b_2 \dots b_l y_l$ von $y_0 = y$ nach $y_l = z$. Dann ist aber $x_k = y = y_0$ und damit $x_0 a_1 x_1 a_2 \dots a_k x_k b_1 y_1 b_2 \dots b_l y_l$ eine Kantenfolge von $x_0 = x$ nach $y_l = z$, es gilt also auch $x \sim z$. Folglich ist $\sim$ transitiv.
Für alle $x \in \mathrm{V}(G)$ ist x eine Kantenfolge von x nach x, es gilt also $x \sim x$. Folglich ist $\sim$ reflexiv.
Es seien $x,y \in \mathrm{V}(G)$ mit $x \sim y$ gegeben, so dass es ein $k \in \mathbb{N}_0$ und eine Kantenfolge $x_0 a_1 x_1 a_2 \dots a_k x_k$ von $x_0 = x$ nach $x_k = y$ gibt. Dann ist $x_k a_k \dots a_2 x_1 a_1 x_0$ eine Kantenfolge von $x_k = y$ nach $x_0 = x$, es gilt also auch $y \sim x$. Folglich ist $\sim$ symmetrisch.
Insgesamt ist $\sim$ eine Äquivalenzrelation auf $\mathrm{V}(G)$. □

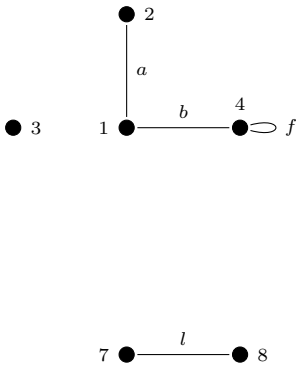
(20.35) Definition (Zusammenhangskomponente)**.** Es sei ein Graph G gegeben. Die Äquivalenzrelation $\sim$ auf $\mathrm{V}(G)$ aus Bemerkung (20.34) heißt *Zusammenhang*. Für $x \in \mathrm{V}(G)$ heißt $G|_{[x]}$ die *Zusammenhangskomponente* von x (in G).
Eine Zusammenhangskomponente heißt *trivial*, falls ihre Eckenmenge nur aus einer isolierten Ecke besteht, und ansonsten *nicht-trivial*.

(20.36) Beispiel. Es sei G der folgende Graph.



(a) Der Graph G hat die Zusammenhangskomponenten $G|_{[1]}$ und $G|_{[3]}$.

(b) Der Graph $H := G \setminus \{5, 6\}$ hat die Zusammenhangskomponenten $H|_{[1]}$, $H|_{[3]}$ und $H|_{[7]}$.



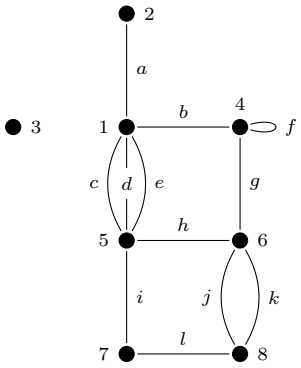
(20.37) Bemerkung. Es seien ein Graph G und Ecken x und y in G gegeben. Genau dann gilt $x \sim y$, wenn es einen Weg von x nach y gibt.

Beweis. Wenn $x \sim y$, d.h. wenn es eine Kantenfolge von x nach y in G gibt, dann gibt es nach Korollar (20.32) auch einen Weg von x nach y in G. Wenn es umgekehrt einen Weg von x nach y gibt, dann gibt es insbesondere auch eine Kantenfolge von x nach y in G, da jeder Weg eine Kantenfolge ist. □

(20.38) Definition (zusammenhängender Graph)**.** Ein Graph G heißt *zusammenhängend*, falls für alle Ecken x und y in G stets $x \sim y$ gilt, sonst *unzusammenhängend*.

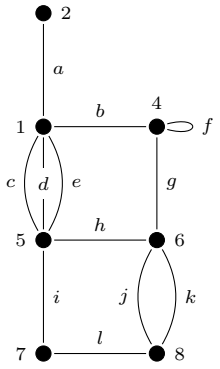
(20.39) Beispiel.

(a) Der Graph



ist unzusammenhängend.

(b) Der Graph



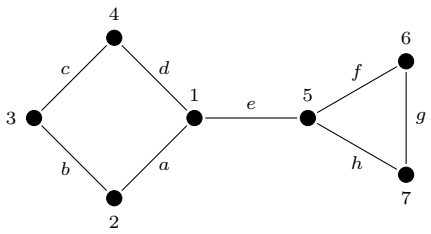
ist zusammenhängend.

Brücken

(20.40) Definition (Brücke)**.** Es seien ein Graph G, Ecken x und y in G und eine Kante a in G mit den Endpunkten x und y gegeben. Wir nennen a eine *Brücke* in G, falls $x \nsim y$ in $G \setminus \{a\}$ gilt, und ansonsten eine *Nichtbrücke* in G.

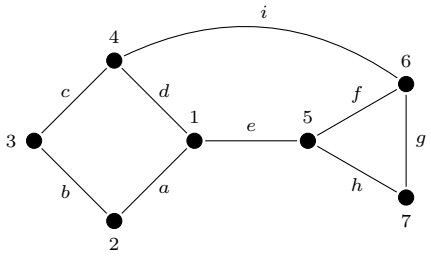
(20.41) Beispiel.

(a) Es sei G der folgende Graph.



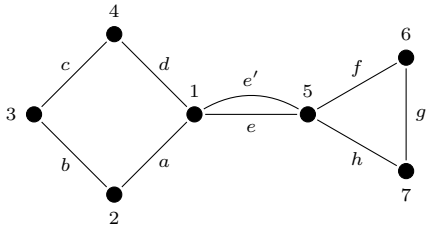
Dann ist e eine Brücke in G.

(b) Es sei G der folgende Graph.



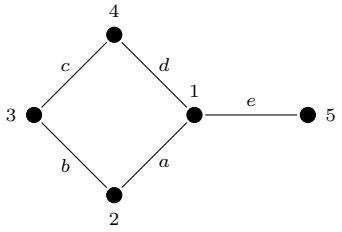
Dann ist e eine Nichtbrücke in G.

(c) Es sei G der folgende Graph.



Dann ist e eine Nichtbrücke in G.

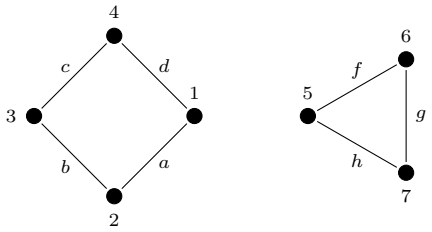
(d) Es sei G der folgende Graph.



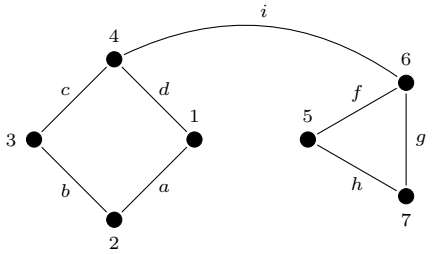
Dann ist e eine Brücke in G.

Beweis.

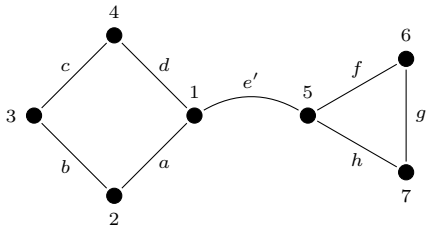
(a) In $G \setminus \{e\}$ gibt es keine Kantenfolge von 1 nach 5, so dass $1 \nsim 5$ gilt. Folglich ist e eine Brücke in G.



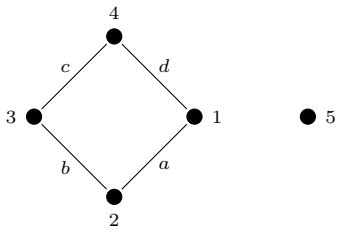
(b) In $G \setminus \{e\}$ ist $1d4i6f5$ eine Kantenfolge von 1 nach 5, so dass $1 \sim 5$ gilt. Folglich ist e eine Nichtbrücke in G.



(c) In $G \setminus \{e\}$ ist $1e'5$ eine Kantenfolge von 1 nach 5, so dass $1 \sim 5$ gilt. Folglich ist e eine Nichtbrücke in G.



(d) In $G \setminus \{e\}$ ist 5 eine isolierte Ecke, so dass insbesondere $1 \nsim 5$ gilt. Folglich ist e eine Brücke in G.



□

(20.42) Bemerkung. Es sei ein Graph G gegeben.

(a) Jede Schlinge in G ist eine Nichtbrücke in G.

(b) Es sei eine Ecke x in G gegeben, welche zu genau einer Nichtschlinge a in G inzident ist. Dann ist a eine Brücke.

Beweis.

(a) Es sei eine Schlinge l in G gegeben und es sei x die zu l inzidente Ecke in G. Wegen der Reflexivität von $\sim$ gilt dann $x \sim x$ in $G \setminus \{l\}$, d.h. l ist eine Nichtbrücke in G.

(b) Es sei y die von x verschiedene zu a inzidente Ecke in G. Da a die einzige zu x inzidente Nichtschlinge a in G ist, sind alle zu x inzidenten Kanten in $G \setminus \{a\}$ Schlingen. Insbesondere gibt es keine Kantenfolge von x nach y in $G \setminus \{a\}$. Folglich gilt $x \nsim y$ in $G \setminus \{a\}$, d.h. a ist eine Brücke in G. □

(20.43) Proposition. Es seien ein endlicher Graph G und eine Brücke a in G mit den Endpunkten x und y gegeben. Dann gibt es eine Ecke z in der Zusammenhangskomponente $(G \setminus \{a\})|_{[y]}$ so, dass $\deg^G(z)$ ungerade ist.

Beweis. Es sei $U := (G\setminus\{a\})|_{[y]}$ und es sei $p := |\{z \in \mathrm{V}(U) \mid \deg^U(z) \text{ ist ungerade}\}|$. Wenn $\deg^G(y)$ ungerade ist, so ist $z := y$ eine Ecke in U derart, dass $\deg^G(z) = \deg^G(y)$ ungerade ist. Daher sei im Folgenden angenommen, dass $\deg^G(y)$ gerade ist. Dann ist

$$\deg^U(y) = \deg^{G\setminus\{a\}}(y) = \deg^G(y) - 1$$

ungerade und damit $p \geq 1$. Nach Korollar (20.28) ist jedoch p gerade, so dass $p \geq 1$ bereits $p \geq 2$ impliziert. Folglich gibt es eine von y verschiedene Ecke z in U so, dass $\deg^U(z)$ ungerade ist. Wegen $z \neq y$ ist allerdings $\deg^G(z) = \deg^{G\setminus\{a\}}(z) = \deg^U(z)$ und damit insbesondere $\deg^G(z)$ ungerade. □

Eulerzüge und Eulertouren

(20.44) Definition (Eulerzug, Eulertour)**.** Es sei ein endlicher Graph G gegeben.

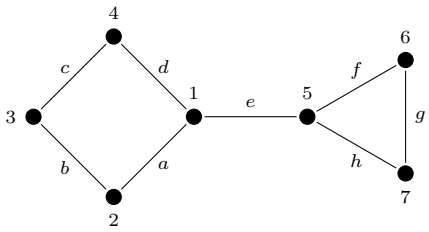
(a) Ein *Eulerzug* in G ist ein Kantenzug in G, in welcher jede Kante von G (genau einmal) vorkommt.

(b) Eine *Eulertour* (oder *Eulerrundgang*) in G ist ein geschlossener Eulerzug in G.

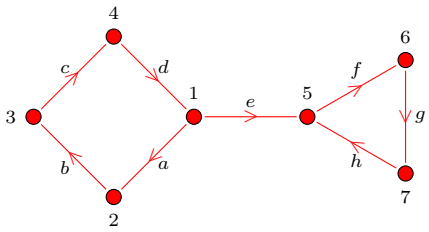
In einem Graphen ist ein Eulerzug also ein Kantenzug, in welchem jede Kante des Graphen (genau einmal) vorkommt. Entsprechend ist eine Eulertour eine Tour, in welcher jede Kante genau einmal vorkommt.

(20.45) Beispiel.

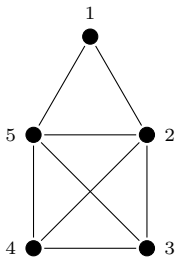
(a) (i) Es sei G der folgende Graph.



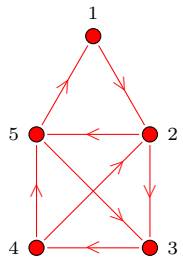
Die Kantenfolge $1a2b3c4d1e5f6g7h5$ ist ein offener Eulerzug in G.



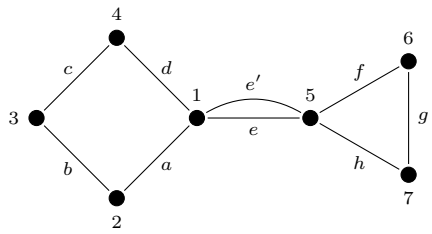
(ii) Es sei G der folgende schlichte Graph.



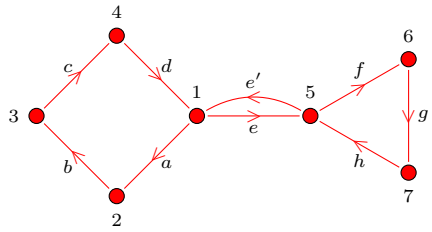
Die Kantenfolge 451234253 ist ein offener Eulerzug in G.



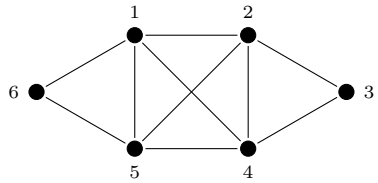
(b) (i) Es sei G der folgende Graph.



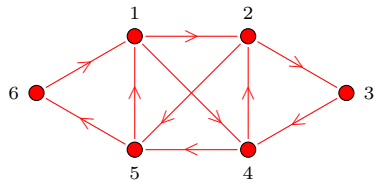
Die Kantenfolge $1a2b3c4d1e5f6g7h5e'1$ ist eine Eulertour in G.



(ii) Es sei G der folgende schlichte Graph.



Die Kantenfolge 12342514561 ist eine Eulertour in G.



Beweis.

(a) (i) In der Kantenfolge $1a2b3c4d1e5f6g7h5$ kommt jede Kante von G genau einmal vor. Folglich ist $1a2b3c4d1e5f6g7h5$ ein offener Eulerzug in G.

(ii) In der Kantenfolge 451234253 kommt jede Kante von G genau einmal vor. Folglich ist 451234253 ein offener Eulerzug in G.

(b) (i) In der Kantenfolge $1a2b3c4d1e5f6g7h5e'1$ kommt jede Kante von G genau einmal vor. Folglich ist $1a2b3c4d1e5f6g7h5e'1$ eine Eulertour in G.

(ii) In der Kantenfolge 12342514561 kommt jede Kante von G genau einmal vor. Folglich ist 12342514561 eine Eulertour in G. □

(20.46) Bemerkung. Es seien ein Graph G, Ecken x und y und eine Kante a in G mit den Endpunkten x und y gegeben. Eine Kantenfolge $p = x_0a_1x_1a_2 \dots a_kx_k$ von x nach y in $G \setminus \{a\}$ für ein $k \in \mathbb{N}_0$ ist genau dann ein Eulerzug in $G \setminus \{a\}$, wenn $x_0a_1x_1a_2 \dots a_kx_kax$ eine Eulertour in G ist.

(20.47) Bemerkung. Es seien ein zusammenhängender endlicher Graph G, Ecken x und y in G sowie ein Eulerzug p von x nach y gegeben.

(a) Für $z \in \mathrm{V}(G) \setminus \{x, y\}$ ist $\deg(z)$ gerade.

(b) Wenn p offen ist, dann sind $\deg(x)$ und $\deg(y)$ ungerade. Wenn p geschlossen ist, dann ist $\deg(x) = \deg(y)$ gerade.

Beweis. Es sei m die Größe von G und es seien Ecken x_i in G für $i \in [0, m]$ und Kanten a_i in G für $i \in [1, m]$ mit $p = x_0a_1x_1a_2 \dots a_mx_m$ gegeben. Für jede Ecke z in G gilt dann

$$\begin{aligned}
\deg(z) &= |\{a \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G) \mid z \text{ inzidiert mit } a\}| + 2\,|\{a \in \mathrm{E}_{\mathrm{loop}}(G) \mid z \text{ inzidiert mit } a\}| \\
&= |\{i \in [1, m] \mid a_i \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G) \text{ und } z \text{ inzidiert mit } a_i\}| \\
&\quad + 2\,|\{i \in [1, m] \mid a_i \in \mathrm{E}_{\mathrm{loop}}(G) \text{ und } z \text{ inzidiert mit } a_i\}| \\
&= |\{i \in [1, m] \mid a_i \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G) \text{ und } z = x_{i-1}\}| \\
&\quad + |\{i \in [1, m] \mid a_i \in \mathrm{E}(G) \setminus \mathrm{E}_{\mathrm{loop}}(G) \text{ und } z = x_i\}| \\
&\quad + |\{i \in [1, m] \mid a_i \in \mathrm{E}_{\mathrm{loop}}(G) \text{ und } z = x_{i-1}\}| + |\{i \in [1, m] \mid a_i \in \mathrm{E}_{\mathrm{loop}}(G) \text{ und } z = x_i\}| \\
&= |\{i \in [1, m] \mid z = x_{i-1}\}| + |\{i \in [1, m] \mid z = x_i\}| \\
&= |\{i \in [0, m-1] \mid z = x_i\}| + |\{i \in [1, m] \mid z = x_i\}| = \delta_{z,x} + 2\,|\{i \in [1, m-1] \mid z = x_i\}| + \delta_{z,y}.
\end{aligned}$$

(a) Für $z \in \mathrm{V}(G) \setminus \{x, y\}$ ist $\delta_{z,x} = 0 = \delta_{z,y}$ und damit $\deg(z) = 2\,|\{i \in [1, m-1] \mid z = x_i\}|$ gerade.

(b) Wenn p offen ist, dann ist $x \neq y$, also $\delta_{x,y} = 0 = \delta_{y,x}$ und damit $\deg(x) = 1 + 2\,|\{i \in [1, m-1] \mid z = x_i\}|$ und $\deg(y) = 2\,|\{i \in [1, m-1] \mid z = x_i\}| + 1$ ungerade. Wenn p geschlossen ist, dann ist $x = y$, also $\delta_{x,y} = 1 = \delta_{y,x}$ und damit $\deg(x) = 1 + 2\,|\{i \in [1, m-1] \mid z = x_i\}| + 1 = \deg(y)$ gerade. □

(20.48) Satz (Algorithmus von Fleury)**.** Es seien $m \in \mathbb{N}_0$, ein zusammenhängender endlicher Graph G der Größe m und Ecken x und y in G so gegeben, dass

$$\deg^G(z) \equiv_2 \begin{cases} 0 & \text{für } z \in \mathrm{V}(G) \setminus \{x, y\}, \\ 0 & \text{für } z \in \{x, y\}, \text{ falls } x = y, \\ 1 & \text{für } z \in \{x, y\}, \text{ falls } x \neq y. \end{cases}$$

Ferner seien Tupel $(a_1, \dots, a_m)$, $(x_0, \dots, x_m)$, $(G_0, \dots, G_m)$ wie folgt rekursiv gegeben.
Für $i \in [1, m]$ sei a_i eine zu x_{i-1} inzidente Nichtbrücke in G_{i-1}, sofern eine solche existiert, und ansonsten eine zu x_{i-1} inzidente Brücke in G_{i-1}.
Es sei $x_0 := x$. Für $i \in [1, m]$ sei x_i der Endpunkt von a_i in G_{i-1} mit $\mathrm{V}^{G_{i-1}}(a_i) = \{x_{i-1}, x_i\}$.
Es sei

$$G_i := \begin{cases} G & \text{für } i = 0, \\ G_{i-1} \setminus \{a_i\} & \text{für } i \in [1, m], \text{ falls } a_i \text{ eine Nichtbrücke in } G_{i-1} \text{ ist}, \\ G_{i-1} \setminus \{x_{i-1}\} & \text{für } i \in [1, m], \text{ falls } a_i \text{ eine Brücke in } G_{i-1} \text{ ist}. \end{cases}$$

Dann gilt:

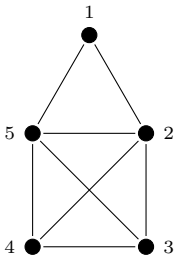
(a) Für alle $i \in [0, m]$ ist G_i ein zusammenhängender endlicher Graph der Größe $m - i$ mit

$$\deg^{G_i}(z) \equiv_2 \begin{cases} 0 & \text{für } z \in \mathrm{V}(G_i) \setminus \{x_i, y\}, \\ 0 & \text{für } z \in \{x_i, y\}, \text{ falls } x_i = y, \\ 1 & \text{für } z \in \{x_i, y\}, \text{ falls } x_i \neq y. \end{cases}$$

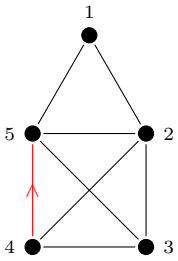
Für alle $i \in [1, m]$ gibt es genau dann keine zu x_{i-1} inzidente Nichtbrücke in G_{i-1}, wenn $\deg^{G_{i-1}}(x_{i-1}) = 1$ ist.

(b) Es ist $x_0 a_1 x_1 a_2 \dots a_m x_m$ ein Eulerzug von x nach y in G.

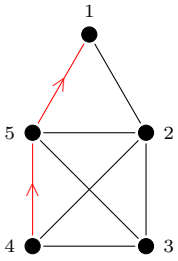
Alternativer Beweis von Beispiel (20.45)(a)(ii). Wir verwenden den Algorithmus von Fleury (20.48).
Es sei $x_0 := 4$ und $G_0 := G$.



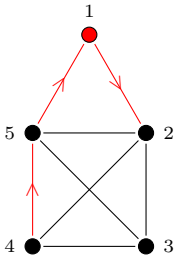
Eine zu $x_0 = 4$ inzidente Nichtbrücke in G_0 ist $a_1 := 45$. Daher setzen wir $x_1 := 5$ und $G_1 := G_0 \setminus \{45\}$.



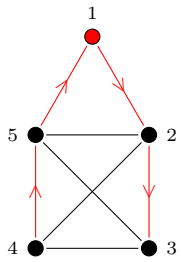
Eine zu $x_1 = 5$ inzidente Nichtbrücke in G_1 ist $a_2 := 51$. Daher setzen wir $x_2 := 1$ und $G_2 := G_1 \setminus \{51\}$.



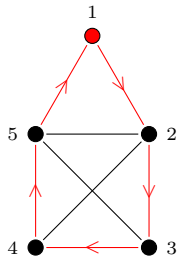
Die einzige zu $x_2 = 1$ inzidente Kante in G_2 ist die Brücke $a_3 := 12$. Daher setzen wir $x_3 := 2$ und $G_3 := G_2 \setminus \{1\}$.



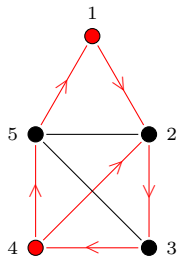
Eine zu $x_3 = 2$ inzidente Nichtbrücke in G_3 ist $a_4 := 23$. Daher setzen wir $x_4 := 3$ und $G_4 := G_3 \setminus \{23\}$.



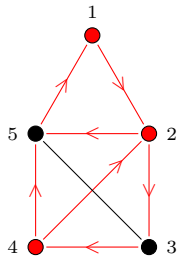
Eine zu $x_4 = 3$ inzidente Nichtbrücke in G_4 ist $a_5 := 34$. Daher setzen wir $x_5 := 4$ und $G_5 := G_4 \setminus \{34\}$.



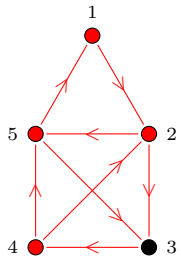
Die einzige zu $x_5 = 4$ inzidente Kante in G_5 ist die Brücke $a_6 := 42$. Daher setzen wir $x_6 := 2$ und $G_6 := G_5 \setminus \{4\}$.



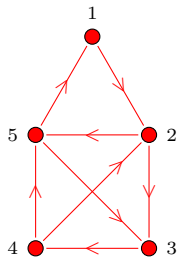
Die einzige zu $x_6 = 2$ inzidente Kante in G_6 ist die Brücke $a_7 := 25$. Daher setzen wir $x_7 := 5$ und $G_7 := G_6 \setminus \{2\}$.



Die einzige zu $x_7 = 5$ inzidente Kante in G_7 ist die Brücke $a_8 := 53$. Daher setzen wir $x_8 := 3$ und $G_8 := G_7 \setminus \{5\}$.



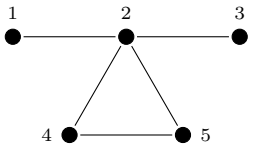
Nach dem Algorithmus von Fleury (20.48) ist $x_0x_1x_2x_3x_4x_5x_6x_7x_8 = 451234253$ ein Eulerzug in G.



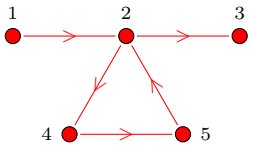
□

Im vorangegangenen Beispiel waren in jedem Schritt $i \in [1, 8]$ mit $\deg^{G_{i-1}}(x_{i-1}) > 1$ alle zu x_{i-1} inzidenten Kanten stets Nichtbrücken, so dass wir beispielsweise statt $a_1 = 45$ alternativ auch $a_1' := 42$ oder $a_1' := 43$ hätten betrachten können. Dies muss nicht der Fall sein, wie wir im nachfolgenden Beispiel sehen werden: Dort könnten wir statt $a_2 = 24$ auch $a_2' := 25$ betrachten, aber nicht $a_2'' := 23$, da dies eine Brücke in G_1 ist.

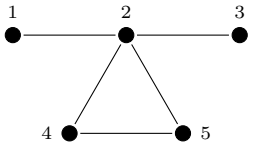
(20.49) Beispiel. Es sei G der folgende schlichte Graph.



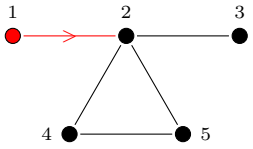
Die Kantenfolge 124523 ist ein Eulerzug in G.



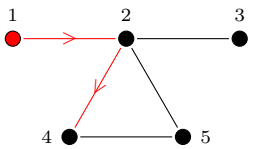
Beweis. Wir verwenden den Algorithmus von Fleury (20.48).
Es sei $x_0 := 1$ und $G_0 := G$.



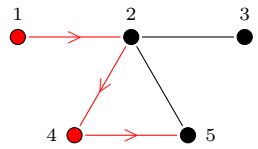
Die einzige zu $x_0 = 1$ inzidente Kante in G_0 ist die Brücke $a_1 := 12$. Daher setzen wir $x_1 := 2$ und $G_1 := G_0 \setminus \{1\}$.



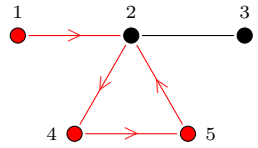
Eine zu $x_1 = 2$ inzidente Nichtbrücke in G_1 ist $a_2 := 24$. Daher setzen wir $x_2 := 4$ und $G_2 := G_1 \setminus \{24\}$.



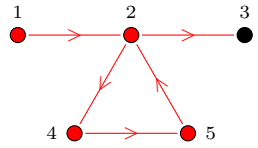
Die einzige zu $x_2 = 4$ inzidente Kante in G_2 ist die Brücke $a_3 := 45$. Daher setzen wir $x_3 := 5$ und $G_3 := G_2 \setminus \{4\}$.



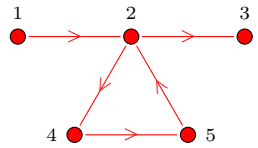
Die einzige zu $x_3 = 5$ inzidente Kante in G_3 ist die Brücke $a_4 := 52$. Daher setzen wir $x_4 := 2$ und $G_4 := G_3 \setminus \{5\}$.



Die einzige zu $x_4 = 5$ inzidente Kante in G_4 ist die Brücke $a_5 := 23$. Daher setzen wir $x_5 := 3$ und $G_5 := G_4 \setminus \{2\}$.



Nach dem Algorithmus von Fleury (20.48) ist $x_0x_1x_2x_3x_4x_5 = 124523$ ein Eulerzug in G.



□

(20.50) Satz (Euler 1736; Hierholzer 1873)**.** Es sei ein zusammenhängender endlicher Graph G gegeben.

(a) Genau dann gibt es einen offenen Eulerzug in G, wenn es genau zwei Ecken ungeraden Grades in G gibt.

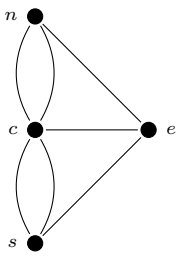
(b) Genau dann gibt es eine Eulertour in G, wenn alle Ecken in G geraden Grad haben.

Beweis.

(a) Wenn es einen offenen Eulerzug p in G gibt, dann haben nach Bemerkung (20.47) Anfangs- und Endpunkt von p ungeraden Grad und alle anderen Ecken in G geraden Grad. Umgekehrt, wenn es genau zwei Ecken ungeraden Grades in G gibt, so liefert der Algorithmus von Fleury (20.48) einen offenen Eulerzug in G von einer dieser beiden Ecken zur anderen.

(b) Wenn es eine Eulertour in G gibt, dann haben nach Bemerkung (20.47) alle Ecken in G geraden Grad. Umgekehrt, wenn alle Ecken in G geraden Grad haben, so liefert der Algorithmus von Fleury (20.48) eine Eulertour in G. □

(20.51) Beispiel (Königsberger Brückenproblem)**.** Es sei G der folgende Graph.



Dann gibt es keine Eulertour in G.

Beweis. Es ist $\deg(n) = \deg(s) = \deg(e) = 3$ und $\deg(c) = 5$. Nach Satz (20.50)(b) gibt es keine Eulertour in G. □

Hamiltonwege und Hamiltonkreise

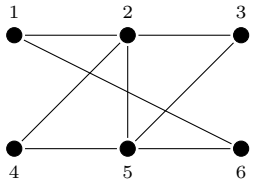
(20.52) Definition (Hamiltonweg, Hamiltonkreis)**.** Es sei ein endlicher Graph G gegeben.

(a) Ein *Hamiltonweg* (oder *Hamiltonpfad*) in G ist ein Weg in G, in welcher jede Ecke von G (genau einmal) vorkommt.

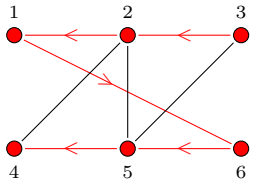
(b) Ein *Hamiltonkreis* in G ist ein geschlossener Hamiltonweg in G.

(20.53) Beispiel.

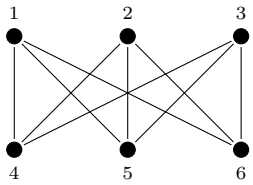
(a) Es sei G der folgende schlichte Graph.



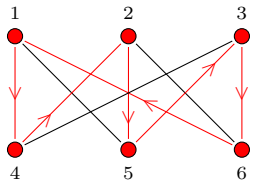
Die Kantenfolge 321654 ist ein offener Hamiltonweg in G.



(b) Es sei G der folgende schlichte Graph.



Die Kantenfolge 1425361 ist ein Hamiltonkreis in G



Wälder und Bäume

Spezielle Arten von Graphen sind Wälder und Bäume:

(20.54) Definition (Wald, Baum, Blatt)**.**

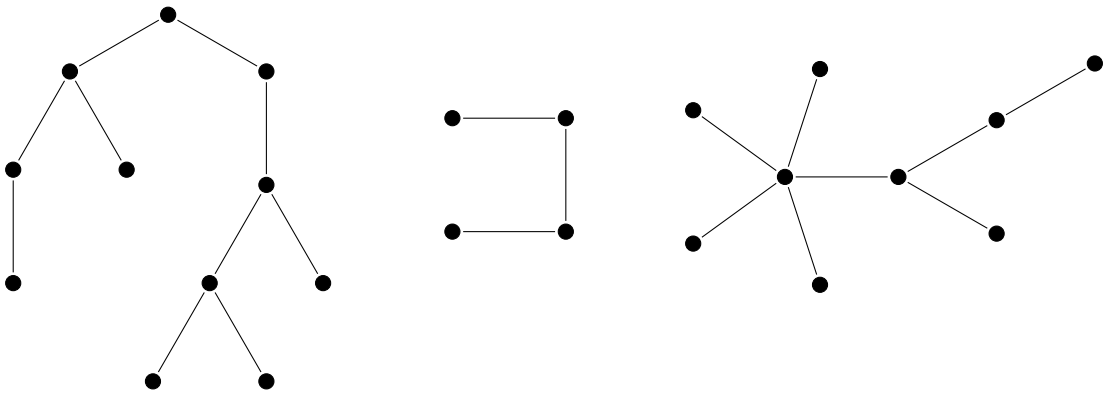
(a) Ein *Wald* ist ein Graph, in welchem es keine nicht-trivialen Kreise gibt.

(b) Ein *Baum* ist ein zusammenhängender Wald.

(c) Es sei ein Wald W gegeben. Ein *Blatt* in W ist eine Ecke in W, welche zu höchstens einer Kante inzident ist.

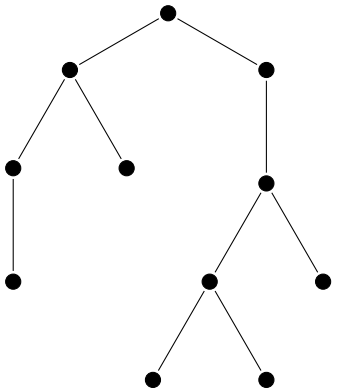
(20.55) Beispiel.

(a) Der Graph



ist ein Wald, in welchem es 13 Blätter gibt.

(b) Der Graph



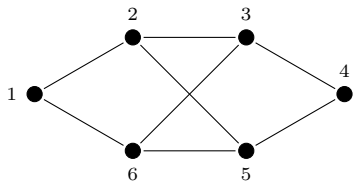
ist ein Baum, in welchem es 5 Blätter gibt.

(20.56) Bemerkung. Jeder Wald ist stets ein schlichter Graph.

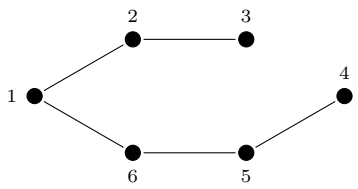
Beweis. Es sei ein Wald G gegeben. Dann gibt es keine nicht-trivialen Kreise in G. Nach Bemerkung (20.33)(a) gibt es also insbesondere keine Schlingen und nach Bemerkung (20.33)(b) gibt es insbesondere keine Mehrfachkanten in G. Folglich ist G schlicht. □

(20.57) Definition (Spannbaum)**.** Es sei ein Graph G gegeben. Ein *Spannbaum* von G ist ein aufspannender Untergraph U von G, welcher ein Baum ist.

(20.58) Beispiel. Es sei G der folgende schlichte Graph.



Dann ist



ein Spannbaum von G.

Gefärbte Graphen

(20.59) Definition (gefärbter Graph)**.** Ein *gefärbter Graph* (oder *eckengefärbter Graph*) besteht aus einem Graphen G zusammen mit einer Familie c über $\mathrm{V}(G)$ derart, dass für alle adjazenten Ecken x und y in G stets

$$c_x \neq c_y$$

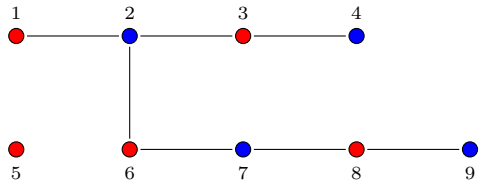
ist. Unter Missbrauch der Notation bezeichnen wir sowohl den besagten gefärbten Graphen als auch den unterliegenden Graphen mit G. Die Familie c wird *Färbung* (oder *Eckenfärbung*) von G genannt. Für jede Ecke x in G wird c_x die *Farbe* von x in G genannt.
Für einen gefärbten Graphen G mit Färbung c schreiben wir $\mathrm{clr} = \mathrm{clr}^G := c$.

(20.60) Beispiel.

(a) Wir haben einen schlichten gefärbten Graphen G gegeben durch

$$\mathrm{V}(G) = \{1, 2, 3, 4, 5, 6, 7, 8, 9\},$$
$$\mathrm{E}(G) = \{12, 23, 26, 34, 67, 78, 89\}$$

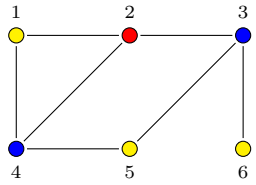
sowie $\mathrm{clr}_1 = \text{rot}$, $\mathrm{clr}_2 = \text{blau}$, $\mathrm{clr}_3 = \text{rot}$, $\mathrm{clr}_4 = \text{blau}$, $\mathrm{clr}_5 = \text{rot}$, $\mathrm{clr}_6 = \text{rot}$, $\mathrm{clr}_7 = \text{blau}$, $\mathrm{clr}_8 = \text{rot}$, $\mathrm{clr}_9 = \text{blau}$.



(b) Wir haben einen schlichten gefärbten Graphen G gegeben durch

$$\mathrm{V}(G) = \{1, 2, 3, 4, 5, 6\},$$
$$\mathrm{E}(G) = \{12, 14, 23, 24, 35, 36, 45\}$$

sowie $\mathrm{clr}_1 = \text{gelb}$, $\mathrm{clr}_2 = \text{rot}$, $\mathrm{clr}_3 = \text{blau}$, $\mathrm{clr}_4 = \text{blau}$, $\mathrm{clr}_5 = \text{gelb}$, $\mathrm{clr}_6 = \text{gelb}$.



(20.61) Definition (gefärbter Graph)**.**

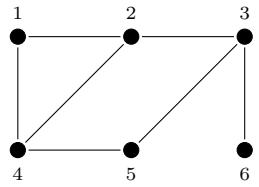
(a) Es sei eine Menge C gegeben. Ein *C-gefärbter Graph* (oder *C-eckengefärbter Graph*) ist ein gefärbter Graph G mit $\mathrm{clr}_x \in C$ für jede Ecke x in G.

(b) Es sei $k \in \mathbb{N}_0$ gegeben. Ein $[1, k]$-gefärbter Graph wird auch *k-gefärbter Graph* (oder *k-eckengefärbter Graph*) genannt.

(20.62) Definition (Färbbarkeit)**.** Es sei $k \in \mathbb{N}_0$ gegeben. Ein Graph G wird *k-färbbar* (oder *k-eckenfärbbar*) genannt, falls es einen k-gefärbten Graphen mit unterliegendem Graphen G gibt.

(20.63) Bemerkung. Es seien ein Graph G und $k \in \mathbb{N}_0$ gegeben. Genau dann ist G ein k-färbbarer Graph, wenn es eine k-elementige Menge C und einen C-gefärbten Graphen mit unterliegendem Graphen G gibt.

(20.64) Beispiel. Der folgende Graph ist 3-färbbar.



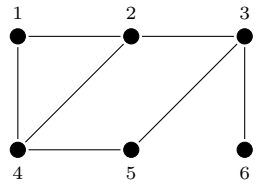
Beweis. Dies folgt aus Beispiel (20.60)(b). □

(20.65) Definition (chromatische Zahl)**.** Es sei ein Graph G gegeben. Wir nennen

$$\min\{k \in \mathbb{N}_0 \mid G \text{ ist } k\text{-färbbar}\}$$

die *chromatische Zahl* (oder *Färbungszahl* oder *Eckenfärbungszahl*) von G.

(20.66) Beispiel. Es sei G der folgende schlichte Graph.



Die chromatische Zahl von G ist 3.

Beweis. Nach Beispiel (20.64) ist G ein 3-färbbarer Graph.
Umgekehrt seien $k \in \mathbb{N}_0$ und ein beliebiger k-gefärbter Graph mit unterliegendem Graphen G gegeben. Wir notieren diesen gefärbten Graphen wieder als G. Da 1 und 2 adjazent in G sind, gilt $\mathrm{clr}_1 \neq \mathrm{clr}_2$. Da 1 und 4 adjazent in G sind, gilt $\mathrm{clr}_1 \neq \mathrm{clr}_4$. Da 2 und 4 adjazent in G sind, gilt $\mathrm{clr}_2 \neq \mathrm{clr}_4$. Folglich ist

$$k \geq |\{\mathrm{clr}_x \mid x \in \mathrm{V}(G)\}| \geq |\{\mathrm{clr}_1, \mathrm{clr}_2, \mathrm{clr}_4\}| = 3.$$

Insgesamt ist die chromatische Zahl von G gleich

$$\min\{k \in \mathbb{N}_0 \mid G \text{ ist } k\text{-färbbar}\} = 3.$$ □

Graphpartitionen

(20.67) Definition (k-partiter Graph)**.** Es sei $k \in \mathbb{N}_0$ gegeben. Ein *k-partiter Graph* besteht aus einem Graphen G zusammen mit einer k-Partition $\mathcal{P}$ von $\mathrm{V}(G)$ derart, dass für alle adjazenten Ecken x und y in G der Teil von x in $\mathcal{P}$ ungleich dem Teil von y in $\mathcal{P}$ ist. Unter Missbrauch der Notation bezeichnen wir sowohl den besagten k-partiten Graphen als auch den unterliegenden Graphen mit G. Die k-Partition $\mathcal{P}$ wird *k-Partition* (oder *Partition*) von G genannt. Für $x \in X$ wird der Teil von x in $\mathcal{P}$ auch der *Teil* von x in G genannt.
Für einen k-partiten Graphen G mit k-Partition $\mathcal{P}$ schreiben wir $\mathrm{Pt}(G) := \mathcal{P}$.

(20.68) Definition (bipartiter Graph, tripartiter Graph)**.**

(a) Ein 2-partiter Graph wird auch *bipartiter Graph* genannt.

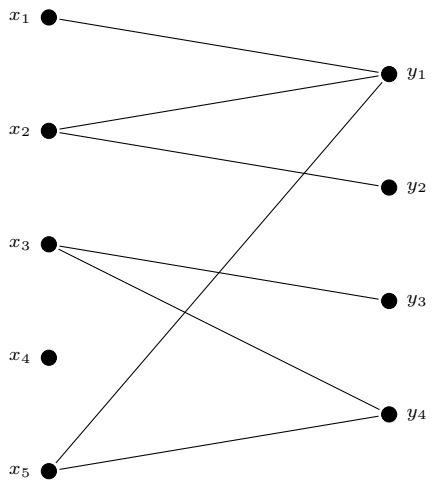
(b) Ein 3-partiter Graph wird auch *tripartiter Graph* genannt.

(20.69) Beispiel.

(a) Wir haben einen schlichten bipartiten Graphen G der Ordnung 9 gegeben durch

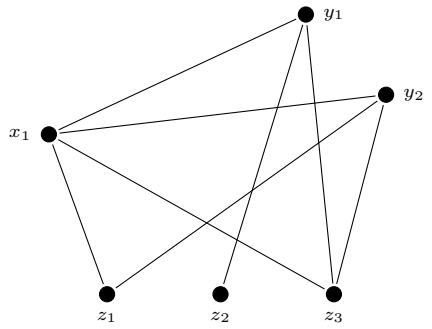
$$\mathrm{V}(G) = \{x_1, x_2, x_3, x_4, x_5, y_1, y_2, y_3, y_4\},$$
$$\mathrm{E}(G) = \{x_1y_1, x_2y_1, x_2y_2, x_3y_3, x_3y_4, x_5y_1, x_5y_4\},$$

$$\mathrm{Pt}(G) = \{\{x_1, x_2, x_3, x_4, x_5\}, \{y_1, y_2, y_3, y_4\}\}.$$



(b) Wir haben einen schlichten tripartiten Graphen G der Ordnung 6 gegeben durch

$$\begin{aligned}\mathrm{V}(G) &= \{x_1, y_1, y_2, z_1, z_2, z_3\},\\ \mathrm{E}(G) &= \{x_1y_1, x_1y_2, x_1z_1, x_1z_3, y_1z_2, y_1z_3, y_2z_1, y_2z_3\},\\ \mathrm{Pt}(G) &= \{\{x_1\}, \{y_1, y_2\}, \{z_1, z_2, z_3\}\}.\end{aligned}$$



(20.70) Bemerkung. Es sei $k \in \mathbb{N}_0$ gegeben.

(a) Es sei ein k-partiter Graph G gegeben. Dann wird der unterliegende Graph von G zu einem $\mathrm{Pt}(G)$-gefärbten Graphen mit Färbung gegeben wie folgt: Für jede Ecke x in G ist clr_x der Teil von x in G.

(b) Es sei ein gefärbter Graph G derart gegeben, dass $\{\mathrm{clr}_x \mid x \in \mathrm{V}(G)\}$ eine k-elementige Menge ist. Dann wird der unterliegende Graph von G zu einem k-partiten Graphen mit Partition von G gegeben durch

$$\mathrm{Pt}(G) = \{\{y \in \mathrm{V}(G) \mid \mathrm{clr}_x = \mathrm{clr}_y\} \mid x \in \mathrm{V}(G)\}.$$

Beweis. Dies sei dem Leser zur Übung überlassen. □

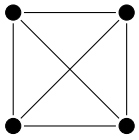
(20.71) Korollar. Es seien $k \in \mathbb{N}_0$ und ein Graph G gegeben. Genau dann ist G ein k-färbbarer Graph, wenn es einen k-partiten Graphen mit unterliegendem Graphen G gibt.

Planare Graphen

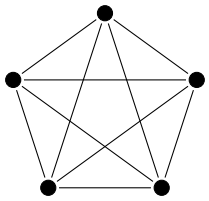
(20.72) Vorstellung (planarer Graph)**.** Ein *planarer Graph* ist ein Graph, welcher so in der Ebene gezeichnet werden kann, dass sich seine Kanten nur an den Endpunkten berühren und ansonsten nicht schneiden.

(20.73) Beispiel.

(a) Der folgende Graph ist planar.



(b) Der folgende Graph ist nicht planar.



Ohne Beweis. □

Es sei ein endlicher zusammenhängender planarer Graph G gegeben. Dann ist die Anzahl derjenigen Flächen in einer Zeichnung von G, bei welcher sich seine Kanten nur an den Endpunkten berühren und ansonsten nicht schneiden, welche durch Kanten von G begrenzt werden, unabhängig von der Zeichnung von G. Bezeichnet n die Ordnung, m die Größe und p die Anzahl dieser Flächen von G, wobei wir die äußere, unendlich große Fläche stets mitzählen, so gilt der *Eulersche Polyedersatz*:

$$n - m + p = 2$$

(20.74) Satz (Vierfarbensatz; Appel/Haken, 1976)**.** Die chromatische Zahl jedes planaren Graphen ist kleiner oder gleich 4.

Ohne Beweis. □

21 Diskrete Optimierung

Zum Abschluss betrachten wir exemplarisch einen einfachen Algorithmus, mit dem sich ein Optimierungsproblem einer durch einen Graphen modellierten Situation lösen lässt. ([55])

Gewichtete Graphen

Zur Beschreibung des Optimierungsproblems müssen wir Graphen mit einer sogenannten Gewichtsfunktion versehen:

(21.1) Definition (gewichteter Graph)**.** Ein *gewichteter Graph* (genauer *kantengewichteter Graph*) besteht aus einem Graphen G zusammen mit einer Abbildung $w\colon \mathrm{E}(G) \to \mathbb{R}$. Unter Missbrauch der Notation bezeichnen wir sowohl den besagten gewichteten Graphen als auch den unterliegenden Graphen mit G. Die Abbildung w wird *Gewichtsfunktion* von G genannt.
Für einen gewichteten Graphen G mit Gewichtsfunktion $w\colon \mathrm{E}(G) \to \mathbb{R}$ schreiben wir $\mathrm{w} = \mathrm{w}^G := w$.

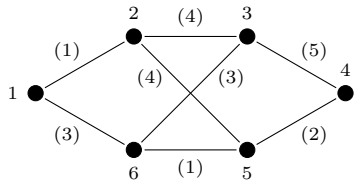
In Skizzen schreiben wir Gewichte der Kanten in einem gewichteten Graphen üblicherweise in runden Klammern an die Kanten:

(21.2) Beispiel. Wir haben einen schlichten gewichteten Graphen G gegeben durch

$$\mathrm{V}(G) = \{1, 2, 3, 4, 5, 6\},$$
$$\mathrm{E}(G) = \{12, 16, 23, 25, 34, 36, 45, 56\}$$

[55] Weitere solche Algorithmen werden in Vorlesungen zur *diskreten Optimierung* studiert; an der RWTH Aachen bspw. im Rahmen des Kurses *Datenstrukturen und Algorithmen* (etwa 2. Semester im Studiengang B.Sc. Informatik).

sowie $\mathrm{w}(12) = 1$, $\mathrm{w}(16) = 3$, $\mathrm{w}(23) = 4$, $\mathrm{w}(25) = 4$, $\mathrm{w}(34) = 5$, $\mathrm{w}(36) = 3$, $\mathrm{w}(45) = 2$, $\mathrm{w}(56) = 1$.



Graphen lassen sich auf kanonische Weise als gewichtete Graphen auffassen:

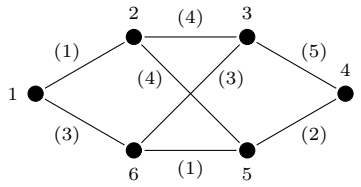
(21.3) Bemerkung. Jeder Graph G wird zu einem gewichteten Graph mit $\mathrm{w}(a) = 1$ für $a \in \mathrm{E}(G)$.

(21.4) Konvention. Es sei ein Graph G gegeben. Wenn wir in Zukunft vom gewichteten Graphen G sprechen, so meinen wir damit stets G mit der Gewichtsfunktion gegeben durch $\mathrm{w}(a) = 1$ für $a \in \mathrm{E}(G)$.

(21.5) Definition (Gewicht eines endlichen Untergraphen)**.** Es seien ein gewichteter Graph G und ein endlicher Untergraph U von G gegeben. Das *Gewicht* von U ist definiert als

$$\mathrm{w}(U) := \sum_{a \in \mathrm{E}(U)} \mathrm{w}(a).$$

(21.6) Beispiel. Es sei G der folgende schlichte gewichtete Graph.



Dann ist

$$\mathrm{w}(G|_{\{1,2,3,5\}}) = 9.$$

Beweis. Es ist

$$\mathrm{w}(G|_{\{1,2,3,5\}}) = \sum_{a \in \mathrm{E}(G|_{\{1,2,3,5\}})} \mathrm{w}(a) = \mathrm{w}(12) + \mathrm{w}(23) + \mathrm{w}(25) = 1 + 4 + 4 = 9. \qquad \square$$

Minimale Spannbäume

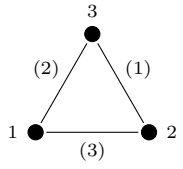
Das Optimierungsproblem, welches wir lösen wollen, lautet nun wie folgt: Man finde in einem gegebenen endlichen gewichteten Graphen einen Spannbaum von minimalem Gewicht, einen sogenannten minimalen Spannbaum:

(21.7) Definition (minimaler Spannbaum)**.** Es sei ein endlicher gewichteter Graph G gegeben. Ein Spannbaum T von G heißt *minimal*, wenn

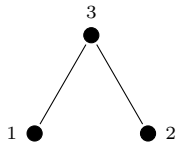
$$\mathrm{w}(T) = \min\{\mathrm{w}(T') \mid T' \text{ ist ein Spannbaum von } G\}$$

ist.

(21.8) Beispiel. Es sei G der folgende schlichte gewichtete Graph.

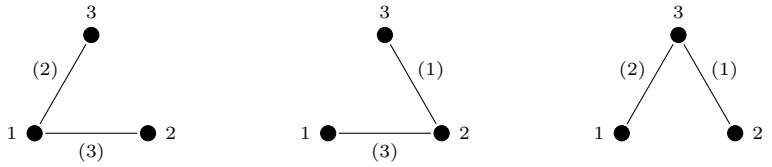


Dann ist



ein minimaler Spannbaum von G.

Beweis. Es sei T_1 der im Folgenden links dargestellte Untergraph von G, es sei T_2 der im Folgenden mittig dargestellte Untergraph von G, und es sei T_3 der im Folgenden rechts dargestellte Untergraph von G.



Dann ist

$$\{T' \mid T' \text{ ist ein Spannbaum von } G\} = \{T_1, T_2, T_3\}.$$

Wegen

$$\begin{aligned} \mathrm{w}(T_1) &= \mathrm{w}(12) + \mathrm{w}(13) = 3 + 2 = 5, \\ \mathrm{w}(T_2) &= \mathrm{w}(12) + \mathrm{w}(23) = 3 + 1 = 4, \\ \mathrm{w}(T_3) &= \mathrm{w}(13) + \mathrm{w}(23) = 2 + 1 = 3 \end{aligned}$$

ist folglich

$$\mathrm{w}(T_3) = 3 = \min\{5, 4, 3\} = \min\{\mathrm{w}(T_1), \mathrm{w}(T_2), \mathrm{w}(T_3)\} = \min\{\mathrm{w}(T') \mid T' \text{ ist ein Spannbaum von } G\}$$

und damit T_3 ein minimaler Spannbaum von G. □

Das Optimierungsproblem zur Bestimmung eines minimalen Spannbaums wird durch folgenden Algorithmus gelöst:

(21.9) Satz (Algorithmus von Kruskal)**.** Es sei ein endlicher gewichteter Graph G der Größe m gegeben. Ferner sei $(a_1, \ldots, a_m)$ eine m-Permutation in $\mathrm{E}(G)$ mit

$$\mathrm{w}(a_1) \leq \mathrm{w}(a_2) \leq \mathrm{w}(a_3) \leq \ldots \leq \mathrm{w}(a_m).$$

Das Tupel $(T_0, \ldots, T_m)$ sei wie folgt rekursiv definiert: Für $i \in [0, m]$ sei

$$T_i := \begin{cases} \emptyset, & \text{falls } i = 0, \\ T_{i-1} \cup \{a_i\}, & \text{falls } i \in [1, m] \text{ und } T_{i-1} \cup \{a_i\} \text{ keinen Kreis enthält}, \\ T_{i-1}, & \text{falls } i \in [1, m] \text{ und } T_{i-1} \cup \{a_i\} \text{ einen Kreis enthält}. \end{cases}$$

Dann ist T_m ein minimaler Spannbaum von G.

Beweisskizze. Es ist vergleichsweise leicht zu zeigen, dass T_m ein Spannbaum von G ist.
Angenommen, T_m ist nicht minimal. Es sei U ein minimaler Spannbaum von G so, dass

$$|\mathrm{E}(T_m) \cap \mathrm{E}(U)| = \max\{|\mathrm{E}(T_m) \cap \mathrm{E}(U')| \mid U' \text{ ist ein minimaler Spannbaum von } G\}$$

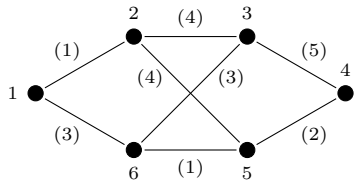
Da T_m nicht minimal ist, gilt $\mathrm{E}(T_m) \setminus \mathrm{E}(U) \neq \emptyset$. Wir setzen $i := \min\{j \in [1, m] \mid a_j \in \mathrm{E}(T_m) \setminus \mathrm{E}(U)\}$.
Da U ein Spannbaum von G ist, enthält $U \cup \{a_i\}$ genau einen Kreis. Als Baum enthält T_m keine Kreise, so dass es auf besagtem Kreis notwendigerweise eine Kante b geben muss, welche nicht zu T_m gehört. Es lässt sich zeigen, dass $U' := (U \cup \{a_i\}) \setminus \{b\}$ ein minimaler Spannbaum von G mit $|\mathrm{E}(T_m) \setminus \mathrm{E}(U')| = |\mathrm{E}(T_m) \setminus \mathrm{E}(U)| + 1$ ist, im Widerspruch zur Wahl von U. □

(21.10) Algorithmus (Algorithmus von Kruskal)**.**

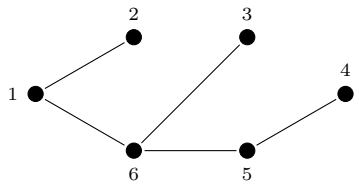
- Eingabe: endlicher, zusammenhängender gewichteter Graph G der Größe m
- Ausgabe: minimaler Spannbaum T von G
- Verfahren:

```
function kruskal(G)
    bestimme m-Permutation (a_1, ..., a_m) in E(G) mit w(a_1) ≤ w(a_2) ≤ ... ≤ w(a_m);
    T := ∅;
    for i from 1 to m do
        if T ∪ {a_i} enthält keinen Kreis then
            T := T ∪ {a_i};
        end if;
    end for;
    return T;
end function;
```

(21.11) Beispiel. Es sei G der folgende schlichte gewichtete Graph.



Dann ist

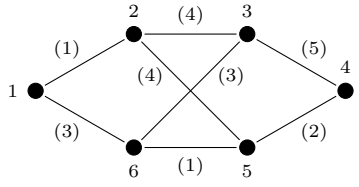


ein minimaler Spannbaum von G.

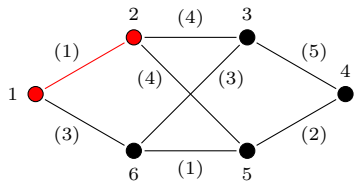
Beweis. Wir verwenden den Algorithmus von Kruskal (21.9). Zunächst ordnen wir die Kanten von G nach aufsteigendem Gewicht:

w(a)	1	2	3	4	5
a	12, 56	45	16, 36	23, 25	34

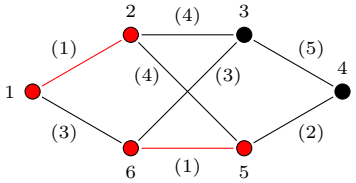
Es sei $T_0 := \emptyset$.



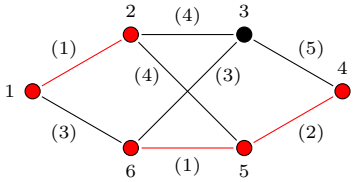
Da $T_0 \cup \{12\}$ keinen Kreis enthält, setzen wir $T_1 := T_0 \cup \{12\}$.



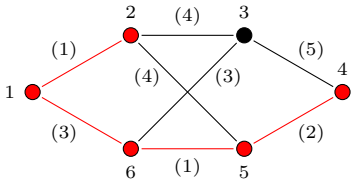
Da $T_1 \cup \{56\}$ keinen Kreis enthält, setzen wir $T_2 := T_1 \cup \{56\}$.



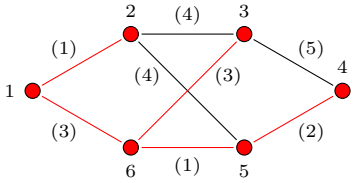
Da $T_2 \cup \{45\}$ keinen Kreis enthält, setzen wir $T_3 := T_2 \cup \{45\}$.



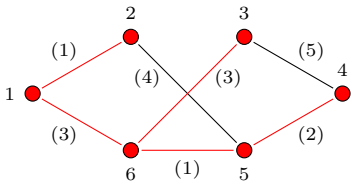
Da $T_3 \cup \{16\}$ keinen Kreis enthält, setzen wir $T_4 := T_3 \cup \{16\}$.



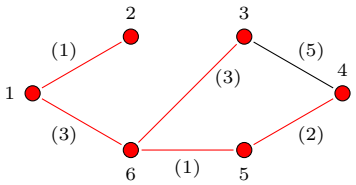
Da $T_4 \cup \{36\}$ keinen Kreis enthält, setzen wir $T_5 := T_4 \cup \{36\}$.



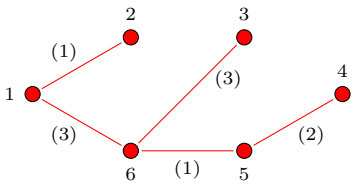
Da $T_5 \cup \{23\}$ den Kreis 23612 enthält, setzen wir $T_6 := T_5$.



Da $T_6 \cup \{25\}$ den Kreis 25612 enthält, setzen wir $T_7 := T_6$.



Da $T_7 \cup \{34\}$ den Kreis 34563 enthält, setzen wir $T_8 := T_7$.



□

Literatur

[1] Aigner, Martin. *Diskrete Mathematik.* Vieweg Studium: Aufbaukurs Mathematik, Vol. 68. Springer Fachmedien, Wiesbaden, 1996. DOI: 10.1007/978-3-663-09809-6.

[2] Cormen, Thomas H.; Leiserson, Charles E.; Rivest, Ronald L.; Stein, Clifford. *Introduction to algorithms.* Third Edition. MIT Press, Cambridge (MA), 2009.

[3] Dietrich, Volker. *Grundlagen der Mathematik: Axiomatische Mengenlehre.* Vorlesungsmanuskript, RWTH Aachen, 2005.

[4] Dietrich, Volker. *Grundlagen der Mathematik: Mathematische Logik.* Vorlesungsmanuskript, RWTH Aachen, 2000.

[5] Grädel, Erich. *Mathematische Logik.* Vorlesungsmanuskript, RWTH Aachen, 2011.

[6] Hanke, Timo; Hiss, Gerhard. *Diskrete Strukturen und Lineare Algebra für Informatiker.* Vorlesungsmanuskript, RWTH Aachen, 2013.

[7] Hiss, Gerhard. *Algebra I.* Vorlesungsnotizen, RWTH Aachen, 2007.

[8] Jongen, Hubertus Theodorus; Meer, Klaus; Triesch, Eberhard. *Optimization theory.* Kluwer Academic Publishers, Boston (MA), 2004.

[9] Kamps, Udo; Cramer, Erhard. *Stochastik I.* Vorlesungsmanuskript, RWTH Aachen, 2016.

[10] Knuth, Donald Ervin. *Two notes on notation.* The American Mathematical Monthly **99**(5) (1992), S. 403–422. DOI: 10.2307/2325085.

[11] Kreussler, Bernd; Pfister, Gerhard. *Mathematik für Informatiker. Algebra, Analysis, Diskrete Strukturen.* eXamen.press. Springer-Verlag, Berlin/Heidelberg, 2009. DOI: 10.1007/978-3-540-89107-9.

[12] Quebbemann, Heinz-Georg. *Diskrete Strukturen.* Vorlesungsmanuskript, Carl von Ossietzky Universität Oldenburg, 2011.

[13] Schaefer, Martin. *Einführung in die Stochastik.* Vorlesungsnotizen, RWTH Aachen, 2003.

[14] Thomas, Sebastian. *Diskrete Strukturen.* Vorlesungsmanuskript, Carl von Ossietzky Universität Oldenburg, 2014.

[15] Thomas, Sebastian. *Diskrete Strukturen.* Vorlesungsmanuskript, RWTH Aachen, 2017 (Version 1.2.11, 31. Januar 2018).

[16] Thomas, Sebastian. *Lineare Algebra.* Vorlesungsmanuskript, Carl von Ossietzky Universität Oldenburg, 2013.

[17] Thomas, Sebastian. *Lineare Algebra für Informatiker.* Vorlesungsmanuskript, Carl von Ossietzky Universität Oldenburg, 2014.

[18] Thomas, Sebastian. *Lineare Algebra für Informatiker.* Vorlesungsmanuskript, RWTH Aachen, 2017 (Version 2.4.1, 1. August 2017).

[19] Thomas, Sebastian. *Vorkurs zur linearen Algebra.* Vorlesungsmanuskript, RWTH Aachen, 2012. `http://www.math.rwth-aachen.de/~Sebastian.Thomas/teaching/vorkurs_lineare_algebra_12/Thomas_Vorkurs_zur_linearen_Algebra_SS2012.pdf`

[20] Tittmann, Peter. *Einführung in die Kombinatorik.* 2. Auflage. Springer-Verlag, Berlin/Heidelberg, 2014. DOI: 10.1007/978-3-642-54589-4.

[21] Uzunkol, Osmanbey. *Diskrete Strukturen.* Vorlesungsmanuskript, Carl von Ossietzky Universität Oldenburg, 2012.

[22] Volkmann, Lutz. *Graphen an allen Ecken und Kanten.* Zweite Version. RWTH Aachen, 2011. `http://www.math2.rwth-aachen.de/files/gt/buch/graphen_an_allen_ecken_und_kanten.pdf`

[23] Zerz, Eva. *Mathematische Grundlagen.* Vorlesungsmanuskript, RWTH Aachen, 2007.

Sebastian Thomas
Lehrstuhl D für Mathematik
RWTH Aachen University
Pontdriesch 14/16
52062 Aachen
Germany
sebastian.thomas@math.rwth-aachen.de
http://www.math.rwth-aachen.de/~Sebastian.Thomas/