Mathematik für Informatiker: Diskrete Strukturen

Dr. Jens Zumbrägel

TU Dresden · WiSe 2016/17

Vorlesungsskript
Version vom 03.02.2017

Dieses Skript begleitet den Vorlesungsteil „Diskrete Strukturen“ des Moduls Mathematik für Informatiker an der TU Dresden im Wintersemester 2016/17. Das Modul, zu dem auch der Vorlesungsteil über lineare Algebra gehört, richtet sich an Studierende im ersten Semester in den Bachelor-Studiengängen Informatik und Medieninformatik, sowie im Diplom-Studiengang Informatik. Es führt in die mathematische Methodik ein und behandelt zentrale mathematische Begriffe, Schreibweisen, sowie Argumentationsformen.

Das Hauptaugenmerk dieser Vorlesung liegt auf den diskreten Strukturen, worunter endliche bzw. endlich beschreibbare Objekte verstanden werden, wie beispielsweise Restklassenringe oder Graphen. Die ersten drei Kapitel führen zunächst in die (ganz allgemein) benötigten Grundlagen aus Logik und Mengenlehre ein. Nachfolgend werden in Kapitel vier und fünf Zahlen und deren Arithmetik behandelt, wobei auch einige Anwendungen zur Sprache kommen. In den anschließenden zwei Kapiteln geht es hingegen um Graphen, Netzwerke und geordnete Mengen, bevor ein kurzer Ausflug in die unendlichen Mengen den Themenkreis abschließt.

Die Vorlesung orientet sich einerseits am Lehrbuch „Diskrete Strukturen – kurz gefasst“ von Ulrich Knauer, welches nun in der zweiten Auflage erschienen ist [1], sowie am Skript von Prof. Dr. Manuel Bodirsky [2], der diese Vorlesung in den letzten beiden Jahren an der TU Dresden gehalten hat. Eine gut lesbare Einführung in die Mengenlehre stellt zudem der Klassiker von Paul Halmos [3] dar. Das Kapitel über geordnete Mengen folgt derweil den ersten Abschnitten eines neuen Lehrbuchs von Bernhard Ganter [4], welches interessierten Lesenden sehr empfohlen sei.

Literatur

[1] U. Knauer, K. Knauer, *Diskrete und algebraische Strukturen – kurz gefasst*, 2. Auflage, Springer Spektrum, 2015.

[2] M. Bodirsky, *Diskrete Strukturen*, Vorlesungsskript, TU Dresden, 2016.

[3] P. R. Halmos, *Naive Mengenlehre*, 5. Auflage, Vandenhoeck & Ruprecht, 1994.

[4] B. Ganter, *Diskrete Mathematik: Geordnete Mengen*, Springer-Lehrbuch, 2013.

Inhaltsverzeichnis

1 Logische Grundlagen

Logic is the beginning of wisdom, Valeris, not the end.
— Spock, in: *The Undiscovered Country*

Wenn neue Begriffe eingeführt werden (insb. bei Definitionen), so werden sie im Text *hervorgehoben*. Alternative Bezeichner oder Sprechweisen stehen in „Anführungszeichen“.

1.1 Aussagenlogik

Definition 1.1. Eine *Aussage* ist eine endliche Zeichenfolge, der genau einer der Wahrheitswerte „wahr“ (1) oder „falsch“ (0) zugeordent ist.

Eine Zeichenfolge kann einer natürlichen Sprache oder der mathematischen Sprache entstammen. Beispiele für Aussagen sind „Dresden liegt an der Elbe.“, „Die Erde ist eine Scheibe.“, „$2 \cdot 3 = 6$“, „4 ist eine Primzahl“, „$a \in \{a, b, c\}$“. Dagegen sind beispielsweise „Wie geht es dir?“, „Morgen wird es regnen.“, „Sie ist eine gute Studentin.“, „$x = 3$“ keine Aussagen.

Aussagen können mittels der Symbole $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$ zu neuen Aussagen *verknüpft* werden, wobei der Wahrheitswert der verknüpften Aussage ausschließlich vom Wahrheitswert der Komponenten abhängt (siehe Tabelle 1). Für Aussagevariablen verwenden wir in der Regel die Bezeichner $A, B, \ldots$.

$\neg A$	„nicht A“	ist wahr wenn A falsch, und falsch wenn A wahr ist
$A \vee B$	„A oder B“	ist wahr wenn A wahr ist oder B wahr ist (oder beide), ansonsten falsch
$A \wedge B$	„A und B“	ist wahr wenn A und B wahr sind, ansonsten falsch
$A \Rightarrow B$	„A impliziert B“, „wenn A dann B“	ist wahr wenn A falsch ist oder B wahr ist, ansonsten falsch
$A \Leftrightarrow B$	„A äquivalent zu B“, „A genau dann, wenn B“, „A gdw. B“	ist wahr wenn A und B beide wahr oder beide falsch sind, ansonsten falsch

Tabelle 1: Aussagenlogische Verknüpfungen

Aussagevariablen, 0, 1, sowie Verknüpfungen hiervon heißen aussagenlogische Formeln oder *Aussageformen*; wir verwenden hierfür typischerweise die Bezeichner $\mathcal{A}, \mathcal{B}, \ldots$. Eine *Belegung* einer Aussageform ist eine Zuordnung von Wahrheitswerten für die Variablen. Alle möglichen Belegungen einer Aussageform können übersichtlich durch eine Wahrheitstabelle dargestellt werden (siehe Tabelle 2).

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

Tabelle 2: Wahrheitstabellen

Definition 1.2. Zwei Aussageformen $\mathcal{A}$ und $\mathcal{B}$ heißen *gleichwertig* (schreibe $\mathcal{A} = \mathcal{B}$), falls für jede Belegung die Wahrheitswerte von $\mathcal{A}$ und $\mathcal{B}$ gleich sind.

Ist eine Aussageform $\mathcal{T}$ für alle Belegungen wahr, so heißt sie *Tautologie*; wir schreiben $\mathcal{T} = 1$. Ist hingegen eine Aussageform $\mathcal{W}$ für alle Belegungen falsch, nennen wir sie *Widerspruch*, $\mathcal{W} = 0$.

Beispielsweise ist $A \vee \neg A$ eine Tautologie und $A \wedge \neg A$ ein Widerspruch.[1] Wir bemerken weiterhin, dass zwei Aussageformen $\mathcal{A}$ und $\mathcal{B}$ genau dann gleichwertig sind, wenn $\mathcal{A} \Leftrightarrow \mathcal{B}$ eine Tautologie ist.

Satz 1.1 (Grundlegende Gesetze)**.** *Für Aussagevariablen A, B, C gelten:*

a)	$(A \vee B) \vee C = A \vee (B \vee C)$ $(A \wedge B) \wedge C = A \wedge (B \wedge C)$	*(Assoziativgesetze)*
b)	$A \vee 0 = A$ *und* $A \wedge 1 = A$	*(neutrale Elemente)*
c)	$A \vee \neg A = 1$ *und* $A \wedge \neg A = 0$	*(Komplemente)*
d)	$A \vee B = B \vee A$ $A \wedge B = B \wedge A$	*(Kommutativgesetze)*
e)	$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$ $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$	*(Distributivgesetze)*

Wir können diese logischen Identitäten für die Umformung von Aussageformen benutzen, also für die Herleitung weiterer Identitäten.

Satz 1.2 (Weitere Eigenschaften)**.** *Für Aussagevariablen A, B gelten:*

a)	$A \Leftrightarrow B \;=\; (A \Rightarrow B) \wedge (B \Rightarrow A)$	
b)	$\neg\neg A \;=\; A$	
c)	$A \Rightarrow B \;=\; \neg A \vee B \;=\; \neg B \Rightarrow \neg A$	*(Kontraposition)*
d)	$\neg(A \vee B) = \neg A \wedge \neg B$ $\neg(A \wedge B) = \neg A \vee \neg B$	*(de Morgansche Regeln)*

Die in Satz 1.1 und Satz 1.2 genannten Identitäten können leicht mittels Wahrheitstafeln bewiesen werden. Exemplarisch sei hier die Identität Satz 1.2, a) behandelt:

A	B	$A \Leftrightarrow B$	$A \Rightarrow B$	$B \Rightarrow A$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$
0	0	1	1	1	1
0	1	0	1	0	0
1	0	0	0	1	0
1	1	1	1	1	1

Da die erste Spalte rechts vom Strich offenbar der letzten Spalte gleicht, sind die Aussageformen $A \Leftrightarrow B$ und $(A \Rightarrow B) \wedge (B \Rightarrow A)$ gleichwertig.

Einige Eigenschaften können auch unter der Benutzung von bereits bewiesenen Gesetzen gezeigt werden, etwa Satz 1.2, c): Nach Definition gilt $A \Rightarrow B \;=\; \neg A \vee B$, sei diese Identität mit $(*)$ bezeichnet. Dann haben wir

$$\neg B \Rightarrow \neg A \overset{(*)}{=} \neg\neg B \vee \neg A \overset{1.2,\,\mathrm{b})}{=} B \vee \neg A \overset{1.1,\,\mathrm{d})}{=} \neg A \vee B \overset{(*)}{=} A \Rightarrow B\,.$$

[1] Wir benutzen die Konvention, dass $\neg$ stärker bindet als $\vee, \wedge, \Rightarrow, \Leftrightarrow$, also $A \vee \neg A := A \vee (\neg A)$; hierbei bedeutet die Notation $L := R$, dass die linke Seite L durch die rechte Seite R definiert wird.

1.2 Umgang mit Quantoren

Neben Aussagevariablen $A, B, \ldots$ betrachten wir nun (Individuen-)Variablen $x, y, \ldots$ aus einem festzulegenden *Universum*, z. B. alle Menschen, $\mathbb{N}$, $\mathbb{R}$.

Definition 1.3. Ein *Prädikat* ist eine Zeichenfolge die Variablen beinhalten kann, der für jede Variablenbelegung aus dem Universum ein Wahrheitswert zugeordnet ist.
Ein Prädikat, das für alle Variablenbelegungen wahr ist, heißt *Tautologie*.

Wir bemerken, dass ein Prädikat ohne Variablen demnach eine Aussage ist.

Prädikat	Universum
$A(x) =$ „x ist eine Katze“	alle Tiere
$B(x, y) =$ „x und y sind ein Paar Schuhe“	alle Schuhe
$C(x) =$ „x ist eine Primzahl“	$\mathbb{N}$
$D(x, y, z) =$ „$x^2 + y^2 = z^2$“	$\mathbb{N}$
$E(x) =$ „x ist Primzahl $\Rightarrow$ x ist ungerade“	$\mathbb{N}$
$F(x, y) =$ „(x gerade) $\wedge$ (y gerade) $\Rightarrow$ $x + y$ gerade“	$\mathbb{Z}$

Tabelle 3: Beispiele für Prädikate

Betrachten wir beispielsweise $E(x)$ und $F(x, y)$ aus Tabelle 3. Es ist $F(x, y)$ eine Tautologie, denn $F(x, y)$ ist wahr für alle $x, y \in \mathbb{Z}$. Hingegen ist $E(x)$ keine Tautologie, denn $E(x)$ ist wahr für alle $x \in \mathbb{N} \setminus \{2\}$, jedoch falsch für $x = 2$.

Wir führen nun den *Allquantor* $\forall$ und den *Existenzquantor* $\exists$ ein.

Definition 1.4. Sei $P(x)$ ein Prädikat. Dann sind $\forall x : P(x)$ und $\exists x : P(x)$ Aussagen mit Wahrheitswerten wie folgt:

$\forall x : P(x)$	„für alle x gilt $P(x)$“	ist wahr wenn $P(x)$ für alle x aus dem Universum wahr ist, ansonsten falsch
$\exists x : P(x)$	„es existiert x mit $P(x)$“	ist wahr wenn $P(x)$ für mindestens ein x aus dem Universum wahr ist, ansonsten falsch

Weiterhin sei die Aussage $\exists! x : P(x)$, sprich „es gibt genau ein x mit $P(x)$“, wahr, wenn es x gibt mit $P(x)$ wahr, und für alle y mit $y \neq x$ ist $P(y)$ falsch.

Beispielsweise ist für $A(x)$ aus Tabelle 3 die Aussage $\forall x : A(x)$ falsch, hingegen die Aussage $\exists x : A(x)$ wahr, jedoch $\exists! x : A(x)$ falsch.
Ferner legen wir als abkürzende Schreibweisen fest:

$$\begin{aligned} \forall x \in X : P(x) &:= \forall x : x \in X \Rightarrow P(x) \\ \exists x \in X : P(x) &:= \exists x : x \in X \wedge P(x) \end{aligned}$$

Wir können Quantoren auch mit mehreren Variablen benutzen. Ist etwa $P(x, y)$ ein Prädikat, dann ist

$$Q(y) := \forall x : P(x, y)$$

ein Prädikat, welches für ein (beliebiges, aber festes) y genau dann wahr ist, wenn $P(x, y)$ für alle x wahr ist. Man nennt dann die Variable x *gebunden* und die Variable y *frei*.

Entsprechend ist $\exists x : P(x, y)$ ein Prädikat, das für ein y genau dann wahr ist, wenn es x gibt mit $P(x, y)$. Bei mehreren Variablen sind auch mehrere Quantoren möglich, wie beispielsweise in der Aussage $\exists y : Q(y) = \exists y \forall x : P(x, y)$.

Für die Negation von Aussagen mit Quantoren gelten die folgenden Identitäten:

$$\begin{aligned}\neg(\forall x : P(x)) &= \exists x : \neg P(x)\\ \neg(\exists x : P(x)) &= \forall x : \neg P(x)\end{aligned}$$

Die Negation der Aussage $A = \exists y : Q(y) = \exists y \forall x : P(x, y)$ beispielsweise ist:

$$\neg A = \neg(\exists y : Q(y)) = \forall y : \neg Q(y) = \forall y : \neg(\forall x : P(x, y)) = \forall y \exists x : \neg P(x, y)$$

Beispiel 1.1. Ein Beispiel aus der Analysis: Sei $(a_n)_{n\in\mathbb{N}}$ eine reelle Folge und sei $a \in \mathbb{R}$. Wir sagen, dass die Folge (a_n) gegen a konvergiert, falls

$$\forall \varepsilon \in \mathbb{R}_{>0}\, \exists N \in \mathbb{N}\, \forall n \in \mathbb{N}_{\geq n} : |a_n - a| < \varepsilon\,.$$

Die Negation dieser Aussage, also dass die Folge (a_n) nicht gegen a konvergiert, lautet

$$\exists \varepsilon \in \mathbb{R}_{>0}\, \forall N \in \mathbb{N}\, \exists n \in \mathbb{N}_{\geq n} : |a_n - a| \geq \varepsilon\,.$$

1.3 Beweisverfahren

Ein mathematischer *Satz* ist (logisch betrachtet) eine Tautologie und oft von der Form $P \Rightarrow Q$ bzw. $\forall x : P(x) \Rightarrow Q(x)$, wobei P die *Voraussetzung* ist und Q die *Behauptung* bzw. (nach Beweis) die *Folgerung*. Andere Bezeichner für Satz sind etwa Theorem, Proposition, Lemma und Corollar.

Bei einem *direkten Beweis* der Aussage $P \Rightarrow Q$ geht man davon aus, dass die Voraussetzung P wahr ist und gelangt durch eine Reihe von logischen Schlüssen zu dem Ergebnis, dass die Behauptung Q wahr ist.

Satz X (Beispielsatz)**.** *Seien A, B Mengen mit $A \cup B \subseteq A \cap B$. Dann gilt $A \subseteq B$.*

Logisch formalisiert betrachten wir das Universum der Mengen und es sei $P(A, B) =$ „$A \cup B \subseteq A \cap B$“ und $Q(A, B) =$ „$A \subseteq B$“, dann ist der Satz X die Aussage $\forall A \forall B : P(A, B) \Rightarrow Q(A, B)$.

Beweis (direkt). Für alle Mengen A, B zeigen wir $P(A, B) \Rightarrow Q(A, B)$. Seien also A, B Mengen mit $A \cup B \subseteq A \cap B$. Dann erhalten wir

$$A \subseteq A \cup B \subseteq A \cap B \subseteq B$$

und somit $A \subseteq B$. □

Betrachten wir den obigen Beweis etwas genauer. Wir benutzen einerseits allgemeingültige Aussagen über beliebige Mengen X, Y, Z, nämlich $X \subseteq X \cup Y$ und $X \cap Y \subseteq X$, sowie $X \subseteq Y \wedge Y \subseteq Z \Rightarrow X \subseteq Z$ (die strenggenommen einen eigenen Beweis erfordern), sowie die Voraussetzung $A \cup B \subseteq A \cap B$ (die nicht für alle Mengen A, B gilt). Des Weiteren könnte man aus der Voraussetzung sogar $A = B$ folgern, was die Richtigkeit von Satz X und dessen Beweis aber nicht beeinträchtigt.

Weitere Beweistechniken für eine Aussage $P \Rightarrow Q$ sind

- *Kontraposition*: direkter Beweis der Aussage $\neg Q \Rightarrow \neg P$,
- *durch Widerspruch*: direkter Beweis von $P \wedge \neg Q \Rightarrow 0$.

In der Tat sind diese Beweisarten zulässig, denn es gilt $P \Rightarrow Q = \neg Q \Rightarrow \neg P$ nach Satz 1.2, c), sowie $P \wedge \neg Q \Rightarrow 0 = \neg(P \wedge \neg Q) = \neg P \vee Q = P \Rightarrow Q$.

Beweis (Kontraposition). Wir zeigen $\neg Q(A,B) \Rightarrow \neg P(A,B)$ für alle Mengen A, B. Gelte $\neg Q(A,B)$, das heißt $A \not\subseteq B$. Dann gibt es $x \in A$ mit $x \notin B$. Es folgt $x \in A \cup B$, sowie $x \notin A \cap B$, und somit $A \cup B \not\subseteq A \cap B$. Somit ist $\neg P(A,B)$ gezeigt. □

Beweis (durch Widerspruch). Wir zeigen für alle Mengen A, B, dass $P(A,B) \wedge \neg Q(A,B)$ zu einem Widerspruch führt. Gelte $\neg Q(A,B)$, dann ist $A \not\subseteq B$, somit gibt es $x \in A$ mit $x \notin B$. Es folgt $x \in A \cup B$, und nach Voraussetzung $P(A,B) = \text{„}A \cup B \subseteq A \cap B\text{“}$ folgt $x \in A \cap B$, und somit $x \in B$. Also gilt $x \notin B$ und $x \in B$, dies ist ein Widerspruch. □

Weiterhin ist die *vollständige Induktion* eine spezielle Beweismethode für Aussagen der Form $\forall n \in \mathbb{N} : P(n)$, wobei $\mathbb{N} := \{0, 1, 2, \dots\}$ die natürlichen Zahlen sind. Man zeigt:

- Induktionsanfang (IA): $P(0)$ ist wahr,
- Induktionsschritt (IS): $\forall n \in \mathbb{N} : (P(n) \Rightarrow P(n+1))$;
  hierbei wird $P(n)$ als Induktionsvoraussetzung (IV) bezeichnet.

Man beachte die richtige Klammerung beim Induktionsschritt; oftmals wird fälschlicherweise in etwa der (unsinnige) Ausdruck $(\forall n \in \mathbb{N} : P(n)) \Rightarrow P(n+1)$ gezeigt.

Beispiel 1.2. Sei $P(n)$ das Prädikat

$$\text{„}0 + 1 + \cdots + n = \tfrac{1}{2}n(n+1)\text{“}.$$

Wir beweisen $\forall n \in \mathbb{N} : P(n)$ mit vollständiger Induktion.
(IA): Es ist $P(0) = \text{„}0 = \tfrac{1}{2}0 \cdot 1\text{“}$ wahr.
(IS): Sei $n \in \mathbb{N}$ und gelte (IV) $P(n)$, zeige $P(n+1)$. Es ist

$$\begin{aligned} 0 + 1 + \cdots + n + n{+}1 &= (0 + 1 + \cdots + n) + n{+}1 \\ &\overset{\text{(IV)}}{=} \tfrac{1}{2}n(n+1) + n{+}1 = \tfrac{1}{2}(n+1)(n+2)\,, \end{aligned}$$

also ist $P(n+1)$ wahr.

Wir erwähnen schließlich noch zwei Varianten der vollständigen Induktion.

- Um eine Aussage $\forall n \in \mathbb{N}_{\geq n_0} : P(n)$, wobei $\mathbb{N}_{\geq n_0} := \{n_0, n_0{+}1, n_0{+}2, \dots\}$, zu zeigen verwende man statt $P(0)$ den Induktionsanfang (IA) $P(n_0)$.
- Bei der *starken Induktion* wird der Induktionsschritt (IS) ersetzt durch

  $$\forall n \in \mathbb{N} : (\forall k \in \{0, 1, \dots, n{-}1\} : P(k)) \Rightarrow P(n)\,;$$

  die (stärkere) Induktionsvoraussetzung (IV) lautet hier $\forall k \in \{0, 1, \dots, n{-}1\} : P(k)$.

2 Mengen

Unter einer „Menge“ verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die „Elemente“ von M genannt werden) zu einem Ganzen.

— Georg Cantor (1895)

Die Mengenlehre erscheint oft als elementar und selbstverständlich, sie liefert jedoch eine wichtige Grundlage für exaktes mathematisches Argumentieren. Ein allzu naiver Umgang mit Mengen kann zu Paradoxien führen (siehe unten), welche wiederum einen deutlichen Entwicklungsschub von Logik und Mengenlehre im frühen 20. Jahrhundert auslösten.

Wir werden nicht definieren, was eine Menge (oder ein Element) ist; stattdessen werden wir den Umgang mit Mengen erklären. Es begegnen uns sehr viele Beispiele für Mengen, etwa $\{\text{rot}, \text{grün}, \text{blau}\}$, $\{0, 1\}$ oder die Zahlenmengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (siehe Tabelle 4), welche wir später genauer einführen.

$\mathbb{N} := \{0, 1, 2, \dots\}$	„natürliche Zahlen“
$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$	„ganze Zahlen“
$\mathbb{Q} := \{\frac{a}{b} \mid a \in \mathbb{Z},\, b \in \mathbb{N} \setminus \{0\}\}$	„rationale Zahlen“
$\mathbb{R}$	„reelle Zahlen“
$\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$	„komplexe Zahlen“

Tabelle 4: Zahlenmengen

Der Hauptbegriff der Mengenlehre ist die Elementbeziehung. Wir schreiben $x \in A$ für die Aussage „x ist Element der Menge A“ bzw. „x liegt in A“. Für deren Negation schreiben wir $x \notin A$. Unter einem *Axiom* versetehen wir einen Grundsatz, welcher als wahr angenommen wird, aber nicht bewiesen wird.

Axiom 1 (Extensionalität)**.** Zwei Mengen sind genau dann gleich, wenn sie dieselben Elemente besitzen. Formal ist für Mengen A, B also

$$A = B \;:\Leftrightarrow\; (\forall x : x \in A \Leftrightarrow x \in B)\,.$$

Nach diesem Prinzip gilt beispielsweise $\{a, a\} = \{a\}$ und $\{a, b\} = \{b, a\}$ für alle Elemente a, b. Für die Negation der Aussage $A = B$ schreiben wir $A \neq B$.

Die Menge, die kein Element enthält, heißt *leere Menge* $\varnothing$. Weiterhin ist eine Menge A eine *Teilmenge* einer Menge B, geschrieben $A \subseteq B$, falls jedes Element der Menge A in der Menge B liegt, also

$$A \subseteq B \;:\Leftrightarrow\; (\forall x : x \in A \Rightarrow x \in B)\,.$$

Lemma 2.1. *Für Mengen A, B, C gilt*

a) $\varnothing \subseteq A$ *und* $A \subseteq A$,

b) $A = B \;\Leftrightarrow\; A \subseteq B \wedge B \subseteq A$,

c) $A \subseteq B \wedge B \subseteq C \;\Rightarrow\; A \subseteq C$.

Beweis. a) Offenbar sind $\forall x : x \in \varnothing \Rightarrow x \in A$ und $\forall x : x \in A \Rightarrow x \in A$ wahre Aussagen.

b) Für alle x ist $x \in A \Leftrightarrow x \in B$ äquivalent zu $(x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)$ nach Satz 1.2, a).

c) Zu zeigen ist $\forall x : x \in A \Rightarrow x \in C$. Sei $x \in A$; wegen $A \subseteq B$ folgt $x \in B$, und wegen $B \subseteq C$ folgt weiter $x \in C$. □

Die Negation von $A \subseteq B$ sei mit $A \nsubseteq B$ bezeichnet; es gilt also $A \nsubseteq B$ genau dann, wenn $\exists x : x \in A \wedge x \notin B$. Ferner sei $A \subsetneq B$ (A ist „echte Teilmenge“ von B) definiert durch $A \subseteq B \wedge A \neq B$.

2.1 Konstruktion von Mengen

Was dürfen wir als eine Menge betrachten? Das folgende Problem bei einer zu einfachen Sichtweise ist als Russellsche Antinomie berühmt geworden. Sei eine Menge x „normal“ genannt, falls $x \notin x$ gilt. Betrachten wir nun die Gesamtheit $N := \{x \mid x \notin x\}$ aller normalen Mengen. Ist N eine Menge? Wenn ja, dann wäre entweder N normal oder N nicht normal. Ist N normal, gilt jedoch $N \notin N$, also $N \in N$. Ist N nicht normal, so gilt $N \in N$ und somit $N \notin N$. In beiden Fällen ergibt sich ein Widerspruch!

Wir müssen also etwas Vorsicht walten lassen, weil Mengen offenbar nicht „zu groß“ sein dürfen. Hierfür verwenden wir ein Axiomensystem, welches einerseits reichhaltig genug ist, um die hier benötigte mathematische Theorie zu entwickeln, andererseits jedoch zu keinen Widersprüchen obiger Art führt.

Axiom 2 (Aussonderung)**.** Sei A eine Menge und $P(x)$ ein Prädikat (hier „Bedingung“ genannt). Dann existiert die Menge

$$B := \{x \in A \mid P(x)\}$$

aller Elemente x von A, für die $P(x)$ gilt. Die Bedingung $P(x)$ ist dabei zusammengesetzt aus Prädikaten der Form „$x \in A$“ und den logischen Symbolen $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow, \forall, \exists$.

Seien A, B Mengen, dann sind beispielsweise die Teilmengen $\{x \in A \mid x \in B\}$ und $\{x \in A \mid x \notin B\}$ von A definiert. Elemente von Mengen können selbst wieder Mengen sein, wie die nachfolgende Konstruktion zeigt.

Axiom 3 (Paarbildung)**.** Sind A, B Mengen, so gibt es die Menge $\{A, B\}$, die genau A und B als Elemente enthält.

Im Fall $A = B$ ist also $\{A\}$ die Menge, die genau A als Element enthält. Wir können nun bereits Einiges aus der leeren Menge $\varnothing$ konstruieren, beispielsweise die Mengen $\{\varnothing\}$ und $\{\varnothing, \{\varnothing\}\}$.

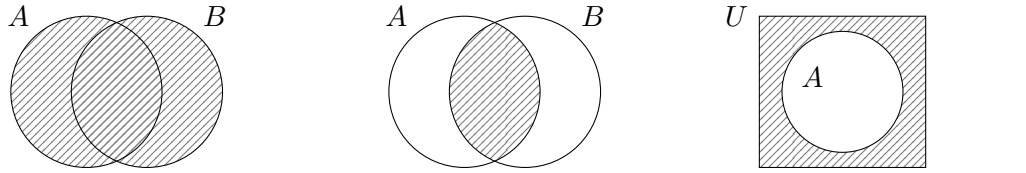
Axiom 4 (Vereinigungsmenge)**.** Sei $\mathcal{C}$ eine Menge von Mengen. Dann ist $\bigcup \mathcal{C}$ die Menge, die genau die Elemente enthält, die in einer Menge aus $\mathcal{C}$ liegen, das heißt

$$x \in \bigcup \mathcal{C} \;:\Leftrightarrow\; \exists A \in \mathcal{C} : x \in A\,.$$

Für $\bigcup \mathcal{C}$ schreiben wir auch $\bigcup_{A \in \mathcal{C}} A$.

Seien A, B Mengen. Dann ist $\mathcal{C} := \{A, B\}$ eine Menge von Mengen und somit ist die *Vereinigungsmenge* $A \cup B := \bigcup \mathcal{C}$ von A und B definiert. Mittels Vereinigung können wir auch drei (oder mehr) Mengen A, B, C in einer Menge zusammenfassen, etwa durch $\{A, B, C\} := \{A, B\} \cup \{C\}$.

Weiterhin bezeichnen wir mit $A \cap B := \{x \in A \mid x \in B\}$ die *Schnittmenge* von A und B, sowie mit $A \setminus B := \{x \in A \mid x \notin B\}$ die *Differenzmenge* „A ohne B“. Ist insbesondere $A \subseteq U$ für eine „Grundmenge“ U, so heißt $U \setminus A = \{x \in U \mid x \notin A\}$ die *Komplementmenge* von A in U, welche wir auch mit A^{c} oder $\overline{A}$ bezeichnen (wenn U klar ist). Mengenkonstruktionen dieser Art lassen sich gut durch *Venn-Diagramme* illustrieren (siehe Abbildung 1).



Vereinigungsmenge $A \cup B$ Schnittmenge $A \cap B$ Komplementmenge $A^{\mathsf{c}} = U \setminus A$

Abbildung 1: Venn-Diagramme

Lemma 2.2. *Seien A, B, U Mengen mit $A \subseteq U$. Dann gilt:*

a) $x \in A^{\mathsf{c}} \;\Leftrightarrow\; \neg(x \in A)$ *für $x \in U$,*

b) $x \in A \cup B \;\Leftrightarrow\; x \in A \vee x \in B$,

c) $x \in A \cap B \;\Leftrightarrow\; x \in A \wedge x \in B$.

Mit den aussagenlogischen Identitäten von Satz 1.1 und Satz 1.2 ergibt sich nun leicht:

Corollar 2.3. *Seien $A, B, C \subseteq U$ Mengen. Dann gilt:*

a)
$$(A \cup B) \cup C = A \cup (B \cup C) \quad A \cup \varnothing = A \quad A \cup A^{\mathsf{c}} = U \quad A \cup B = B \cup A$$
$$(A \cap B) \cap C = A \cap (B \cap C) \quad A \cap U = A \quad A \cap A^{\mathsf{c}} = \varnothing \quad A \cap B = B \cap A$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \text{ und } A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

b) $A = B \;\Leftrightarrow\; (A \subseteq B) \wedge (B \subseteq A) \qquad A^{\mathsf{cc}} = A \qquad A \subseteq B \;\Leftrightarrow\; B^{\mathsf{c}} \subseteq A^{\mathsf{c}}$
$(A \cup B)^{\mathsf{c}} = A^{\mathsf{c}} \cap B^{\mathsf{c}}$ *und* $(A \cap B)^{\mathsf{c}} = A^{\mathsf{c}} \cup B^{\mathsf{c}}$ *(de Morgansche Regeln)*

Um zu sehen, wie die Mengengesetze auf logische Gesetze zurückgeführt werden können, betrachten wir exemplarisch die Identität $(A \cup B)^{\mathsf{c}} = A^{\mathsf{c}} \cap B^{\mathsf{c}}$. Für alle $x \in U$ gilt $x \in (A \cup B)^{\mathsf{c}} \;\Leftrightarrow\; \neg(x \in A \cup B) \;\Leftrightarrow\; \neg(x \in A \vee x \in B)$. Nach Satz 1.2, d) ist dies äquivalent zu $\neg(x \in A) \wedge \neg(x \in B) \;\Leftrightarrow\; x \in A^{\mathsf{c}} \wedge x \in B^{\mathsf{c}} \;\Leftrightarrow\; x \in A^{\mathsf{c}} \cap B^{\mathsf{c}}$.

Axiom 5 (Potenzmenge)**.** Für jede Menge A existiert die *Potenzmenge* $\mathcal{P}(A)$, welche als Elemente genau die Teilmengen von A enthält.

Ist etwa $A = \{x, y\}$, so gilt $\mathcal{P}(A) = \{\varnothing, \{x\}, \{y\}, \{x, y\}\}$. Die Potenzmenge der leeren Menge ist $\mathcal{P}(\varnothing) = \{\varnothing\}$.

Die Regeln von de Morgan können auf beliebige Vereinigungen und Durchschnitte verallgemeinert werden. Für eine Menge von Mengen $\mathcal{C}$ ist nach Axiom 4 die Vereinigungsmenge $\bigcup \mathcal{C}$ definiert durch $x \in \bigcup \mathcal{C} \;\Leftrightarrow\; \exists A \in \mathcal{C} : x \in A$. Ist $\mathcal{C}$ nicht-leer, enthält also mindestens eine Menge A_0, so definieren wir die *Schnittmenge* $\bigcap \mathcal{C} := \{x \in A_0 \mid \forall A \in \mathcal{C} : x \in A\}$, so dass also gilt

$$x \in \bigcap \mathcal{C} \;\Leftrightarrow\; \forall A \in \mathcal{C} : x \in A\,.$$

Für $\bigcup \mathcal{C}$ bzw. $\bigcap \mathcal{C}$ schreiben wir auch $\bigcup_{A \in \mathcal{C}} A$ bzw. $\bigcap_{A \in \mathcal{C}} A$. Im Kontext einer Grundmenge U können wir im Fall $\mathcal{C} = \varnothing$ auch $\bigcap \varnothing := U$ definieren.

Corollar 2.4. *Sei $\mathcal{C} \subseteq \mathcal{P}(U)$ für eine Menge U. Dann gilt*

$$\big(\bigcup_{A\in\mathcal{C}} A\big)^{\mathsf{c}} = \bigcap_{A\in\mathcal{C}} A^{\mathsf{c}} \quad \textit{und} \quad \big(\bigcap_{A\in\mathcal{C}} A\big)^{\mathsf{c}} = \bigcup_{A\in\mathcal{C}} A^{\mathsf{c}}\,.$$

Mit $\bigcap_{A\in\mathcal{C}} A^{\mathsf{c}}$ ist genauer die Menge $\bigcap \mathcal{C}'$ mit $\mathcal{C}' := \{B \in \mathcal{P}(U) \mid B^{\mathsf{c}} \in \mathcal{C}\}$ gemeint; entsprechend bezeichnet $\bigcup_{A\in\mathcal{C}} A^{\mathsf{c}}$ die Menge $\bigcup \mathcal{C}'$.

Beweis. Für $x \in U$ gilt $x \in (\bigcup_{A\in\mathcal{C}} A)^{\mathsf{c}} \;\Leftrightarrow\; \neg(x \in \bigcup_{A\in\mathcal{C}} A) \;\Leftrightarrow\; \neg(\exists A \in \mathcal{C} : x \in A)$, dies ist äquivalent zu $\forall A \in \mathcal{C} : \neg(x \in A) \;\Leftrightarrow\; \forall A \in \mathcal{C} : x \in A^{\mathsf{c}} \;\Leftrightarrow\; x \in \bigcap_{A\in\mathcal{C}} A^{\mathsf{c}}$. Der Beweis der zweiten Identität verläuft entsprechend. □

Seien A, B Mengen. Wir wollen ein Paar (a, b) mit $a \in A$ und $b \in B$ so definieren, dass Gleichheit $(a, b) = (x, y)$ nur dann gilt, wenn $a = x$ und $b = y$ ist, d. h. die Reihenfolge (Ordnung) soll berücksichtigt werden. Dies wird durch die folgende, leider etwas willkürlich erscheinende, Mengenkonstruktion ermöglicht.

Definition 2.1. Zu $a \in A$ und $b \in B$ definiere das *(geordnete) Paar*

$$(a, b) := \big\{\{a\}, \{a, b\}\big\}\,.$$

Lemma 2.5. *Für $a, x \in A$ und $b, y \in B$ gilt*

$$(a, b) = (x, y) \quad \Leftrightarrow \quad a = x \;\textit{ und }\; b = y\,.$$

Beweis. Offenbar gilt $(a, b) = (x, y)$ falls $a = x$ und $b = y$. Sei umgekehrt $\{\{a\}, \{a, b\}\} = \{\{x\}, \{x, y\}\}$ vorausgesetzt. Wir betrachten die Fälle $a = b$ und $a \neq b$.

Ist $a = b$, so haben wir $\{x, y\} \in \{\{a\}, \{a, b\}\} = \{\{a\}\}$, also folgt $x = y = a$.

Sei nun $a \neq b$, so folgt wegen $\{a\} \in \{\{x\}, \{x, y\}\}$ zunächst $a = x$. Weiter ist $\{a, b\} \in \{\{x\}, \{x, y\}\}$, woraus $x \neq y$ und $\{a, b\} = \{x, y\}$ folgt. Da $a = x$ ist, folgt $b = y$. □

Definition 2.2. Seien A, B Mengen. Das *kartesische Produkt* $A \times B$ ist die Menge aller geordneten Paare (a, b) mit $a \in A$ und $b \in B$, also

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

(Mengentheoretisch genauer $A \times B := \{x \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid \exists a \in A\, \exists b \in B :\; x = (a, b)\}$.)

Satz 2.6. *Für Mengen A, B, X, Y gilt:*

a) $(A \cup B) \times X \;=\; (A \times X) \cup (B \times X)$

b) $(A \cap B) \times (X \cap Y) \;=\; (A \times X) \cap (B \times Y)$

c) $A \times B = \varnothing \;\Leftrightarrow\; A = \varnothing \;\vee\; B = \varnothing$

Beweis. a): Es gilt $(u, v) \in (A \cup B) \times X$ genau dann, wenn $(u \in A \vee u \in B) \wedge v \in X$, was nach Distributivgesetz Satz 1.1, e) äquivalent ist zu $(u \in A \wedge v \in X) \vee (u \in B \wedge v \in X)$, das heißt $(u, v) \in (A \times X) \cup (B \times X)$.

b): Es ist $(u, v) \in (A \cap B) \times (X \cap Y)$ äquivalent zu $(u \in A \wedge u \in B) \wedge (v \in X \wedge v \in Y)$, also zu $(u \in A \wedge v \in X) \wedge (u \in B \wedge v \in Y)$, das heißt $(u, v) \in (A \times X) \cap (B \times Y)$.

c): Hierfür können wir $A \times B \neq \varnothing \;\Leftrightarrow\; A \neq \varnothing \wedge B \neq \varnothing$ zeigen. Dies ist aber klar, denn $A \times B \neq \varnothing$ heißt, dass es u, v gibt mit $(u, v) \in A \times B$, also mit $u \in A$ und $v \in B$. □

2.2 Kombinatorik

Für diesen Abschnitt verlassen wir kurz die strikte Mengenlehre und wenden uns dem Zählen endlicher Mengen zu. Eine Menge M ist *endlich*, falls sie endlich viele Elemente hat; deren Anzahl nennen wir die *Kardinalität* von M und schreiben $|M|$ oder $\#M$.

Satz 2.7. *Ist M eine endliche Menge mit n Elementen, so gilt $|\mathcal{P}(M)| = 2^n$.*

Beweis. Mit vollständiger Induktion (Übung). □

Zu einer Menge M und $k \in \mathbb{N}$ definiere die Menge

$$\binom{M}{k} := \{A \subseteq M \mid \#A = k\} \subseteq \mathcal{P}(M)$$

aller k-elementigen Teilmengen von M.

Satz 2.8. *Sei M eine endliche Menge mit n Elementen, sowie $k \in \{0, 1, \ldots, n\}$, dann ist*

$$\left|\binom{M}{k}\right| = \binom{n}{k} := \frac{n!}{k!\,(n-k)!}\,,$$

wobei $\binom{n}{k}$ der Binomialkoeffizient *„n über k“ und $\ell! := 1 \cdot \ldots \cdot \ell$ für $\ell \in \mathbb{N}$ die* Fakultät *sei.*

Beweis. Vollständige Induktion über n (Übung). □

Beispiel 2.1. Betrachten wir ein Tischtennisturnier von fünf Studierenden im Modus „jeder gegen jeden“. Wie viele Partien sind nötig? Dazu betrachten wir die Menge

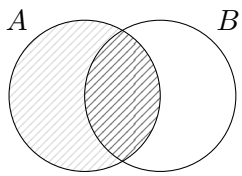
$$\binom{\{a,b,c,d,e\}}{2} = \big\{\{a,b\},\{a,c\},\{a,d\},\{a,e\},\{b,c\},\{b,d\},\{b,e\},\{c,d\},\{c,e\},\{d,e\}\big\}\,,$$

welche $\binom{5}{2} = \frac{5!}{2!\,3!} = 10$ Elemente besitzt, also wird zehnmal gespielt.

Zwei Mengen A, B heißen *disjunkt*, falls $A \cap B = \varnothing$; für die Vereinigung schreibt man dann auch $A \cup B = A \dot\cup B$. Offenbar gilt $|A \dot\cup B| = |A| + |B|$ für endliche disjunkte Mengen A, B. Der folgende Satz verallgemeinert diesen Sachverhalt, siehe Abbildung 2.

Satz 2.9 (Inklusion und Exklusion)**.** *Für endliche Mengen A, B gilt*

$$|A \cup B| = |A| + |B| - |A \cap B|\,.$$



$C = A \cap B$

Abbildung 2: Inklusion und Exklusion

Beweis. Sei $C := A \cap B$. Wegen $B = C \dot\cup B \setminus C$ folgt $|B| = |C| + |B \setminus C|$, also $|B \setminus C| = |B| - |C|$. Und aus $A \cup B = A \dot\cup B \setminus C$ folgt $|A \cup B| = |A| + |B \setminus C| = |A| + |B| - |C|$. □

Beispiel 2.2. Wie viele ganze Zahlen von eins bis hundert sind durch vier oder durch fünf teilbar? Sei $M := \{1, 2, \ldots, 100\}$, sowie $A := \{x \in M \mid 4 \text{ teilt } x\}$ und $B := \{x \in M \mid 5 \text{ teilt } x\}$, dann ist also $|A \cup B|$ gesucht.

Hier ist $|A| = 25$ und $|B| = 20$, sowie $A \cap B = \{x \in M \mid 20 \text{ teilt } x\}$, also $|A \cap B| = 5$. Nach Satz 2.9 folgt somit $|A \cup B| = 25 + 20 - 5 = 40$, die Antwort ist also vierzig.

2.3 Relationen

Relationen beschreiben Beziehungen zwischen Elementen von (zwei) Mengen, etwa X, Y. Wir können sie durch Angabe aller Paare (x, y) mit $x \in X$ und $y \in Y$, für die die Beziehung gilt, spezifizieren.

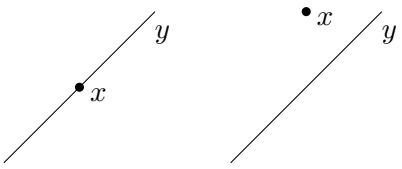
Definition 2.3. Seien X, Y Mengen. Eine *Relation* zwischen X und Y ist eine Teilmenge $R \subseteq X \times Y$; für $(x, y) \in R$ schreiben wir auch $x\,R\,y$.

Wir betrachten hier genauer binäre Relationen. Allgemeiner ist eine „n-äre“ Relation eine Teilmenge $R \subseteq X_1 \times \cdots \times X_n$ eines n-fachen kartesischen Produkts ($n \in \mathbb{N}$); man nennt eine solche Relation für $n = 1$ unär, für $n = 3$ ternär.

$X = Y$ Menschen	$x\,R_1\,y \;:\Leftrightarrow\;$ x ist befreundet mit y
X Punkte, Y Geraden	$x\,R_2\,y \;:\Leftrightarrow\;$ x liegt auf y
$X = Y = \mathbb{Z}$	$x\,R_3\,y \;:\Leftrightarrow\;$ x teilt y
$X = Y = \{a, b, c\}$	$R_4 := \{(a, a), (a, b), (b, c), (c, c)\}$

Tabelle 5: Beispiele für Relationen

Tabelle 5 enthält Beispiele für (binäre) Relationen. Relationen zwischen endlichen Mengen, wie im Beispiel R_4, lassen sich als Kreuztabelle darstellen (setze ein Kreuz in Zeile x und Spalte y, falls $(x, y) \in R$).



x liegt auf y $\quad$ x liegt nicht auf y

Illustration von R_2

	a	b	c
a	×	×	
b			×
c			×

Kreuztabelle von R_4

Eine sehr wichtige Art von Relationen stellen die Äquivalenzrelationen dar.

Definition 2.4. Sei X eine Menge. Eine Relation $R \subseteq X \times X$ heißt *Äquivalenzrelation* auf X, falls gilt:

1) R ist „reflexiv“, d. h. $\forall x \in X : x\,R\,x$,

2) R ist „symmetrisch“, d. h. $\forall x, y \in X : x\,R\,y \;\Rightarrow\; y\,R\,x$,

3) R ist „transitiv“, d. h. $\forall x, y, z \in X : x\,R\,y \;\wedge\; y\,R\,z \;\Rightarrow\; x\,R\,z$.

Wir könnten „symmetrisch“ auch durch $\forall x, y \in X : x\,R\,y \;\Leftrightarrow\; y\,R\,x$ definieren; die beiden Definitionen sind äquivalent. Übung: Welche Eigenschaften erfüllen die Relationen R_1, R_3, R_4 aus Tabelle 5?

Wie wir sehen werden, besteht ein enger Zusammenhang zwischen Äquivalenzrelation und Zerlegungen. Es sei erinnert, dass zwei Mengen A, B disjunkt heißen, falls $A \cap B = \varnothing$ gilt. Ist $\mathcal{C}$ eine Menge von Mengen, so heißen die Mengen in $\mathcal{C}$ *paarweise disjunkt*, falls je zwei verschiedene Mengen $A, B \in \mathcal{C}$ disjunkt sind.

Definition 2.5. Sei X eine Menge. Eine *Zerlegung* von X ist eine Menge $\mathcal{C}$ von paarweise disjunkten, nicht-leeren Mengen mit $\bigcup \mathcal{C} = X$.

Für Zerlegung sagt man auch „Partition“. Die Elemente einer Zerlegung nennt man Teile oder Klassen. Eine Zerlegung von $X = \{a, b, c, d\}$ ist beispielsweise $\mathcal{C} := \{\{a\}, \{b, d\}, \{c\}\}$.

Wir werden nun zu einer Äquivalenzrelation eine Zerlegung konstruieren. Sei R eine Äquivalenzrelation auf X. Zu $x \in X$ sei

$$[x]_R := \{y \in X \mid x\,R\,y\} \subseteq X$$

die *Äquivalenzklasse* von x (bzgl. R); man schreibt auch x/R für $[x]_R$.

Bemerkung 2.10. *Für $x, y \in X$ gilt: $x\,R\,y \;\Leftrightarrow\; [x]_R = [y]_R$.*

Beweis. „$\Leftarrow$“ Gelte $[x]_R = [y]_R$. Da R reflexiv ist, gilt $y \in [y]_R = [x]_R$, also $x\,R\,y$.

„$\Rightarrow$“ Gelte $x\,R\,y$. Wir zeigen $x\,R\,z \;\Leftrightarrow\; y\,R\,z$ für alle $z \in X$, woraus $[x]_R = [y]_R$ folgt. Sei also $x\,R\,z$. Wegen $x\,R\,y$ und da R symmetrisch ist, folgt $y\,R\,x$. Aus $y\,R\,x$, $x\,R\,z$ und der Transitivität von R folgt schließlich $y\,R\,z$. Ist umgekehrt $y\,R\,z$, so folgt wegen $x\,R\,y$ und da R transitiv ist, dass $x\,R\,z$ gilt. □

Definition 2.6. Sei R eine Äquivalenzrelation auf X. Dann ist

$$X/R := \{[x]_R \mid x \in X\} \subseteq \mathcal{P}(X)$$

die Menge der Äquivalenzklassen „X modulo R“.

Wir behaupten, dass $\mathcal{C} := X/R$ eine Zerlegung von X ist. Da R reflexiv ist, gilt $x \in [x]_R \neq \varnothing$ für alle $x \in X$, also ist jede Äquivalenzklasse in der Tat nicht leer. Um zu sehen, dass die Klassen paarweise disjunkt sind, sei angenommen, dass $[x]_R$ und $[y]_R$ für gewisse $x, y \in X$ nicht disjunkt seien. Dann gibt es $z \in X$ mit $z \in [x]_R \cap [y]_R$, also $x\,R\,z$ und $y\,R\,z$. Da R symmetrisch ist folgt $z\,R\,y$ und aus der Transitivität folgt $x\,R\,y$, woraus wir $[x]_R = [y]_R$ mit Bemerkung 2.10 folgern. Schließlich ist $\bigcup \mathcal{C} = X$, denn $\mathcal{C} \subseteq \mathcal{P}(X)$ und für jedes $x \in X$ gilt $x \in [x]_R \in \mathcal{C}$.

Sei nun umgekehrt eine Zerlegung $\mathcal{C}$ gegeben, so definieren wir die Relation $R_\mathcal{C} \subseteq X \times X$ durch

$$x\,R_\mathcal{C}\,y \;:\Leftrightarrow\; \exists A \in \mathcal{C} : x, y \in A$$

(wir schreiben $x, y \in A$ für $x \in A \wedge y \in A$), also $R_\mathcal{C} = \bigcup_{A \in \mathcal{C}} A \times A$.

Dann erfüllt $R_\mathcal{C}$ die Eigenschaften einer Äquivalenzrelation. In der Tat gibt es für jedes $x \in X$ einen Teil $A \in \mathcal{C}$ mit $x \in A$, also gilt $x\,R_\mathcal{C}\,x$ und R ist somit reflexiv. Die Symmetrie ist klar, denn $x, y \in A$ ist offenbar äquivalent zu $y, x \in A$. Seien schließlich $x, y, z \in X$ mit $x\,R_\mathcal{C}\,y$ und $y\,R_\mathcal{C}\,z$, das heißt es gibt Teile $A, B \in \mathcal{C}$ mit $x, y \in A$ und $y, z \in B$. Dann ist $y \in A \cap B \neq \varnothing$, somit sind die Teile A und B gleich. Also gilt $x, z \in A$, das heißt $x\,R_\mathcal{C}\,z$, und R ist somit transitiv.

Satz 2.11. *Sei X eine Menge. Ist R eine Äquivalenzrelation auf X, so ist X/R eine Zerlegung von X. Ist umgekehrt $\mathcal{C}$ eine Zerlegung von X, so ist $R_\mathcal{C}$ eine Äquivalenzrelation auf X. Die beiden Konstruktionen sind invers zueinander, das heißt*

$$R_{X/R} = R \quad \textit{und} \quad X/R_\mathcal{C} = \mathcal{C}\,.$$

Beweis. Die ersten beiden Aussagen haben wir oben bereits gezeigt, also bleibt die dritte Behauptung zu beweisen.

Wir zeigen zunächst die Gleichheit der Relationen $R_{X/R}$ und R. Für $x, y \in X$ gilt

$$\begin{aligned} x\, R_{X/R}\, y &\Leftrightarrow \exists A \in X/R : x, y \in A \\ &\Leftrightarrow \exists z \in X : z\, R\, x \ \wedge\ z\, R\, y\,, \end{aligned}$$

und weil R eine Äquivalenzrelation ist, ist dies äquivalent zu $x\, R\, y$.

Nun zeigen wir die Gleichheit der Zerlegungen $X/R_{\mathcal{C}}$ und $\mathcal{C}$. Für $A \subseteq X$ gilt

$$\begin{aligned} A \in X/R_{\mathcal{C}} &\Leftrightarrow \exists x \in X : A = [x]_{R_{\mathcal{C}}} = \{y \in X \mid x\, R_{\mathcal{C}}\, y\} \\ &\Leftrightarrow \exists x \in X : A = \{y \in X \mid \exists B \in \mathcal{C} : x, y \in B\}\,, \end{aligned}$$

und diese Aussage ist äquivalent zu $A \in \mathcal{C}$, denn: „$\Rightarrow$“ sei $B \in \mathcal{C}$ mit $x \in B$, dann gilt $A = B \in \mathcal{C}$; „$\Leftarrow$“ wähle $x \in A$, dann gilt $\{y \in X \mid \exists B \in \mathcal{C} : x, y \in B\} = A$. □

Beispiel 2.3. Es gibt fünf Zerlegungen von $X = \{a, b, c\}$, nämlich

$$\big\{\{a\}, \{b\}, \{c\}\big\}\,, \quad \big\{\{a, b\}, \{c\}\big\}\,, \quad \big\{\{a, c\}, \{b\}\big\}\,, \quad \big\{\{b, c\}, \{a\}\big\}\,, \quad \big\{\{a, b, c\}\big\}\,.$$

Die zugehörigen Äquivalenzrelationen sind die Folgenden:

	a	b	c
a	×		
b		×	
c			×

	a	b	c
a	×	×	
b	×	×	
c			×

	a	b	c
a	×		×
b		×	
c	×		×

	a	b	c
a	×		
b		×	×
c		×	×

	a	b	c
a	×	×	×
b	×	×	×
c	×	×	×

.

3 Abbildungen

Zudem ist es ein Irrtum zu glauben, dass die Strenge in der Beweisführung die Feindin der Einfachheit wäre.

— David Hilbert (1900)

Seien X und Y Mengen. Unter einer Abbildung von X nach Y verstehen wir eine Vorschrift, die jedem Element $x \in X$ genau ein Element $y \in Y$ zuordnet. Dies können wir mengentheoretisch präzise als eine spezielle Relation definieren.

Definition 3.1. Eine *Abbildung* (oder *Funktion*) f von X nach Y (schreibe $f\colon X \to Y$) ist eine Relation $f \subseteq X \times Y$ derart, dass

$$\forall x \in X\ \exists! y \in Y : (x, y) \in f\,.$$

Für das eindeutig bestimmte Element y schreiben wir $f(x)$, genannt „Funktionswert“ an der „Stelle“ x; wir sagen auch „f bildet (das Argument) x auf (den Wert) y“ ab.

Die Menge X heißt *Definitionsbereich* (engl. domain) und die Menge Y *Zielbereich* (engl. codomain, range).

Eine Relation $f \subseteq X \times Y$ ist also genau dann eine Abbildung, wenn gilt:

a) $\forall x \in X\ \exists y \in Y : (x, y) \in f$ und

b) $\forall x \in X\ \forall y, z \in Y : (x, y) \in f \wedge (x, z) \in f \Rightarrow y = z\,.$

Falls nur b) gilt, so spricht man von einer *partiellen* Abbildung oder Funktion.

Beispiel 3.1. Beispiele für Abbildungen sind sehr zahlreich.

1) Jede eindeutige Zuordnung, zum Beispiel eine Geburtstagstabelle von Kollegen X mit Daten Y kann als Abbildung $f\colon X \to Y$ aufgefasst werden, etwa

$$f := \{(\text{Paul}, 13.10.), (\text{Karin}, 25.4.), (\text{Eva}, 20.7.), \dots\}\,.$$

2) Aus der Analysis sind beispielsweise reelle Funktionen bekannt, wie $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$, das heißt $f := \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$.

3) In der Informatik betrachtet man Unterprogramme oft als Funktionen, die eine Eingabe auf eine Ausgabe abbilden. Eine Hashfunktion etwa bildet größere Datensätze auf einzelne Zeichen oder Zahlen ab, um das Suchen zu erleichtern.

Viele weitere Beispiele für Abbildungen werden uns im Verlauf begegnen.

Wie wir sehen, kann man eine Abbildung $f\colon X \to Y$ direkt als eine Menge geordneter Paare $(x, y) \in X \times Y$ definieren, wie im Beispiel 1). Daneben ist die Argument-Wert-Schreibweise üblich, wie im Beispiel 2): Wir schreiben $f(x) := A(x)$ oder $x \mapsto A(x)$, wobei $A(x)$ ein Ausdruck in der Variable x ist; hiermit ist dann strenggenommen die Relation $f = \{(x, y) \in X \times Y \mid y = A(x)\}$ gemeint.

Wir bemerken zudem, dass unsere mengentheoretische Formulierung eher statischer Natur ist. Einige Mathematiker betrachten Funktionen lieber als aktiv und bezeichnen die Relation $f \subseteq X \times Y$ dann als „Graph“ von f.

Ist $f\colon X \to Y$ eine Abbildung, so ist das *Bild* von f definiert als Menge ihrer Funktionswerte, also

$$\operatorname{im}(f) := \{y \in Y \mid \exists x \in X : f(x) = y\} \subseteq Y\,.$$

Für eine Teilmenge $A \subseteq X$ bezeichnen wir ferner mit $f(A) := \{y \in Y \mid \exists x \in A : f(x) = y\}$ das Bild von A unter f, demnach gilt $\operatorname{im}(f) = f(X)$. Wir definieren die *Einschränkung* $f|_A\colon A \to Y$ der Abbildung f auf A durch $f|_A(x) := f(x)$, das heißt $f|_A = f \cap A \times Y$; dann ist also $\operatorname{im}(f|_A) = f(A)$.

Definition 3.2. Eine Abbildung $f\colon X \to Y$ heißt

- *injektiv*, falls $\forall x, z \in X : f(x) = f(z) \;\Rightarrow\; x = z$,
- *surjektiv*, falls $\forall y \in Y\ \exists x \in X : f(x) = y$,
- *bijektiv*, falls f injektiv und surjektiv ist.

Man nennt eine injektive, surjektive bzw. bijektive Abbildung auch „Injektion“, „Surjektion“ bzw. „Bijektion“.

Bemerkung 3.1. *Sei $f\colon X \to Y$ eine Abbildung. Dann gilt:*

a) f ist genau dann injektiv, wenn $\forall x, z \in X\ \forall y \in Y : (x, y) \in f \wedge (z, y) \in f \;\Rightarrow\; x = z$,

b) f ist genau dann surjektiv, wenn $\forall y \in Y\ \exists x \in X : (x, y) \in f$, bzw. wenn $\operatorname{im}(f) = Y$.

Zerlegungen von Mengen definieren in naheliegender Weise Abbildungen. Ist nämlich $\mathcal{C}$ eine Zerlegung auf X, so ordnen wir jedem $x \in X$ denjenigen Teil $A \in \mathcal{C}$ zu, der x enthält. Somit definiert

$$f := \{(x, A) \in X \times \mathcal{C} \mid x \in A\}$$

eine Abbildung $f\colon X \to \mathcal{C}$, welche zudem surjektiv ist.

Ist zum Beispiel $X := \{a, b, c, d\}$ und sei die Zerlegung $\mathcal{C} := \{A, B, C\}$ gegeben mit $A := \{a\}$, $B := \{b, d\}$ und $C := \{c\}$, so erhalten wir die surjektive Abbildung

$$f\colon X \to \mathcal{C}\,, \quad f = \{(a, A), (b, B), (c, C), (d, B)\}\,.$$

Wir betrachten nun den Fall, dass die Zerlegung $\mathcal{C}$ die Menge der Äquivalenzklassen X/R einer Äquivalenzrelation R ist.

Definition 3.3. Sei R eine Äquivalenzrelation auf X. Dann definiert

$$\pi_R\colon X \to X/R\,, \quad x \mapsto [x]_R$$

eine surjektive Abbildung, die *kanonische* Abbildung.

Umgekehrt spezifiziert jede Abbildung in natürlicher Weise eine Äquivalenzrelation auf dem Definitionsbereich (und damit eine Zerlegung). Und zwar, ist $f\colon X \to Y$ eine Abbildung, so definiert

$$x\, R_f\, y \quad :\Leftrightarrow \quad f(x) = f(y)$$

eine Äquivalenzrelation auf X. Jede Äquivalenzrelation R kann als eine solche aufgefassst werden, denn für die kanonische Abbildung π_R gilt $x\, R_{\pi_R}\, y \;\Leftrightarrow\; [x]_R = [y]_R \;\Leftrightarrow\; x\, R\, y$ nach Bemerkung 2.10, und somit $R_{\pi_R} = R$.

Zum Beispiel können wir so mit der Geburtstagstabelle Kollegen nach deren Geburtstag klassifizieren, das heißt wir haben die Äquivalenzrelation:

$$x\, R_f\, y \quad \Leftrightarrow \quad x \text{ und } y \text{ haben am gleichen Tag Geburtstag}\,.$$

Beim Beispiel der Funktion $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$, erhalten wir eine Äquivalenzrelation auf $\mathbb{R}$ bei der zwei reelle Zahlen genau dann äquivalent sind, wenn sie den gleichen Betrag haben.

Menge aller Abbildungen

Seien X, Y Mengen. Die Menge aller Abbildungen $f\colon X \to Y$ sei mit Y^X bezeichnet; dies ist eine Teilmenge von $\mathcal{P}(X \times Y)$.

Satz 3.2. *Sind X und Y endliche Mengen, so gilt $|Y^X| = |Y|^{|X|}$.*

Beweis. Sei $n := |X| \in \mathbb{N}$ und $m := |Y| \in \mathbb{N}$, dann lautet die Behauptung $|Y^X| = m^n$. Wir beweisen diese mit vollständiger Induktion über n.

(IA): Sei $n = 0$, also $X = \varnothing$. Es gibt $1 = m^0$ Abbildungen $f\colon \varnothing \to Y$ (beachte $\varnothing \times Y = \varnothing$), also ist die Behauptung wahr.

(IS): Sei $|X| = n + 1$. Wähle $z \in X$ und sei $X_0 := X \setminus \{z\}$, also $|X_0| = n$. Mit $Y = \{y_1, \dots, y_m\}$ zerlegen wir die Menge Y^X wie folgt:

$$Y^X = A_1 \dot\cup \dots \dot\cup A_m \quad \text{mit} \quad A_j := \{f \in Y^X \mid f(z) = y_j\}\,.$$

Wir behaupten $|A_j| = m^n$ für alle $j \in \{1, \dots, m\}$. Hierfür betrachten wir die Abbildung $g_j\colon A_j \to Y^{X_0}$, $f \mapsto f|_{X_0}$ (Einschränkung), welche bijektiv ist, und daher gilt $|A_j| = |Y^{X_0}|$. Nach (IV) mit $n = |X_0|$ ist aber $|Y^{X_0}| = m^n$, und somit $|A_j| = m^n$. Schließlich folgt $|Y^X| = m \cdot m^n = m^{n+1}$, wie gewünscht. □

Der Fall $Y = \{0, 1\}$ verdient besondere Aufmerksamkeit. Zu einer Teilmenge $A \subseteq X$ definieren wir die *charakteristische Funktion* $\chi_A \in \{0, 1\}^X$ durch

$$\chi_A(x) := \begin{cases} 1 & \text{falls } x \in A\,, \\ 0 & \text{falls } x \notin A\,. \end{cases}$$

Dann ist die so definierte Abblidung

$$g\colon \mathcal{P}(X) \to \{0, 1\}^X\,, \quad A \mapsto \chi_A$$

eine Bijektion. Wenn X endlich ist, so folgt also $|\mathcal{P}(X)| = |\{0, 1\}^X| = 2^{|X|}$, wie bereits in Satz 2.7 festgestellt wurde.

Familien

Eine abweichende Notation ist für Abbildungen üblich, wenn der Zielbereich wesentlicher erscheint als der Definitionsbereich. Sind I und X Mengen, so bezeichnet man eine Abbildung $x\colon I \to X$ auch als *Familie* in X und schreibt hierfür $(x_i)_{i \in I}$ (oder kurz (x_i)), wobei $x_i := x(i)$ für $i \in I$; dabei nennt man I „Indexmenge“. Wichtige Spezialfälle für diese Schreibweise sind die Folgenden.

1) Sei $I := \{1, \dots, n\}$ mit $n \in \mathbb{N}$. Wir schreiben $(x_i)_{i \in I} = (x_1, \dots, x_n) \in X^n := X^I$ und nennen eine solche Familie auch „n-tupel“.

2) Seien $I := \{1, \dots, m\}$ und $J := \{1, \dots, n\}$ mit $m, n \in \mathbb{N}$. Dann heißt eine Abbildung $A\colon I \times J \to X$ eine „$m \times n$-Matrix“ über X; wir schreiben $A = (a_{ij})_{i \in I,\, j \in J}$ mit $a_{ij} := A(i, j)$, bzw. in Tabellenform

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}.$$

3) Sei $I := \mathbb{N}$, dann heißt $(x_i)_{i\in I}$ eine „Folge“ in X.

4) Sei $X := \mathcal{P}(Y)$ für eine Menge Y. Dann heißt $(A_i)_{i\in I}$ mit $A_i \subseteq Y$ eine „Mengenfamilie“, und wir schreiben $\bigcup_{i\in I} A_i$ für die Vereinigung $\bigcup \mathcal{C}$, sowie $\bigcap_{i\in I} A_i$ für den Durchschnitt $\bigcap \mathcal{C}$, wobei $\mathcal{C} := \{A_i \mid i \in I\} \subseteq \mathcal{P}(Y)$.

Mittels Familien können wir das Konzept des kartesischen Produkts (als Menge aller geordneten Paare) für mehr als zwei Faktoren erweitern.

Definition 3.4. Zu einer Mengenfamilie $(X_i)_{i\in I}$ sei das *kartesische Produkt* definiert als

$$\bigtimes_{i\in I} X_i := \{(x_i)_{i\in I} \mid \forall i \in I : x_i \in X_i\}.$$

Insbesondere ist mit $I := \{1, \dots, n\}$ das kartesische Produkt $X_1 \times \cdots \times X_n$ von Mengen $X_1, \dots, X_n$ definiert ($n \in \mathbb{N}$).

Verkettung

Wir betrachten nun die Hintereinanderausführung von Abbildungen.

Definition 3.5. Seien X, Y, Z Mengen, sowie $f\colon X \to Y$ und $g\colon Y \to Z$ Abbildungen, so ist die Abbildung $g \circ f\colon X \to Z$ definiert durch

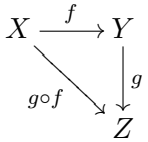
$$(g \circ f)(x) := g(f(x)),$$

das heißt $(x, z) \in g \circ f$ genau dann, wenn $\exists y \in Y : (x, y) \in f \wedge (y, z) \in g$. Man bezeichnet $g \circ f$ als *Verkettung* (oder *Komposition*) „g nach f“.

Die Verkettung von Funktionen definiert also eine Abbildung

$$\circ\colon Y^X \times Z^Y \to Z^X, \quad (f, g) \mapsto g \circ f.$$

Zu beachten ist, dass die Verkettung $g \circ f$ zuerst die Abbildung f auf das Argument anwendet und danach die Abbildung g; dies ist der üblichen Schreibweise geschuldet, die das Argument x rechts von der Funktion f notiert. Oft ist es sinnvoll, Abbildungen und deren Verkettungen durch ein Diagramm zu illustrieren:

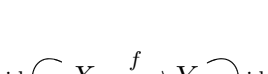


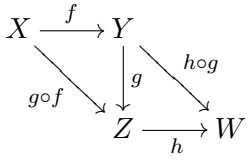
Zu einer Menge X sei die Abbildung $\mathrm{id}_X\colon X \to X$ definiert durch $x \mapsto x$, wir nennen sie „Identitätsabbildung“.

Lemma 3.3. *Seien $f \in Y^X$, $g \in Z^Y$, $h \in W^Z$. Dann gilt:*

a) $\mathrm{id}_Y \circ f = f = f \circ id_X$

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





Beweis. Als Vorbemerkung, zwei Abbildungen $u, v\colon A \to B$ sind genau dann gleich, wenn $u(a) = v(a)$ für alle $a \in A$ gilt.

Teil a) folgt dann aus $\mathrm{id}_Y(f(x)) = f(x) = f(\mathrm{id}_X(x))$ für alle $x \in X$. Für b) betrachte

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x)\,. \qquad \square$$

Umkehrabbildung

Definition 3.6. Eine Abbildung $f\colon X \to Y$ heißt

- *links-invertierbar*, falls $g\colon Y \to X$ existiert mit $g \circ f = \mathrm{id}_X$,
- *rechts-invertierbar*, falls $g\colon Y \to X$ existiert mit $f \circ g = \mathrm{id}_Y$,
- *invertierbar*, falls f links- und rechtsinvertierbar ist.

Sind $g_1, g_2 : Y \to X$ Abbildungen mit $g_1 \circ f = \mathrm{id}_X$ und $f \circ g_2 = \mathrm{id}_Y$, dann ist $g_1 = g_2$. Denn mit Lemma 3.3 gilt $g_2 = \mathrm{id}_X \circ g_2 = (g_1 \circ f) \circ g_2 = g_1 \circ (f \circ g_2) = g_1 \circ \mathrm{id}_Y = g_1$.

Eine Abbildung $f\colon X \to Y$ ist also genau dann invertierbar, wenn es $g\colon Y \to X$ gibt mit $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$. Die Abbildung g ist dann eindeutig und heißt die *Umkehrabbildung* von f, geschrieben $f^{-1} := g$.

Es ist leicht zu sehen, dass eine links-invertierbare Abbildung stets injektiv ist, und dass eine rechts-invertierbare Abbildung stets surjektiv ist.

In der Tat, sind $f\colon X \to Y$ und $g\colon Y \to X$ Abbildungen mit $g \circ f = \mathrm{id}_X$, und gelte $f(x) = f(z)$ für $x, z \in X$, so folgt $x = g(f(x)) = g(f(z)) = z$; also ist f injektiv. Falls $f \circ g = \mathrm{id}_Y$ gilt, so gibt es für jedes $y \in Y$ ein $x \in X$ mit $f(x) = y$, und zwar $x := g(y)$, denn $f(x) = f(g(y)) = y$; somit ist f surjektiv.

Lemma 3.4. *Eine Abbildung $f\colon X \to Y$ ist genau dann invertierbar, wenn sie bijektiv ist. In diesem Fall ist $g := \{(y, x) \in Y \times X \mid (x, y) \in f\}$ die Umkehrabbildung zu f.*

Beweis. Wir haben bereits gesehen, dass eine links- und rechts-invertierbare Abbildung injektiv und surjektiv, also bijektiv ist.

Ist umgekehrt $f\colon X \to Y$ bijektiv, so definiert $\{(y, x) \in Y \times X \mid (x, y) \in f\}$ eine Abbildung $g\colon Y \to X$ und es gilt $g \circ f = \mathrm{id}_X$, sowie $f \circ g = \mathrm{id}_Y$. $\square$

Beispiel 3.2. Die Sinusfunktion $\sin\colon \mathbb{R} \to \mathbb{R}$ ist weder injektiv noch surjektiv. Wenn wir den Definitionsbereich jedoch auf $I := [-\frac{\pi}{2}, \frac{\pi}{2}]$ und den Zielbereich auf $J := [-1, 1]$ einschränken, erhalten wir eine bijektive Abbildung $\sin_*\colon I \to J$, deren Umkehrabbildung der Arcussinus $\arcsin := \sin_*^{-1}\colon J \to I$ ist.

Schließlich sei noch darauf hingewiesen, dass die Notation f^{-1} auch für beliebige Abbildungen $f\colon X \to Y$ benutzt wird, nämlich um für eine Teilmenge $B \subseteq Y$ die „Urbildmenge“

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

von B zu definieren; hierbei braucht f nicht bijektiv zu sein.

4 Zahlen

Die ganzen Zahlen hat der liebe Gott
gemacht, alles andere ist Menschenwerk.
— Leopold Kronecker (1886)

Wie sollen wir Zahlen definieren? Was ist „zwei“? Man könnte versuchen, „zwei“ als Eigenschaft zu definieren, die allen Mengen $\{a, b\}$ mit $a \neq b$ zukommt. Aber was ist die Definition von „Eigenschaft“? Eine Möglichkeit wäre, die Gesamtheit all solcher Mengen $\{a, b\}$ zu betrachten, jedoch ist dann diese Gesamtheit zu groß, um noch eine Menge zu sein. Stattdessen legen wir uns auf ein Standardmodell fest.

Zu einer beliebigen Menge x sei der *Nachfolger* x^+ von x definiert als

$$x^+ := x \cup \{x\}\,.$$

Die Intention dabei ist, dass der Nachfolger x^+ genau ein Element mehr besitzen möge als x. Damit lassen sich die ersten natürlichen Zahlen aus dem „Nichts“ aufbauen:

$$\begin{aligned}
0 &:= \varnothing\,,\\
1 &:= 0^+ = \{0\} = \{\varnothing\}\,,\\
2 &:= 1^+ = \{0, 1\} = \{\varnothing, \{\varnothing\}\}\,,\\
3 &:= 2^+ = \{0, 1, 2\} = \big\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\big\}\,,
\end{aligned}$$

und so weiter. Dass sich diese Konstruktion innerhalb derselben Menge durchführen lässt, wird durch das folgende zusätzliche Mengenaxiom sichergestellt.

Axiom 6 (Unendlichkeit)**.** Es gibt eine Menge M mit $0 \in M$ und $\forall x \in M : x^+ \in M$.

Nun können wir die natürlichen Zahlen präzise definieren.

Definition 4.1. Sei M eine Menge wie in Axiom 6, dann ist die Menge der *natürlichen Zahlen* definiert als kleinste Teilmenge mit der Eigenschaft aus Axiom 6, formal

$$\mathbb{N} := \bigcap \{S \subseteq M \mid 0 \in S \wedge \forall x \in S : x^+ \in S\}\,.$$

Aufgrund der Minimaleigenschaft ist diese Definition unabhängig von M.

Satz 4.1. *Die Menge der natürlichen Zahlen* $\mathbb{N}$ *mit* $0 := \varnothing$ *und* $n^+ := n \cup \{n\}$ *erfüllt die folgenden „Peano-Axiome“:*

a) $0 \in \mathbb{N}$,

b) $\forall n \in \mathbb{N} : n^+ \in \mathbb{N}$,

c) *sei* $S \subseteq \mathbb{N}$ *mit* $0 \in S$ *und* $\forall n \in S : n^+ \in S$, *dann ist* $S = \mathbb{N}$,
(Prinzip der vollständigen Induktion)

d) $\forall n \in \mathbb{N} : n^+ \neq 0$,

e) $\forall n, m \in \mathbb{N} : n^+ = m^+ \;\Rightarrow\; n = m$.

Aus b), d), e) folgt, dass die „Nachfolgeabbildung“ $s\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto n^+$ definiert und nicht surjektiv, aber injektiv ist.

Die natürlichen Zahlen sind durch die Peano-Axiome (bis auf Benennung) eindeutig bestimmt; alle Eigenschaften lassen sich also aus diesen ableiten.

Beweis. Sei $\mathcal{C} := \{S \subseteq M \mid 0 \in S \wedge \forall x \in S : x^+ \in S\}$, so dass also $\mathbb{N} = \bigcap \mathcal{C}$ ist. Die Eigenschaften a) und b) sind klar, da diese für alle $S \in \mathcal{C}$ gelten. Eine Menge $S \subseteq \mathbb{N}$ wie in c) liegt in $\mathcal{C}$, also gilt $\mathbb{N} \subseteq S$ und somit $\mathbb{N} = S$. Weiterhin ist $n \in n^+ \neq \varnothing$ für alle $n \in \mathbb{N}$, also gilt d).

Um Eigenschaft e) zu zeigen, seien $m, n \in \mathbb{N}$ mit

$$n^+ = n \cup \{n\} \;=\; m \cup \{m\} = m^+ .$$

Wegen $n \in m \cup \{m\}$ gilt $n \in m$ oder $n = m$; andersherum gilt $m \in n$ oder $m = n$. Angenommen, es wäre $n \neq m$, dann müsste $n \in m$ und $m \in n$ gelten. Dies führen wir mit den nachfolgenden zwei Hilfsaussagen zu einem Widerspruch. Aus $n \in m \wedge m \in n$ folgt mit ii) dass $n \in n$, und mit i) folgt $n \notin n$, was $n \subseteq n$ widerspricht. Also gilt $n = m$. □

Für natürliche Zahlen $x, y, z \in \mathbb{N}$ gelten:

i) $x \in y \;\Rightarrow\; y \nsubseteq x$,

ii) $x \in y \wedge y \in z \;\Rightarrow\; x \in z$.

Beweis. Um i) zu zeigen, betrachte die Menge $S := \{y \in \mathbb{N} \mid \forall x \in y : y \nsubseteq x\}$. Wir benutzen das Induktionsaxiom Satz 4.1, c), um $S = \mathbb{N}$ zu zeigen. Offenbar ist $0 \in S$. Ist weiter $y \in S$, so folgt $y^+ \in S$. Denn sei $y \in S$ und $x \in y^+$, so ist $x \in y \vee x = y$; wegen $y \in S$ folgt $y \nsubseteq x$ (falls $x \in y$) oder $y \notin x$ (falls $x = y$), somit gilt $y^+ \nsubseteq x$, also $y^+ \in S$.

Analog betrachten wir für ii) die Menge $T := \{z \in \mathbb{N} \mid \forall y \in z \forall x \in y : x \in z\}$. Wiederum gilt $0 \in T$. Und wenn $z \in T$ ist, dann ist $z^+ \in T$. Denn sei $z \in T$ und sei $y \in z^+$, also $y \in z \vee y = z$; für $x \in y$ gilt wegen $z \in T$ dann jeweils $x \in z$ und somit $x \in z^+$, also $z^+ \in T$. Erneut mit Satz 4.1, c) folgern wir $T = \mathbb{N}$. □

4.1 Arithmetik

Das Induktionsprinzip ermöglicht uns, die *Addition* von natürlichen Zahlen rekursiv zu definieren. Für $m, n \in \mathbb{N}$ sei

$$\begin{aligned} m + 0 &:= m \\ m + n^+ &:= (m + n)^+ \end{aligned}$$

(vollständige Induktion über n). Mit $1 = 0^+$ ist also $m + 1 = m + 0^+ = (m + 0)^+ = m^+$.

Lemma 4.2 (Gesetze der Addition)**.** *Für natürliche Zahlen $k, m, n \in \mathbb{N}$ gelten:*

a) $(k + m) + n = k + (m + n)$ *(Assoziativgesetz)*

b) $0 + n = n = n + 0$ *(neutrales Element)*

c) $m + n = n + m$ *(Kommutativgesetz)*

Beweis. Wir zeigen das Assoziativgesetz durch vollständige Induktion über n. Für $n = 0$ gilt $(k + m) + 0 = k + m = k + (m + 0)$. Um von n auf n^+ zu schließen, betrachte $(k + m) + n^+ = ((k + m) + n)^+$; nach Induktionsvoraussetzung ist dies $(k + (m + n))^+ = k + (m + n)^+ = k + (m + n^+)$, also gilt $(k + m) + n^+ = k + (m + n^+)$.

Zum neutralen Element, es ist $n + 0 = n$ nach Definition, also bleibt $0 + n = n$ zu zeigen. Für $n = 0$ ist $0+0 = 0$. Und gilt $0+n = n$ für $n \in \mathbb{N}$, so folgt $0+n^+ = (0+n)^+ = n^+$. Analog beweist man das Kommutativgesetz (Übung; es ist nützlich, zuerst $m^+ + n = (m + n)^+$ zu zeigen). □

Ebenso können wir die *Multiplikation* natürlicher Zahlen rekursiv definieren, wobei wir auf die bereits eingeführte Addition zurückgreifen. Für $m, n \in \mathbb{N}$ sei

$$\begin{aligned} m \cdot 0 &:= 0 \\ m \cdot n^+ &:= m \cdot n + m \end{aligned}$$

(vollständige Induktion über n). Wie üblich legen wir fest, dass die Multiplikation stärker bindet als die Addition, also „Punkt vor Strich“. Es ist auch verbreitet, den Multiplikationspunkt wegzulassen, also $mn := m \cdot n$. Wir halten die folgenden Eigenschaften fest.

Lemma 4.3 (Gesetze der Multiplikation)**.** *Für natürliche Zahlen $k, m, n \in \mathbb{N}$ gelten:*

a)	$(k \cdot m) \cdot n = k \cdot (m \cdot n)$	*(Assoziativgesetz)*
b)	$1 \cdot n = n = n \cdot 1$	*(neutrales Element)*
c)	$0 \cdot n = 0 = n \cdot 0$	*(absorbierendes Element)*
d)	$m \cdot n = n \cdot m$	*(Kommutativgesetz)*
e)	$k \cdot (m + n) = k \cdot m + k \cdot n$	*(Distributivgesetz)*

Beweis. Jeweils mit vollständiger Induktion über n; es ist ratsam, mit dem Distributivgesetz zu beginnen (Übung). □

Eine Menge X mit zwei Verknüpfungen $+\colon X \times X \to X$ und $\cdot\colon X \times X \to X$, für welche die Gesetze aus Lemma 4.2 und Lemma 4.3 gelten, nennt man einen *kommutativen Semiring*. Die natürlichen Zahlen $(\mathbb{N}, +, \cdot)$ bilden also einen kommutativen Semiring.

Weiterhin definiert man die *Potenz* natürlicher Zahlen für $m, n \in \mathbb{N}$ durch

$$\begin{aligned} m^0 &:= 1 \\ m^{n^+} &:= m^n \cdot m \end{aligned}$$

und es lassen sich die üblichen Potenzgesetze per vollständiger Induktion beweisen.

Für die Addition und Multiplikation endlich vieler Zahlen ist das Summensymbol $\sum$ bzw. das Produktsymbol $\prod$ gebräuchlich, welches wir ebenfalls rekursiv definieren können. Ist nämlich $(x_i)_{i \in \mathbb{N}}$ eine Folge in $\mathbb{N}$, so sei für $n \in \mathbb{N}$ definiert:

$$\sum_{i=1}^{0} x_i := 0\,, \qquad \sum_{i=1}^{n^+} x_i := \Big(\sum_{i=1}^{n} x_i\Big) + x_{n+1}$$

$$\prod_{i=1}^{0} x_i := 1\,, \qquad \prod_{i=1}^{n^+} x_i := \Big(\prod_{i=1}^{n} x_i\Big) \cdot x_{n+1}$$

Mit dieser Schreibweise gilt zum Beispiel für die Fakultät $n! = \prod_{i=1}^{n} i$.

Ordnung

Neben den arithmetischen Operationen ist die Vergleichbarkeit der Größe von (natürlichen) Zahlen ein grundlegendes Konzept. Auf der Menge der natürlichen Zahlen $\mathbb{N}$ sei die Relation $\leq \subseteq \mathbb{N} \times \mathbb{N}$ („kleiner gleich“) definiert durch

$$a \leq b \quad :\Leftrightarrow \quad \exists x \in \mathbb{N} \colon\ b = a + x\,.$$

Satz 4.4. *Die Relation $\leq$ auf $\mathbb{N}$ erfüllt folgende Eigenschaften:*

a) $\leq$ *ist reflexiv,*

b) $\leq$ *ist transitiv,*

c) $\leq$ *ist* anti-symmetrisch*, d. h.* $\forall a, b \in \mathbb{N} : \; a \leq b \; \wedge \; b \leq a \; \Rightarrow a = b$*,*

d) $\leq$ *ist* total*, d. h.* $\forall a, b \in \mathbb{N} : \; a \leq b \; \vee \; b \leq a$*.*

Eine reflexive, transitive und anti-symmetrische Relation $\leq$ auf einer Menge X nennt man eine *Ordnung* auf X, somit ist $\leq$ eine *totale Ordnung* auf $\mathbb{N}$. Wir werden Ordnungen auf Mengen in Kapitel 7 detaillierter behandeln.

Beweis. Es ist $\leq$ reflexiv, denn für alle $a \in \mathbb{N}$ ist $a \leq a$ wegen $a = a + 0$. Um die Transitivität zu zeigen, seien $a, b, c \in \mathbb{N}$ mit $a \leq b$ und $b \leq c$. Es gibt also $x, y \in \mathbb{N}$ mit $b = a + x$ und $c = b + y$, woraus $c = a + x + y$ folgt, und somit ist $a \leq c$.

Dass $\leq$ anti-symmetrisch ist, ergibt sich aus den folgenden Eigenschaften der Addition von natürlichen Zahlen. Für $u, v, n \in \mathbb{N}$ gilt:

i) $u + n = v + n \; \Rightarrow \; u = v$ „kürzbar“,

ii) $u + v = 0 \; \Rightarrow \; u = v = 0$ „nullsummenfrei“.

Sei nun $a \leq b$ und $b \leq a$, dann gibt es $x, y \in \mathbb{N}$ mit $b = a + x$ und $a = b + y$, also $a = a + x + y$. Aus i) folgt $x + y = 0$ und wegen ii) ist $x = y = 0$, also $a = b$.

Um zu zeigen, dass $\leq$ total ist, betrachte die Aussage

$$P(n) := \text{„}\forall a \in \mathbb{N} : \; n \leq a \vee a \leq n\text{“}.$$

Wir zeigen $\forall n \in \mathbb{N} : \; P(n)$ per vollständiger Induktion. Es gilt $P(0)$, denn für alle $a \in \mathbb{N}$ ist $0 \leq a$ wegen $a = 0 + a$. Sei nun $P(n)$ vorausgesetzt und wir zeigen $P(n+1)$. Sei also $a \in \mathbb{N}$, dann ist $n \leq a$ oder $a \leq n$ wegen $P(n)$. Im Fall $a \leq n$ folgt $a \leq n + 1$. Sei nun $n \leq a$, es gibt also $x \in \mathbb{N}$ mit $a = n + x$. Ist $x = 0$ so folgt $a = n \leq n + 1$. Ist $x \neq 0$ so gibt es $y \in \mathbb{N}$ mit $x = y + 1$ (Übung), somit ist $a = n + y + 1 = n + 1 + y$, also $n + 1 \leq a$. Damit haben wir $P(n + 1)$ gezeigt. □

Wir verwenden außerdem die üblichen Bezeichnungen

$$a < b \quad :\Leftrightarrow \quad a \leq b \; \wedge \; a \neq b$$

(„echt kleiner gleich“), sowie $a \geq b$ für $b \leq a$ und $a > b$ für $b < a$.

Algebraische Begriffe

Für den Umgang mit arithmetischen Operationen auf verschiedenen Mengen definieren wir nun einige wichtige algebraische Strukturen. Unter einer (zweistelligen) *Verknüpfung* auf einer Menge X verstehen wir eine Abbildung $X \times X \to X$.

Definition 4.2. Eine Menge X mit einer Verknüpfung $*\colon X \times X \to X$, $(x, y) \mapsto x * y$ heißt ein *Monoid* $(X, *)$, falls gilt:

a) $\forall x, y, z \in X : \; (x * y) * z = x * (y * z)$ (Assoziativgesetz)

b) $\exists e \in X \, \forall x \in X : \; e * x = x = x * e$ (e ist eindeutig, *neutrales Element*)

Ein Monoid $(X, *)$ mit neutralem Element $e \in X$ heißt *Gruppe*, falls:

c) $\forall x \in X\, \exists y \in X:\ y * x = e = x * y$ ($x^{-1} := y$ ist eindeutig, *inverses Element*)

Ein Monoid oder eine Gruppe $(X, *)$ ist *kommutativ* (bei Gruppen auch „abelsch"), falls:

d) $\forall x, y \in X:\ x * y = y * x$ (Kommutativgesetz)

Die Eindeutigkeit vom neutralen und inversen Element ist einfach zu sehen: Sind nämlich $e, e' \in X$ neutrale Elemente, so folgt $e' = e * e' = e$; und sind $y, y' \in X$ inverse Elemente zu x, so folgt $y' = e * y' = (y * x) * y' = y * (x * y') = y * e = y$.

Beispiel 4.1. Wir sind bereits Monoiden unterschiedlicher Natur begegnet.

1) Sei X eine Menge. Dann bildet die Menge X^X aller Abbildungen $X \to X$ mit der Verkettung von Abbildungen nach Lemma 3.3 ein Monoid $(X^X, \circ)$.

2) Zu einer Menge X sei $\mathrm{Sym}(X) \subseteq X^X$ die Menge aller bijektiven Abbildungen $X \to X$. Diese bildet mit der Verkettung nach Lemma 3.4 eine Gruppe $(\mathrm{Sym}(X), \circ)$, genannt „symmetrische Gruppe".

3) Nach Lemma 4.2 ist $(\mathbb{N}, +)$ ein kommutatives Monoid.

Häufig sind auf einer Menge zwei Verknüpfungen gegeben, wobei wir die erste „Addition" und die zweite „Multiplikation" nennen. Für derartige Strukturen ist die folgende Definition wichtig.

Definition 4.3. Eine Menge X mit Verknüpfungen $+\colon X \times X \to X$ und $\cdot\colon X \times X \to X$ heißt ein *Semiring* $(X, +, \cdot)$, falls

1) $(X, +)$ ist ein kommutatives Monoid, mit neutralem Element $0 \in X$,

2) $(X, \cdot)$ ist ein Monoid, mit neutralem Element $1 \in X$, und $\forall x \in X:\ 0 \cdot x = 0 = x \cdot 0$,

3) $\forall x, y, z \in X:\ x(y + z) = xy + xz \ \wedge\ (x + y)z = xz + yz$ (Distributivgesetze)

(schreibe $xy := x \cdot y$). Gilt sogar

1') $(X, +)$ ist eine kommutative Gruppe,

so heißt $(X, +, \cdot)$ ein *Ring*. Ein (Semi-)Ring heißt *kommutativ*, falls

2') $(X, \cdot)$ ist ein kommutatives Monoid (und $\forall x \in X:\ 0 \cdot x = 0 = x \cdot 0$).

Schließlich heißt ein kommutativer Ring $(X, +, \cdot)$ ein *Körper*, falls

4) $1 \neq 0$ und $\forall x \in X \setminus \{0\}\, \exists y \in X:\ y \cdot x = 1\, (= x \cdot y)$. (multiplikative Inverse)

Die ganzen Zahlen

Unter Voraussetzung der natürlichen Zahlen führen wir nun die ganzen Zahlen ein. Auf der Menge $X := \mathbb{N} \times \mathbb{N}$ ist eine Äquivalenzrelation $\sim\ \subseteq X \times X$ gegeben durch

$$(a, b) \sim (a', b') \quad :\Leftrightarrow \quad a + b' = a' + b\,.$$

Offenbar gelten Reflexivität und Symmetrie. Ist nun $(a, b) \sim (a', b')$ und $(a', b') \sim (a'', b'')$, also $a + b' = a' + b$ und $a' + b'' = a'' + b'$, so folgt $a + b'' + b' = a' + b'' + b = a'' + b + b'$, wegen Kürzbarkeit also $a + b'' = a'' + b$, das heißt $(a, b) \sim (a'', b'')$, somit ist $\sim$ transitiv.

Wir bezeichnen die Menge der Äquivalenzklassen

$$\mathbb{Z} := \mathbb{N} \times \mathbb{N}/\sim \; = \{[(a,b)] \mid a,b \in \mathbb{N}\}$$

als die Menge der *ganzen Zahlen*. (Wir können $[(a,b)] \in \mathbb{Z}$ als „Bilanz“ interpretieren, mit „Haben“ a und „Soll“ b.)

Via der natürlichen Injektion $\iota\colon \mathbb{N} \to \mathbb{Z}$, $a \mapsto [(a,0)]$ identifizieren wir die natürlichen Zahlen als eine Teilmenge der ganzen Zahlen; wir schreiben fortan $a = [(a,0)]$ für $a \in \mathbb{N}$.

Lemma 4.5. *Die ganzen Zahlen $\mathbb{Z}$ bilden mit der „Addition“ $+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, definiert durch*

$$[(a,b)] + [(c,d)] \; := \; [(a+c, b+d)]$$

für $a,b,c,d \in \mathbb{N}$, eine kommutative Gruppe $(\mathbb{Z},+)$.

Beweis. Zuerst ist die Wohldefiniertheit zu zeigen, also die Unabhängigkeit der Definition von der Wahl der Repräsentanten. Gelte $(a,b) \sim (a',b')$ und $(c,d) \sim (c',d')$, so ist also $(a+c, b+d) \sim (a'+c', b'+d')$ zu zeigen. Dies gilt, denn $a+b' = a'+b$ und $c+d' = c'+d$ impliziert $a+c+b'+d' = a'+c'+b+d$.

Dass dann $(\mathbb{Z},+)$ ein kommutatives Monoid ist folgt unmittelbar, da $(\mathbb{N},+)$ ein kommutatives Monoid ist (Lemma 4.2); das neutrale Element ist $0 = [(0,0)]$. Schließlich gibt es zu jedem $[(a,b)] \in \mathbb{Z}$ ein inverses Element $[(b,a)] \in \mathbb{Z}$, denn $[(a,b)] + [(b,a)] = [(a+b, a+b)] = [(0,0)]$, somit ist $(\mathbb{Z},+)$ eine Gruppe. □

Wir bezeichnen das inverse Element von $[(a,b)] \in \mathbb{Z}$ mit $-[(a,b)] := [(b,a)]$. Für natürliche Zahlen $a \in \mathbb{N}$ ist insbesondere $-a = -[(a,0)] = [(0,a)]$ definiert. Hieraus ergibt sich, dass jede Zahl $z = [(a,b)] \in \mathbb{Z}$ eine Darstellung $z = [(a,0)] + [(0,b)] = a + (-b) =: a - b$ mit $a,b \in \mathbb{N}$ hat, und es gilt $(a,b) \sim (a',b') \;\Leftrightarrow\; a - b = a' - b'$.

Für jede ganze Zahl $z \in \mathbb{Z}$ gibt es sogar eine (eindeutige) natürliche Zahl $x \in \mathbb{N}$ mit $z = x$ oder $z = -x$; das heißt (etwas unpräzise, aber prägnant) $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$. Denn ist $z = [(a,b)] \in \mathbb{Z}$, so ist nach Satz 4.4, d) $a \le b$ oder $b \le a$, also existiert $x \in \mathbb{N}$ mit $b = a + x$ oder $a = b + x$, somit ist $z = [(0,x)] = -x$ oder $z = [(x,0)] = x$.

Lemma 4.6. *Die ganzen Zahlen $\mathbb{Z}$ bilden mit der Addition $+\colon \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ aus Lemma 4.5 und der „Multiplikation“ $\cdot\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, definiert durch*

$$[(a,b)] \cdot [(c,d)] \; := \; [(ac+bd, ad+bc)]$$

für $a,b,c,d \in \mathbb{N}$, einen kommutativen Ring $(\mathbb{Z},+,\cdot)$.

Nach dieser Definition ist also $(a-b)\cdot(c-d) = (ac+bd) - (ad+bc)$.

Beweis. Wesentlich ist die Wohldefiniertheit. Bezeichne $(a,b)\cdot(c,d) := (ac+bd, ad+bc)$, und gelte $(a,b) \sim (a',b')$ und $(c,d) \sim (c',d')$, so zeigen wir $(a,b)\cdot(c,d) \sim (a',b')\cdot(c,d)$ und $(a',b')\cdot(c,d) \sim (a',b')\cdot(c',d')$, woraus $(a,b)\cdot(c,d) \sim (a',b')\cdot(c',d')$ folgt.

Gelte $(a,b) \sim (a',b')$, also $a + b' = a' + b$, so folgt

$$\begin{aligned} ac + bd + a'd + b'c &= (a+b')c + (a'+b)d \\ &= (a'+b)c + (a+b')d = a'c + b'd + ad + bc\,, \end{aligned}$$

also $(a,b)\cdot(c,d) \sim (a',b')\cdot(c,d)$; analog zeigt man $(a',b')\cdot(c,d) \sim (a',b')\cdot(c',d')$.

Die algebraischen Eigenschaften ergeben sich dann leicht aus denjenigen der natürlichen Zahlen (Lemma 4.2 und Lemma 4.3). □

Schließlich sei bemerkt, dass die Multiplikation „nullteilerfrei“ ist, d. h. für $x,y \in \mathbb{Z}$ gilt

$$x \cdot y = 0 \quad \Rightarrow \quad x = 0 \;\vee\; y = 0\,.$$

Die rationalen Zahlen

Die rationalen Zahlen lassen sich wie folgt als „Brüche“ ganzer Zahlen konstruieren. Auf der Menge $X := \mathbb{Z} \times \mathbb{Z}\backslash\{0\}$ definieren wir eine Äquivalenzrelation $\sim \subseteq X \times X$ durch

$$(x, y) \sim (x', y') \quad :\Leftrightarrow \quad xy' = x'y\,.$$

Wieder ist klar, dass $\sim$ reflexiv und symmetrisch ist. Für die Transitivität, sei $(x, y) \sim (x', y')$ und $(x', y') \sim (x'', y'')$, gelte also $xy' = x'y$ und $x'y'' = x''y'$, so folgt $xy''y' = x'yy'' = x''yy'$, wegen $y' \neq 0$ und der Nullteilerfreiheit also $xy'' = x''y$.

Die Menge der Äquivalenzklassen

$$\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}\backslash\{0\}/\sim \; = \{[(x, y)] \mid x, y \in \mathbb{Z},\, y \neq 0\}$$

bezeichnen wir als Menge der *rationalen Zahlen*. Mit der natürlichen Injektion $\iota\colon \mathbb{Z} \to \mathbb{Q}$, $x \mapsto [(x, 1)]$ können wir $\mathbb{Z}$ als Teilmenge von $\mathbb{Q}$ identifizieren.

Lemma 4.7. *Die rationalen Zahlen $\mathbb{Q}$ bilden mit der „Addition“ $+\colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ und der „Multiplikation“ $\cdot\colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, gegeben durch*

$$\begin{aligned} [(x, y)] + [(z, w)] &:= [(xw + yz, yw)] \\ [(x, y)] \cdot [(z, w)] &:= [(xz, yw)] \end{aligned}$$

für $x, y, z, w \in \mathbb{Z}$, $z, w \neq 0$, einen Körper $(\mathbb{Q}, +, \cdot)$.

Beweis. Für die Wohldefiniertheit beachte zunächst $yw \neq 0$ für $y, w \neq 0$. Seien nun $(x, y) \sim (x', y')$ und $(z, w) \sim (z', w')$, also $xy' = x'y$ und $zw' = z'w$, dann gilt

$$(xw + yz)y'w' = (x'w' + y'z')yw \quad \text{und} \quad (xz)(y'w') = (x'z')(yw);$$

also ist $(xw + yz, yw) \sim (x'w' + y'z', y'w')$ und $(xz, yw) \sim (x'z', y'w')$, das heißt die Verknüpfungen sind wohldefiniert.

Die algebraischen Eigenschaften eines Körpers ergeben sich nun wieder einfach aus den Eigenschaften der ganzen Zahlen (Lemma 4.6). Die Eins ist $1 = [(1, 1)]$ und wir haben $[(x, y)] \cdot [(y, x)] = [(xy, xy)] = [(1, 1)]$ für $x, y \in \mathbb{Z}$ mit $x \neq 0$. □

Insbesondere ist $\frac{1}{x} := x^{-1} = [(x, 1)]^{-1} = [(1, x)]$ für eine ganze Zahl $x \in \mathbb{Z}\backslash\{0\}$ definiert, und jede rationale Zahl $q = [(x, y)] \in \mathbb{Q}$ hat eine Darstellung $q = [(x, 1)] \cdot [(1, y)] = x \cdot \frac{1}{y} =: \frac{x}{y}$ mit $x, y \in \mathbb{Z}$ und $y \neq 0$. Für die arithmetischen Operationen auf $\mathbb{Q}$ gilt also

$$\frac{x}{y} + \frac{z}{w} = \frac{xw + yz}{yw} \quad \text{und} \quad \frac{x}{y} \cdot \frac{z}{w} = \frac{xz}{yw}\,.$$

4.2 Teilbarkeit

Wir beleuchten nun die Struktur der Multiplikation auf den natürlichen Zahlen. Auf der Menge $\mathbb{N}$ sei die Relation $\mid \subseteq \mathbb{N} \times \mathbb{N}$ („teilt“) definiert als

$$a \mid b \quad :\Leftrightarrow \quad \exists x \in \mathbb{N} :\, b = ax\,.$$

Die Relation $\mid \subseteq \mathbb{N} \times \mathbb{N}$ ist reflexiv, transitiv und anti-symmetrisch.

Zu einer natürlichen Zahl $n \in \mathbb{N}$ sei

$$T(n) := \{a \in \mathbb{N} \mid a \mid n\}$$

die Menge der *Teiler* von n und $\tau(n) := |T(n)|$ die Anzahl der Teiler von $n > 0$. Beispielsweise gilt $T(0) = \mathbb{N}$ und $T(1) = \{1\}$.

Eine Zahl $n \in \mathbb{N} \setminus \{0, 1\}$ heißt *prim*, falls für $a, b \in \mathbb{N}$ gilt

$$n = ab \quad \Rightarrow \quad a = 1 \ \vee \ b = 1\,.$$

Eine natürliche Zahl n ist also genau dann Primzahl, wenn sie genau zwei Teiler $\tau(n) = 2$ hat, nämlich $T(n) = \{1, n\}$, wobei $n \neq 1$.

Wir betrachten als nächstes Primfaktorzerlegungen. Sei $\mathbb{P} \subseteq \mathbb{N}$ die Menge aller Primzahlen. Jede Familie $(e_p)_{p\in\mathbb{P}}$ von Exponenten $e_p \in \mathbb{N}$ (mit $e_p \neq 0$ für endlich viele p) definiert ein Produkt $\prod_{p\in\mathbb{P}} p^{e_p}$ von Primzahlpotenzen. Sei $\mathbb{N}^{(\mathbb{P})} := \big\{(e_p) \in \mathbb{N}^{\mathbb{P}} \mid \{p \mid e_p \neq 0\} \text{ endlich}\big\}$ die Menge all solcher Familien von Exponenten, so erhalten wir eine Abbildung

$$\psi\colon \mathbb{N}^{(\mathbb{P})} \to \mathbb{N}\setminus\{0\}\,, \quad (e_p) \mapsto \prod_{p\in\mathbb{P}} p^{e_p}\,.$$

Ist beispielsweise $(e_p)_{p\in\mathbb{P}}$ gegeben durch $e_2 = 5$, $e_3 = 2$, $e_7 = 1$, und $e_p = 0$ für alle anderen p, so haben wir $\psi((e_p)) = \prod_{p\in\mathbb{P}} p^{e_p} = 2^5 \cdot 3^2 \cdot 7$.

Wir halten folgende Beobachtung fest: Zu $e = (e_p)$, $f = (f_p) \in \mathbb{N}^{(\mathbb{P})}$ sei $e + f := (e_p + f_p) \in \mathbb{N}^{(\mathbb{P})}$, dann gilt $\prod p^{e_p+f_p} = \prod p^{e_p} \cdot \prod p^{f_p}$, das heißt

$$\psi(e + f) \ = \ \psi(e) \cdot \psi(f)\,.$$

Für die Teilertheorie ist das folgende Theorem, welches wir im Anschluss beweisen werden, von grundlegender Bedeutung. Sei $\mathbb{N}_{>0} := \mathbb{N}\setminus\{0\}$.

Satz 4.8 (Fundamentalsatz der Arithmetik)**.** *Jede Zahl $n \in \mathbb{N}_{>0}$ besitzt eine eindeutige Primfaktorzerlegung*

$$n \ = \ \prod_{p\in\mathbb{P}} p^{e_p}\,.$$

Satz 4.8 besagt gerade, dass die Abbildung ψ bijektiv ist: Die Existenz von Primfaktorzerlegungen bedeutet, dass ψ surjektiv ist und die Eindeutigkeit, dass ψ injektiv ist.

Corollar 4.9. *Für Produkte von Primzahlpotenzen gilt:*

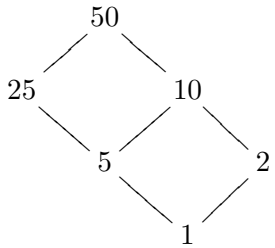
a) $\prod p^{f_p} \mid \prod p^{e_p} \quad \Leftrightarrow \quad \forall p \in \mathbb{P}:\ f_p \leq e_p$

b) $\tau(\prod p^{e_p}) = \prod(e_p + 1)$

Beweis. Zu a): Seien $e = (e_p)$ und $f = (f_p)$ Familien von Exponenten. Wegen der Surjektivität gilt $\psi(f) \mid \psi(e)$ genau dann, wenn es $g = (g_p)$ gibt mit $\psi(f) \cdot \psi(g) = \psi(e)$, also $\psi(f + g) = \psi(e)$. Wegen der Injektivität bedeutet dies $f + g = e$, also $f_p + g_p = e_p$ für gewisse $g_p \in \mathbb{N}$, was äquivalent ist zu $\forall p \in \mathbb{P}:\ f_p \leq e_p$.

Zu b): Aus Teil a) folgt für die Menge der Teiler $T(\psi(e)) = \{\psi(f) \mid \forall p:\ f_p \in \{0, .., e_p\}\}$ und somit $|T(\psi(e))| = \prod(e_p + 1)$. □

Beispiel 4.2. Für $n = 50 = 2 \cdot 5^2$ ist die Teilermenge $T(50) = \{1, 2, 5, 2 \cdot 5, 5^2, 2 \cdot 5^2\}$. Darstellung als „Teilerdiagramm“ (verbinde $a, b \in T(n)$ falls $b = ap$ mit $p \in \mathbb{P}$):



Die Zahl 2016 dagegen hat 36 Teiler, denn $\tau(2016) = \tau(2^5 \cdot 3^2 \cdot 7) = 6 \cdot 3 \cdot 2 = 36$.

Definition 4.4. Seien $a, b \in \mathbb{N}$. Dann heißt eine Zahl $d \in \mathbb{N}$ *größter gemeinsamer Teiler (ggT)* von a und b, falls

$$d \mid a \quad \wedge \quad d \mid b \quad \wedge \quad (\forall d' \in \mathbb{N} : d' \mid a \wedge d' \mid b \;\Rightarrow\; d' \mid d)\,.$$

Dual dazu heißt eine Zahl $e \in \mathbb{N}$ *kleinstes gemeinsames Vielfaches (kgV)* von a und b, falls

$$a \mid e \quad \wedge \quad b \mid e \quad \wedge \quad (\forall e' \in \mathbb{N} : a \mid e' \wedge b \mid e' \;\Rightarrow\; e \mid e')\,.$$

Aus der Definition von ggT und kgV folgt leicht die Eindeutigkeit, denn sind d, d' jeweils größte gemeinsame Teiler von a und b, so gilt $d' \mid d$ und $d \mid d'$, also $d = d'$; analog gilt für kleinste gemeinsame Vielfache e, e', dass $e \mid e'$ und $e' \mid e$, also $e = e'$. Deren Existenz sichert das nächste Resultat.

Corollar 4.10. *Zu natürlichen Zahlen $a = \prod p^{e_p}$ und $b = \prod p^{f_p}$ gibt es jeweils genau einen größten gemeinsamen Teiler d und ein kleinstes gemeinsames Vielfaches e, nämlich*

$$d = \prod p^{\min\{e_p, f_p\}} \quad \text{und} \quad e = \prod p^{\max\{e_p, f_p\}}\,.$$

Hierbei bezeichne $\min\{x, y\}$ bzw. $\max\{x, y\}$ für zwei Zahlen x, y die kleinere bzw. die größere Zahl.

Beweis. Wir übersetzen die Definition von ggT mittels Corollar 4.9, a). Für alle $p \in \mathbb{P}$ gilt $\min\{e_p, f_p\} \leq e_p$ und $\min\{e_p, f_p\} \leq f_p$, also $d \mid a$ und $d \mid b$. Und ist $d' = \prod p^{g_p}$ mit $d' \mid a$ und $d' \mid b$, also $g_p \leq e_p$ und $g_p \leq f_p$ für alle p, so gilt $g_p \leq \min\{e_p, f_p\}$ für alle p, das heißt $d' \mid d$. Dies zeigt, dass d ein ggT von a und b ist, und der Beweis für kgV folgt analog. □

Als weiteres wichtiges Corollar ergibt sich, dass unendliche viele Primzahlen existieren, wie bereits vom Mathematiker Euklid gezeigt wurde. Denn wäre $\mathbb{P} = \{p_1, \ldots, p_k\}$ endlich, so betrachte $n = \prod_{i=1}^{k} p_i + 1$ und leite mit Satz 4.8 einen Widerspruch her (Übung).

Nun beweisen wir den Satz über die eindeutige Primfaktorzerlegung.

Beweis von Satz 4.8 (Existenz). Für die natürlichen Zahlen gilt folgende Eigenschaft:

Jede nicht-leere Menge $A \subseteq \mathbb{N}$ besitzt ein kleinstes Element („Wohlordnung“).

Sei nun angenommen, es habe nicht jede Zahl $n \in \mathbb{N}_{>0}$ eine Primfaktorzerlegung. Dann folgt aus der Wohlordnung, dass es eine kleinste Zahl n ohne Primfaktorzerlegung gibt. Offenbar ist $n \neq 1$ und n nicht prim. Folglich gibt es $a, b \in \mathbb{N}$ mit $n = ab$ und $a, b < n$. Wegen der Minimalität von n haben a und b jedoch Primfaktorzerlegungen, also besitzt auch n eine Primfaktorzerlegung – Widerspruch! □

Für den Beweis der Eindeutigkeit von Primfaktorzerlegungen benutzen wir folgendes Lemma, welches weiter unten gezeigt wird.

Lemma 4.11 (Euklid)**.** *Sei $p \in \mathbb{P}$ und $a, b \in \mathbb{N}$ mit $p \mid ab$, dann gilt $p \mid a \;\vee\; p \mid b$.*

Beweis von Satz 4.8 (Eindeutigkeit). Gilt die Eindeutigkeit nicht, so gibt es eine kleinste Zahl n mit verschiedenen Primfaktorzerlegungen $n = \prod p^{e_p} = \prod p^{f_p}$ (d. h. es gibt $p \in \mathbb{P}$ mit $e_p \neq f_p$). Offenbar ist $n \neq 1$, also gibt es $q \in \mathbb{P}$ mit $e_q \geq 1$. Es folgt

$$q \mid n = \prod_{p \in \mathbb{P}} p^{f_p}\,.$$

Nach Lemma 4.11 teilt q dann einen der Faktoren des Produkts $\prod p^{f_p}$, d. h. es gibt $p \in \mathbb{P}$ mit $f_p \geq 1$ und $q \mid p$. Weil p prim ist, folgt $q = p$, also $f_q \geq 1$. Nun betrachten wir die Primfaktorzerlegungen

$$\tfrac{n}{q} = \prod_{p \in \mathbb{P}} p^{e'_p} = \prod_{p \in \mathbb{P}} p^{f'_p}$$

mit $e'_q = e_q - 1$ und $e'_p = e_p$ für $p \neq q$, sowie $f'_q = f_q - 1$ und $f'_p = f_p$ für $p \neq q$. Diese Primfaktorzerlegungen sind ebenfalls verschieden, im Widerspruch zu $\frac{n}{q} < n$ und der Minimalität von n. □

Der Beweis von Lemma 4.11 schließlich wird aus dem (erweiterten) euklidischen Algorithmus folgen. Grundlage hierfür ist die „Division mit Rest“:

$$\text{Zu } a, b \in \mathbb{N},\ b \neq 0 \ \text{ gibt es } q, r \in \mathbb{N},\ r < b \ \text{ mit } \ a = qb + r\,.$$

Beweis. Per vollständiger Induktion über a. Für $a = 0$ ist $0 = q0 + 0$. Gelte nun $a = qb + r$ mit $r < b$, so ist $a+1 = qb + r + 1$, und falls $r = b-1$ schreiben wir $a+1 = (q+1)b + 0$. □

Lemma 4.12. *Für alle $a, b \in \mathbb{N}$ gibt es $s, t \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = sa + tb$.*

Beweis. Wir konstruieren $s, t \in \mathbb{Z}$ wie gewünscht mit dem *euklidischen Algorithmus*:

Start: $r_0 := a$ $\quad s_0 := 1$ $\quad t_0 := 0$
$\quad\quad r_1 := b$ $\quad s_1 := 0$ $\quad t_1 := 1$

Schritt: sei $r_{n-1} = qr_n + r_{n+1}$ (Division mit Rest), also
$r_{n+1} := r_{n-1} - qr_n \quad s_{n+1} := s_{n-1} - qs_n \quad t_{n+1} := t_{n-1} - qt_n$
wenn $r_{n+1} = 0$ Stopp, setze $s := s_n$ und $t := t_n$.

Für die Korrektheit beachte zunächst, dass $r_i = s_i a + t_i b$ für alle i gilt, insbesondere ist $r_n = sa + tb$. Wir behaupten nun, dass $r_n = d := \mathrm{ggT}(a, b)$ gilt. Wegen $d \mid a$ und $d \mid b$ gilt $d \mid sa + tb = r_n$. Umgekehrt lässt sich zeigen, dass alle r_i mit $i < n$ Vielfache von r_n sind, insbesondere $r_n \mid a$ und $r_n \mid b$; dies impliziert $r_n \mid d$ und somit $r_n = d = sa + tb$. □

Beweis von Lemma 4.11. Gelte $p \mid ab$, aber $p \nmid a$. Dann ist $\mathrm{ggT}(a, p) = 1 = sa + tp$ für gewisse $s, t \in \mathbb{Z}$, also $p \mid sab + tpb = (sa + tp)b = b$. □

Wir haben hiermit den Beweis von Satz 4.8 vollständig abgeschlossen.

Beispiel 4.3. Wir wenden den euklidischen Algorithmus auf $a = 51$ und $b = 15$ an.

$-q$	r_n	s_n	t_n
	51	1	0
-3	15	0	1
-2	6	1	-3
-2	3	-2	7
	0		

Also ist $\mathrm{ggT}(51, 15) = 3 = 7 \cdot 15 - 2 \cdot 51$.

5 Modulare Arithmetik

> *Si numerus a numerorum b, c differentiam metitur, b et c* secundum *a* congrui *dicuntur, sin minus,* incongrui*: ipsum a* modulum *appellamus.*
> — Carl F. Gauß, in: *Disquisitiones Arithmeticae*

Wir kennen bereits den Ring $(\mathbb{Z}, +, \cdot)$ der ganzen Zahlen. Zu $m \in \mathbb{N}_{>0}$ konstruieren wir nun einen endlichen Ring $(\mathbb{Z}_m, +, \cdot)$ mit $|\mathbb{Z}_m| = m$ Elementen. Hierfür betrachten wir auf der Menge $\mathbb{Z}$ die Äquivalenzrelation

$$x \sim_m y \quad :\Leftrightarrow \quad m \mid x - y \quad \Leftrightarrow \quad \exists z \in \mathbb{Z} : x - y = mz\,.$$

Die Reflexivität und die Symmetrie sind jeweils klar; seien $x, y, z \in \mathbb{Z}$ gegeben mit $x \sim_m y$ und $y \sim_m z$, also $m \mid x - y$ und $m \mid y - z$, so folgt $m \mid x - y + y - z = x - z$, also $x \sim_m z$, und somit gilt auch Transitivität. Für $x \sim_m y$ schreibt man auch $x \equiv_m y$ oder $x \equiv y \pmod m$, und man sagt, x und y sind *kongruent modulo* m.

Nun betrachten wir die Menge der Äquivalenzklassen

$$\mathbb{Z}_m := \mathbb{Z}/\!\sim_m = \{[x]_m \mid x \in \mathbb{Z}\}\,.$$

Es ist hilfreich, die „Division mit Rest“ wie folgt zu erweitern:

$$\text{Zu } x \in \mathbb{Z} \text{ gibt es genau ein Paar } q \in \mathbb{Z},\, r \in \{0, .., m-1\} \text{ mit } x = qm + r\,.$$

Beweis. Für $x \in \mathbb{N}$ haben wir die Existenz bereits gezeigt, und daraus folgt diese leicht auch für den Fall $-x \in \mathbb{N}$. Zur Eindeutigkeit, seien $q, q' \in \mathbb{Z}$ und $r, r' \in \{0, .., m-1\}$ mit $qm + r = q'm + r'$, so ist $r - r' = (q' - q)m$, woraus $r = r'$ und $q = q'$ folgt. □

Das (eindeutige) $r \in \{0, ..., m-1\}$ bei der Division von x durch m bezeichnet man als *Rest* $x \bmod m$. Es folgt, dass jedes $[x] \in \mathbb{Z}_m$ von der Form $[x] = [r]$ mit $r = x \bmod m$ ist, und man bezeichnet $[x]$ daher auch als *Restklasse*. Demnach ist $\mathbb{Z}_m = \{[0], \ldots, [m-1]\}$ (schreibe hier $[x] := [x]_m$) und es gilt $|\mathbb{Z}_m| = m$.

Lemma 5.1. *Sei $m \in \mathbb{N}_{>0}$. Die Menge der Restklassen $\mathbb{Z}_m$ bildet mit der „Addition“ $+\colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ und der „Multiplikation“ $\cdot\colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$, gegeben durch*

$$[x] + [y] := [x + y]\,, \qquad [x] \cdot [y] := [x \cdot y]$$

für $x, y \in \mathbb{Z}$, einen kommutativen Ring $(\mathbb{Z}_m, +, \cdot)$.

Beweis. Um die Wohldefiniertheit der Verknüpfungen zu zeigen, seien $x, x', y, y' \in \mathbb{Z}$ mit $x \sim x'$ und $y \sim y'$ gegeben, also $m \mid x - x'$ und $m \mid y - y'$. Dann folgt

$$\begin{aligned} m \mid x - x' + y - y' &= (x + y) - (x' + y') \\ \text{und} \quad m \mid (x - x')y + x'(y - y') &= xy - x'y'\,, \end{aligned}$$

also $x + y \sim x' + y'$ und $xy \sim x'y'$, wie gewünscht. Die Ringgesetze folgen nun direkt aus denen des kommutativen Rings $(\mathbb{Z}, +, \cdot)$; die Null in $\mathbb{Z}_m$ ist $[0]$ und die Eins ist $[1]$. □

Definition 5.1. Man bezeichnet $(\mathbb{Z}_m, +, \cdot)$ als den *Restklassenring* „$\mathbb{Z}$ modulo m“.

Beispiel 5.1. Für eine Restklasse $[x] \in \mathbb{Z}_m$ schreibt man der Einfachheit halber oft $x \in \{0, ..., m-1\}$. Der Ring $(\mathbb{Z}_3 = \{0, 1, 2\}, +, \cdot)$ hat folgende Verknüpfungstafeln:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Im Fall $(\mathbb{Z}_4 = \{0, 1, 2, 3\}, +, \cdot)$ sehen die Tafeln so aus:

$+$	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	3	0	1	2

Wir stellen fest, dass $(\mathbb{Z}_3, +, \cdot)$ sogar ein Körper ist ($[1], [2] \in \mathbb{Z}_3$ haben ein multiplikatives Inverses), während $(\mathbb{Z}_4, +, \cdot)$ kein Körper ist ($[2] \in \mathbb{Z}_4$ hat kein Inverses).

Satz 5.2. *Es ist $(\mathbb{Z}_m, +, \cdot)$ genau dann ein Körper, wenn m eine Primzahl ist.*

Beweis. „$\Rightarrow$“: Wäre m keine Primzahl, so gibt es ein Produkt $m = ab$ mit $a, b \in \mathbb{N}$ und $0 < a, b < m$. Das heißt $[a], [b] \neq [0]$ in $\mathbb{Z}_m$, aber $[0] = [a] \cdot [b]$. Weil $\mathbb{Z}_m$ ein Körper ist, existiert $[a]^{-1}$ und es folgt $[0] = [a]^{-1}([a] \cdot [b]) = [b]$, ein Widerspruch.

„$\Leftarrow$“: Sei $m = p$ eine Primzahl und sei $[0] \neq [x] \in \mathbb{Z}_p$, also ist $p \nmid x$. Dann ist $\mathrm{ggT}(x, p) = 1$ und nach Lemma 4.12 gibt es $s, t \in \mathbb{Z}$ mit $1 = sx + tp$. Daraus folgt $[s] \cdot [x] = [sx] = [1]$, das heißt $[x]^{-1} = [s]$ ist das Inverse zu $[x]$. Also ist $(\mathbb{Z}_p, +, \cdot)$ ein Körper. □

5.1 Die Einheitengruppe $\mathbb{Z}_n^*$

Wir wollen nun die invertierbaren Elemente eines Restklassenrings $\mathbb{Z}_n$ genauer studieren. Diese bilden eine Gruppe, wie folgende allgemeinere Überlegung zeigt.

In einem Monoid $(M, \circ)$ mit neutralem Element $e \in M$ bildet die Menge

$$M^* := \{x \in M \mid \exists y \in M : x \circ y = e = y \circ x\}$$

der invertierbaren Elemente mit der Verknüpfung $\circ\colon M^* \times M^* \to M^*$, $(x, y) \mapsto x \circ y$ eine Gruppe $(M^*, \circ)$.

Beweis. Zunächst ist die Wohldefiniertheit von $\circ$ zu zeigen, d. h. hier $x, y \in M^*$ impliziert $x \circ y \in M^*$. Sind $x^{-1}, y^{-1} \in M$ die Inversen von x und y, so ist $(x \circ y) \circ (y^{-1} \circ x^{-1}) = x \circ (y \circ y^{-1}) \circ x^{-1} = x \circ e \circ x^{-1} = x \circ x^{-1} = e$ und entsprechend $(y^{-1} \circ x^{-1}) \circ (x \circ y) = e$, also ist $x \circ y$ invertierbar mit $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.

Die Assoziativität in M^* ist klar, weil $(M, \circ)$ ein Monoid ist. Wegen $e \in M^*$ gibt es auch ein neutrales Element. Schließlich hat jedes $x \in M^*$ ein inverses Element, denn $x^{-1} \in M^*$. In der Tat ist $x^{-1} \circ x = e = x \circ x^{-1}$, also ist x^{-1} invertierbar mit $(x^{-1})^{-1} = x$. □

Für das Monoid $(M, \circ) = (X^X, \circ)$ aller Abbildungen $X \to X$ auf einer Menge X beispielsweise ist $M^* = \mathrm{Sym}(X)$ die Menge aller bijektiven Abbildungen $X \to X$, welche die „symmetrische Gruppe“ $(\mathrm{Sym}(X), \circ)$ bildet (vgl. Beispiel 4.1).

Wir betrachten nun das multiplikative Monoid eines Rings.

Definition 5.2. Sei $(R, +, \cdot)$ ein Ring. Die Menge der „Einheiten“

$$R^* := \{x \in R \mid \exists y \in R : xy = 1 = yx\}$$

bildet die *Einheitengruppe* $(R^*, \cdot)$ von R.

Proposition 5.3. $\mathbb{Z}_n^* = \{[a] \in \mathbb{Z}_n \mid \mathrm{ggT}(a, n) = 1\}$.

Man nennt Zahlen $a, n \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$ auch *teilerfremd*.

Beweis. Für jede Zahl $a \in \mathbb{Z}$ gilt

$$[a] \in \mathbb{Z}_n^* \quad \Leftrightarrow \quad \exists s \in \mathbb{Z} : [s][a] = [1] \quad \Leftrightarrow \quad \exists s, t \in \mathbb{Z} : sa + tn = 1\,.$$

Gilt nun $\mathrm{ggT}(a, n) = 1$ so gibt es $s, t \in \mathbb{Z}$ mit $sa + tn = 1$ nach Lemma 4.12. Ist umgekehrt $sa + tn = 1$ für gewisse $s, t \in \mathbb{Z}$ erfüllt, so folgt $\mathrm{ggT}(a, n) = 1$; denn ist $d \in \mathbb{N}$ ein gemeinsamer Teiler, also $d \mid a$ und $d \mid n$, so gilt $d \mid sa + tn = 1$, also $d = 1$. □

Beispiel 5.2. Für $n = 8$ erhalten wir die Einheitengruppe $(\mathbb{Z}_8^*, \cdot)$ mit $\mathbb{Z}_8^* = \{[1], [3], [5], [7]\}$ und Verknüpfungstafel:

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Definition 5.3. Zu $n \in \mathbb{N}_{>0}$ sei die *Eulersche Phi-Funktion* definiert durch

$$\varphi(n) := |\mathbb{Z}_n^*| = \big|\{a \in \{0, .., n-1\} \mid \mathrm{ggT}(a, n) = 1\}\big|\,.$$

Beispielsweise gilt $\varphi(1) = 1$ und $\varphi(p) = p-1$ für jede Primzahl $p \in \mathbb{P}$, sowie $\varphi(4) = 2$, $\varphi(6) = 2$, $\varphi(8) = 4$, $\varphi(9) = 6$ und $\varphi(10) = 4$. Die allgemeine Formel für $n = \prod p^{e_p}$ lautet

$$\varphi(n) = n \prod_{p \mid n} (1 - \tfrac{1}{p}) = \prod_{p \in \mathbb{P},\, e_p \geq 1} p^{e_p - 1}(p - 1)\,.$$

Für $n = 2016 = 2^5 \cdot 3^2 \cdot 7$ hat $\mathbb{Z}_n^*$ also $\varphi(n) = 2^4 \cdot 1 \cdot 3^1 \cdot 2 \cdot 7^0 \cdot 6 = 16 \cdot 6 \cdot 6 = 576$ Elemente.

Endliche Mengen

Weitere interessante Eigenschaften der Multiplikation in $\mathbb{Z}_n$ basieren auf der Theorie endlicher Gruppen. Hierfür stellen wir zunächst einige Grundlagen endlicher Mengen bereit. Für $n \in \mathbb{N}$ sei die Menge $[n] := \{1, 2, \ldots, n\}$ (und $[0] := \varnothing$) definiert, welche wir als Standardmodell einer endlichen Menge auffassen können.

Lemma 5.4. *Für $n \in \mathbb{N}$ gilt: Eine injektive Abbildung $f : [n] \to [n]$ ist stets surjektiv.*

Beweis. Wir verwenden vollständige Induktion über n. Im Fall $n = 0$ ist $f : \varnothing \to \varnothing$ nach Definition eine surjektive Abbildung.

Sei die Aussage nun für ein $n \in \mathbb{N}$ wahr und sei $f : [n+1] \to [n+1]$ injektiv. Zu zeigen ist $\mathrm{im}(f) = [n+1]$. Wäre $\mathrm{im}(f) \subseteq [n]$ (Fall I), so ist die Einschränkung $f|_{[n]} : [n] \to [n]$ injektiv, nach Induktionsvoraussetzung also surjektiv; wegen $f(n+1) \in [n]$ gibt es dann $k \in [n]$ mit $f(k) = f(n+1)$, im Widerspruch zur Injektivität von f, denn $k \neq n+1$.

Also gilt $n+1 \in \mathrm{im}(f)$ (Fall II) und somit gibt es $k \in [n+1]$ mit $f(k) = n+1$. Nun ist entweder $k = n+1$ (Fall II-a), dann ist die Einschränkung $f|_{[n]} \colon [n] \to [n]$ injektiv, also surjektiv nach Induktionsvoraussetzung, und somit $[n] \subseteq \mathrm{im}(f)$. Oder es ist $k \neq n+1$ (Fall II-b) und wir definieren $g \colon [n] \to [n]$ durch $g(i) := f(i)$ für $i \neq k$, sowie $g(k) := f(n+1)$; nun ist g injektiv, also nach Induktionsvoraussetzung surjektiv, und wir erhalten wiederum $[n] \subseteq \mathrm{im}(f)$. Zusammen mit $n+1 \in \mathrm{im}(f)$ haben wir somit in jedem Fall $\mathrm{im}(f) = [n+1]$, wie gewünscht. □

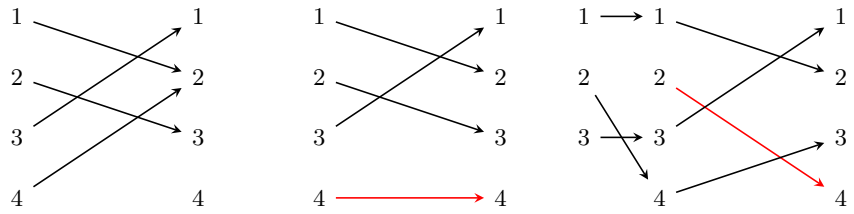


Abbildung 3: Illustration des Induktionsschritts für $n = 3$

Corollar 5.5. *Für $n, m \in \mathbb{N}$ gilt:*

a) Ist $f \colon [n] \to [m]$ injektiv, so ist $n \leq m$.

b) Ist $f \colon [n] \to [m]$ bijektiv, so ist $n = m$.

Beweis. Zu a): Wäre $m < n$, dann wäre $[m] \subsetneq [n]$ und somit f als Abbildung $[n] \to [n]$ nicht surjektiv, im Widerspruch zu Lemma 5.4.

Zu b): Nach a) gilt $n \leq m$. Da die Umkehrabbildung $f^{-1} \colon [m] \to [n]$ injektiv ist, folgt mit a) auch $m \leq n$. □

Nun können wir die Begriffe „endliche Menge“ und „Kardinalität“ präzisieren.

Definition 5.4. Eine Menge X heißt *endlich*, falls $n \in \mathbb{N}$ mit einer Bijektion $f \colon X \to [n]$ existiert. Nach Corollar 5.5, b) ist dieses n eindeutig und wird als *Kardinalität* $|X| := n$ von X bezeichnet.

Für endliche Mengen X, Y können wir nun leicht folgern:

1) Besteht eine Bijektion $f \colon X \to Y$, dann gilt $|X| = |Y|$.

2) Ist $f \colon X \to X$ injektiv, dann ist f surjektiv.

3) Ist $f \colon X \to Y$ injektiv, dann gilt $|X| \leq |Y|$.

Um etwa 3) zu beweisen, sei $|X| = n$, $|Y| = m$ und betrachte das folgende Diagramm:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ [n] & \xrightarrow{F} & [m] \end{array}$$

mit bijektiven Abbildungen g und h. Dann ist $F := h \circ f \circ g^{-1} \colon [n] \to [m]$ injektiv, und somit $n \leq m$ nach Corollar 5.5, a).

Die Kontraposition von 3) ist als „Schubfachprinzip“ bekannt:

$$\text{Falls } |X| > |Y| \text{ gilt, so ist jede Abbildung } f\colon X \to Y \text{ nicht injektiv.}$$

Anschaulich bedeutet dies Folgendes. Wenn man Objekte in Schubfächer legt und es mehr Objekte als Schubfächer gibt, so landen in einem Schubfach mindestens zwei Objekte.

Wir fassen die wichtigsten Aussagen über Abbildungen endlicher Mengen zusammen.

Proposition 5.6. *Seien X, Y endliche Mengen.*

a) Es gelten folgende Äquivalenzen:

i) $|X| \leq |Y| \quad \Leftrightarrow \quad \exists f\colon X \to Y$ *injektiv,*

ii) $|X| \geq |Y| \quad \Leftrightarrow \quad \exists f\colon X \to Y$ *surjektiv,*

iii) $|X| = |Y| \quad \Leftrightarrow \quad \exists f\colon X \to Y$ *bijektiv.*

b) Eine Abbildung $f\colon X \to X$ ist genau dann injektiv, wenn sie surjektiv ist.

Man beachte, dass Aussage b) für nicht-endliche Mengen falsch ist, denn beispielsweise ist die (Nachfolge-)Abbildung $f\colon \mathbb{N} \to \mathbb{N}$, $x \mapsto x+1$ injektiv, aber nicht surjektiv.

Beweis. Zu a). Die Implikationen „$\Rightarrow$“ ergeben sich jeweils leicht aus der Definition von Kardinalität. Die Aussage „i) $\Leftarrow$“ gilt nach der vorigen Bemerkung, 3), und Teil „iii) $\Leftarrow$“ ergibt sich unmittelbar aus i) und ii).

Für „ii) $\Leftarrow$“ betrachte nun eine surjektive Abbildung $f\colon X \to Y$. Weil für alle $y \in Y$ die Urbildmenge $f^{-1}(\{y\})$ nicht-leer ist, existiert[2] eine Abbildung $g\colon Y \to X$ mit $g(y) \in f^{-1}(\{y\})$, also mit $f \circ g = \mathrm{id}_Y$. Es folgt, dass g injektiv ist, und mit i) gilt $|Y| \leq |X|$.

Zu b). Nach der vorigen Bemerkung wissen wir bereits, dass eine injektive Abbildung $f\colon X \to X$ stets surjektiv ist. Sei nun umgekehrt $f\colon X \to X$ surjektiv, dann gibt es wiederum $g\colon X \to X$ mit $f \circ g = \mathrm{id}_X$ und g ist injektiv. Wir wissen dann erneut, dass g surjektiv ist, woraus sich nun die Injektivität von f ergibt. Denn seien $x, y \in X$ mit $f(x) = f(y)$, so gibt es $u, v \in X$ mit $g(u) = x$ und $g(v) = y$, und es folgt

$$u = f(g(u)) = f(x) = f(y) = f(g(v)) = v\,,$$

und somit $x = g(u) = g(v) = y$, das heißt f ist injektiv. □

Für die Arithmetik von Kardinalitäten endlicher Mengen halten wir schließlich folgende Bemerkungen fest. Seien X und Y endliche Mengen.

1) $A \subseteq X \;\Rightarrow\; A$ endlich $\wedge\; |A| \leq |X|$,

2) $X \cap Y = \varnothing \;\Rightarrow\; |X \dot\cup Y| = |X| + |Y|$,

3) $|X \times Y| = |X| \cdot |Y| \quad$ und $\quad |Y^X| = |Y|^{|X|}$,

4) sei $\mathcal{C}$ eine Zerlegung von X, so gilt $|X| = \sum_{A \in \mathcal{C}} |A|$.

[2] Die Existenz einer solchen Abbildung $g\colon Y \to X$ müsste strenggenommen mengentheoretisch sicher gestellt werden und erfordert ein zusätzliches Axiom, das sog. *Auswahlaxiom*. Für endliche Mengen Y kann man jedoch die Existenz aus den bisherigen Axiomen per vollständiger Induktion ableiten.

Endliche Gruppen

Wir beobachten, dass $a^5 \equiv a \pmod 5$ für beliebige Zahlen $a \in \mathbb{Z}$ gilt. Gilt vielleicht $a^p \equiv a \pmod p$ für alle Primzahlen p? Und wie lassen sich solche Aussagen beweisen? Tatsächlich ergeben sie sich als Corollare von Sätzen über endliche Gruppen. In diesem Fall ist die betrachtete Gruppe die Einheitengruppe $\mathbb{Z}_p^*$.

Definition 5.5. Sei $(G, \cdot)$ eine Gruppe mit neutralem Element e. Eine Teilmenge $H \subseteq G$ heißt *Untergruppe* (schreibe $H \leq G$), falls gilt

a) $g, h \in H \;\Rightarrow\; g \cdot h \in H$,

b) $e \in H$,

c) $g \in H \;\Rightarrow\; g^{-1} \in H$.

Dann bildet die Menge H mit der Verknüpfung von G selbst eine Gruppe $(H, \cdot)$.

Zu einer Teilmenge $A \subseteq G$ definieren wir die von A *erzeugte* Untergruppe als

$$\langle A \rangle \;:=\; \bigcap \mathcal{C}_A \,,$$

wobei $\mathcal{C}_A$ die Menge aller Untergruppen $H \leq G$ mit $A \subseteq H$ sei; es ist $\langle A \rangle$ die kleinste Untergruppe von G, welche die Menge A enthält.

Insbesondere haben wir für ein einzelnes Element $a \in G$ als erzeugte Untergruppe

$$\langle a \rangle \;:=\; \langle \{a\} \rangle = \{a^x \mid x \in \mathbb{Z}\}$$

(hierbei sei die Potenz a^x induktiv definiert, via $a^0 := e$ und $a^{n+1} := a^n \cdot a$, sowie $a^{-n} := (a^n)^{-1}$ für $n \in \mathbb{N}$).

Definition 5.6. Eine Gruppe G heißt *zyklisch*, falls es $a \in G$ gibt mit $G = \langle a \rangle$.

Betrachten wir etwa die Gruppe $G := \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$, so ist $H := \langle 2 \rangle = \{1, 2, 4\}$ eine (echte) Untergruppe; andererseits gilt $\langle 3 \rangle = G$, das heißt $\mathbb{Z}_7^*$ ist zyklisch. In der Tat gilt der Satz, dass alle Einheitengruppen $\mathbb{Z}_p^*$ für $p \in \mathbb{P}$ zyklisch sind (ohne Beweis).

Zur effizienten Berechnung einer Potenz a^n (mit $n \in \mathbb{N}$) kann die „square-and-multiply"-Methode angewandt werden. Schreibe hierfür $n = \sum b_i 2^i$ in Binärdarstellung, also mit $b_i \in \{0, 1\}$, so gilt $a^n = \prod (a^{2^i})^{b_i}$, wobei die Potenzen a^{2^i} durch wiederholtes Quadrieren berechnet werden. Zum Beispiel:

$$13 = 2^3 + 2^2 + 1 \quad\Rightarrow\quad a^{13} = ((a^2)^2)^2 \cdot (a^2)^2 \cdot a \,.$$

Hierfür werden höchstens $2 \log_2 n$ Gruppenoperationen benötigt. Alternativ kann man nach folgendem Schema rechnen:

$$13 = 2 \cdot (2 \cdot (2 \cdot 1 + 1) + 0) + 1 \quad\Rightarrow\quad a^{13} = ((a^2 \cdot a)^2)^2 \cdot a \,.$$

Definition 5.7. Eine Gruppe $(G, \cdot)$ heißt endlich, falls die Menge G endlich ist; die Kardinalität $|G|$ wird dann als *Ordnung* von G bezeichnet. Die *Ordnung* eines Elements $a \in G$ ist die Kardinalität $\operatorname{ord}(a) := |\langle a \rangle|$.

Lemma 5.7. *Sei G eine endliche Gruppe und $a \in G$. Dann ist*

$$\operatorname{ord}(a) \;=\; \min\{n \in \mathbb{N}_{>0} \mid a^n = e\} \,,$$

und für $x \in \mathbb{Z}$ gilt $a^x = e \;\Leftrightarrow\; \operatorname{ord}(a) \mid x$.

Beweis. Nach dem Schubfachprinzip gibt es $k, \ell \in \mathbb{Z}$ mit $k < \ell$ und $a^k = a^\ell$, woraus $a^{\ell-k} = e$ folgt, wobei $n := \ell - k > 0$. Also ist das Minimum $m := \min\{n \in \mathbb{N}_{>0} \mid a^n = e\}$ definiert. Für $x \in \mathbb{Z}$ seien nun $q \in \mathbb{Z}$ und $r \in \{0, ..., m-1\}$ mit $x = qm + r$ (Division mit Rest). Wegen $a^m = e$ gilt dann

$$a^x = a^{qm+r} = (a^m)^q a^r = a^r \,.$$

Daraus folgt $\langle a \rangle = \{a^0, a^1, \ldots, a^{m-1}\}$ und $\mathrm{ord}(a) = |\langle a \rangle| = m$. Außerdem sehen wir $a^x = e \;\Leftrightarrow\; r = 0 \;\Leftrightarrow\; m \mid x$. □

Das folgende grundlegende Resultat über endliche Gruppen besagt, dass die Kardinalität von Untergruppen nicht beliebig sein kann.

Satz 5.8 (Lagrange)**.** *Sei G eine endliche Gruppe und sei $H \leq G$ eine Untegruppe. Dann ist $|H|$ ein Teiler von $|G|$.*

Aus diesem wichtigen Satz ergibt sich eine Reihe von Corollaren.

Corollar 5.9. *Sei G eine endliche Gruppe und $a \in G$. Dann gilt $a^{|G|} = e$.*

Beweis. Nach Satz 5.8 teilt $\mathrm{ord}(a) = |\langle a \rangle|$ die Ordnung $|G|$, benutze dann Lemma 5.7. □

Daraus erhalten wir unmittelbar die folgenden zahlentheoretischen Resultate.

Corollar 5.10. *Seien $a \in \mathbb{Z}$, sowie $n \in \mathbb{N}_{>0}$ und $p \in \mathbb{P}$.*

1) Für $[a] \in \mathbb{Z}_n^*$ ist $[a]^{\varphi(n)} = [1]$, das heißt $\mathrm{ggT}(a, n) = 1 \;\Rightarrow\; a^{\varphi(n)} \equiv 1 \pmod{n}$. *(Satz von Euler)*

2) Für $[a] \in \mathbb{Z}_p$ ist $[a]^p = [a]$, das heißt $a^p \equiv a \pmod{p}$. *(Satz von Fermat)*

Nun beweisen wir den Satz von Lagrange.

Beweis von Satz 5.8. Auf der Menge G definiere eine Relation $\sim \subseteq G \times G$ durch

$$g \sim h \quad :\Leftrightarrow \quad g^{-1}h \in H \,.$$

Dann ist $\sim$ eine Äquivalenzrelation, weil H eine Untegruppe ist. In der Tat ist $\sim$ reflexiv, da $e \in H$; es ist $\sim$ auch symmetrisch, denn $g^{-1}h \in H$ impliziert $h^{-1}g = (g^{-1}h)^{-1} \in H$; weiter ist $\sim$ transitiv, denn aus $g^{-1}h \in H$ und $h^{-1}\ell \in H$ folgt $g^{-1}\ell = g^{-1}h \cdot h^{-1}\ell \in H$.

Die Äquivalenzklasse zu einem Element $g \in G$ hat die Form

$$[g]_\sim \;=\; \{h \in G \mid h^{-1}g \in H\} \;=\; \{gh \in G \mid h \in H\} \;=:\; gH \,.$$

Da die Bijektion $f\colon H \to gH$, $h \mapsto gh$ besteht, haben wir $|gH| = |H|$, d. h. alle Klassen haben gleiche Kardinalität. Betrachten wir nun die Zerlegung $\mathcal{C} := G/\!\sim$, so folgt

$$|G| \;=\; \sum_{A \in \mathcal{C}} |A| \;=\; |\mathcal{C}| \cdot |H| \,,$$

und somit ist $|H|$ ein Teiler von $|G|$. □

Man bezeichnet die Kardinalität $|\mathcal{C}|$ der Zerlegung $\mathcal{C} = G/\!\sim$ im obigen Beweis auch als *Index* $[G : H]$ von H in G.

5.2 Anwendungen

Wir stellen hier einige Anwendungen der modularen Arithmetik insbesondere in der Kryptographie vor. Eine wichtige Grundlage dabei ist das schnelle Potenzieren mit der „square-and-multiply"-Methode.

Fermat-Test Ist $p \in \mathbb{P}$ eine Primzahl, so gilt $a^p \equiv a \pmod{p}$ für alle $a \in \mathbb{Z}$ nach Corollar 5.10, b). Wenn es also ein $a \in \mathbb{Z}$ gibt mit $a^p \not\equiv a \pmod{p}$ (oder mit $a^{p-1} \not\equiv 1$, falls $p \nmid a$), dann ist p keine Primzahl.

Dieser einfache Test kann für einen indirekten Nachweis verwendet werden, dass eine Zahl aus mehreren Faktoren zusammengesetzt ist, ohne einen solchen Faktor anzugeben.

Beispiel 5.3 (Fermat-Zahlen)**.** Fermat vermutete 1640, dass die Zahl

$$F_n := 2^{2^n} + 1$$

für $n \in \mathbb{N}$ stets prim sei. Jedenfalls kann man zeigen, dass $2^m + 1$ nur dann eine Primzahl sein kann, wenn $m = 2^n$ für ein $n \in \mathbb{N}$ ist (Übung). Die ersten Fermat-Zahlen lauten

n	0	1	2	3	4
F_n	3	5	17	257	65 537

und bis hierhin stimmt die Vermutung.

Untersuchen wir nun die Zahl $F_5 = 2^{32} + 1 = 4\,294\,967\,297$. Für $n = F_5 - 1 = 2^{32}$ können wir $a^n = a^{2^{32}} \equiv 1$ mittels 32 Quadrierungen modulo F_5 überprüfen. (Im Vergleich dazu müsste man ansonten 6542 Probedivisionen durch Primzahlen $\leq \sqrt{F_5}$ machen.) Mit $a = 3$ erhält man beispielsweise $a^{2^{32}} \equiv 3\,029\,026\,160 \not\equiv 1$, also ist F_5 nicht prim.

Euler zeigte bereits 1732, dass F_5 nicht prim ist, und widerlegte damit Fermats Vermutung. Er fand sogar einen Faktor, nämlich 641, wobei ihm folgende Beobachtung half:

$$\text{Ist } p \in \mathbb{P} \text{ ein Primfaktor von } F_n, \text{ so gilt } p \equiv 1 \pmod{2^{n+1}}.$$

Beweis. Falls $p \mid 2^{2^n} + 1$ gilt, so ist $2^{2^n} \equiv -1 \pmod{p}$. In $\mathbb{Z}_p^*$ ist also $\operatorname{ord}(2) = 2^{n+1}$, was nach Satz 5.8 ein Teiler von $|\mathbb{Z}_p^*| = p - 1$ ist. □

So müssen für $n = 5$ nur Primzahlen $p \equiv 1 \pmod{64}$ getestet werden. Und in der Tat gilt $641 \mid 2^{32} + 1$, denn $2^{32} = (256^2)^2 \equiv 154^2 \equiv -1 \pmod{641}$.

Bemerkung: Es gibt zusammengesetzte Zahlen p, für die $a^p \equiv a \pmod{p}$ für alle $a \in \mathbb{Z}$ gilt. Diese „Pseudo-Primzahlen" werden als *Carmichael-Zahlen* bezeichnet; die kleinste solche Zahl ist $p = 561 = 3 \cdot 11 \cdot 17$.

Grundsätzlich ist es für große Zahlen aufwändiger, sie zu faktorisieren als sie auf Primalität zu testen. Nach aktuellem Stand (2016) ist bekannt, dass alle Fermat-Zahlen $F_5, F_6, \ldots, F_{32}$ nicht prim sind, während nur die Fermat-Zahlen bis F_{11} vollständig faktorisiert sind (und für F_{20} und F_{24} wurde bislang kein einziger Faktor gefunden).

Diffie-Hellman-Schlüsselaustausch Wie vereinbart man einen geheimen Schlüssel über einem öffentlichen Kanal, wie dem Internet, um beispielsweise eine sichere SSL/TLS-Verbindung herzustellen oder für Online-Banking? Viele standardisierte Verfahren basieren auf der von Diffie und Hellman 1976 vorgeschlagenen Methode.

Sei p eine sehr große Primzahl (mindestens 1024 Bits) und sei $g \in \mathbb{Z}_p^*$ ein multiplikativer Erzeuger modulo p, das heißt $\mathbb{Z}_p^* = \langle g \rangle$. Zwei Teilnehmer, sagen wir Alice und Bob, die einen Schlüssel vereinbaren wollen, einigen sich zunächst auf p und g. Danach gehen sie nach folgendem Protokoll vor:

Alice		*öffentlich*		Bob
$a \in \mathbb{Z}_{p-1}$	$\to$	$h_A := g^a$		
		$h_B := g^b$	$\leftarrow$	$b \in \mathbb{Z}_{p-1}$
$k_A := h_B^a = g^{ba}$				$k_B := h_A^b = g^{ab}$

Dadurch haben Alice und Bob den gemeinsamen Schlüssel $k_A = k_B$ vereinbart. Im obigen Protokoll sind die Elemente $a, b \in \mathbb{Z}_{p-1}$ zufällig gewählte „private“ Schlüssel, die unmittelbar nach der Schlüsselvereinbarung gelöscht werden können.

Beispiel 5.4. Betrachte die Gruppe $\mathbb{Z}_{13}^* = \langle 2 \rangle$.

Alice		*öffentlich*		Bob
$a = 4$	$\to$	$h_A = 2^4 \equiv 3$		
		$h_B = 2^5 \equiv 6$	$\leftarrow$	$b = 5$
$h_B^a = 6^4 \equiv 9$				$h_A^b = 3^5 \equiv 9$

Es wurde also der Schlüssel $k_A = k_B = 9 \in \mathbb{Z}_{13}^*$ vereinbart.

Die Sicherheit des vorgestellten Diffie-Hellman-Kryptosystems beruht darauf, dass ein Angreifer selbst dann den Schlüssel g^{ab} praktisch nicht berechnen kann, wenn er die Elemente g, g^a, g^b abhört. Dieses schwierige Berechenbarkeits-Problem wird als *Diffie-Hellman-Problem* (DHP) bezeichnet.

Das DHP und das Protokoll können offenbar gebrochen weden, wenn das *diskrete Logarithmusproblem* (DLP) gelöst wird, nämlich zu gegebenen g, g^a den Exponenten a zu berechnen. Aber auch dieses Problem ist nach heutigem Stand zu schwierig.[3] Die bijektive Abbildung $f\colon \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$, $a \mapsto g^a$ ist eine sogenannte *Einbahnfunktion*, das heißt

- sie ist leicht zu berechnen (mittels „square-and-multiply“),
- die Umkehrabbildung f^{-1} ist schwierig zu berechnen.

Solche Funktionen sind ein wichtiges Fundament für die Kryptographie. Für die obige Abbildung f wird $\log_g := f^{-1}\colon \mathbb{Z}_p^* \to \mathbb{Z}_{p-1}$ als „diskreter Logarithmus“ bezeichnet.

Schließlich sei noch ein wichtiger Aspekt der praktischen Sicherheit erwähnt. Die Kommunikation zwischen Alice und Bob muss (durch zusätzliche Kryptoverfahren) authentisiert werden, da sonst sogenannte „man-in-the-middle“-Angriffe möglich sind, die die Kommunikation auf halbem Wege abfangen und mit beiden Parteien je einen erfolgreichen Diffie-Hellman-Schlüsselaustausch simulieren.

RSA-Verschlüsselung Rivest, Shamir und Adleman schlugen 1978 ihr heute weitverbreitetes Public-Key-Kryptosystem vor, welches auf dem Faktorisierungsproblem basiert. Es handelt sich um ein asymmetrisches Verfahren mit zwei Arten von Schlüsseln, einen öffentlichen zum Verschlüsseln und einen geheimen zum Entschlüsseln.

Man wähle zwei große Primzahlen $p, q \in \mathbb{P}$ (mindestens 512 Bits) und betrachte $n := pq$, so dass also $\varphi(n) = (p-1)(q-1)$. Seien außerdem $e, d \in \mathbb{Z}$ mit $ed \equiv 1 \pmod{\varphi(n)}$, das heißt $[e] \in \mathbb{Z}_{\varphi(n)}^*$ und $[d] = [e]^{-1}$.

$$\begin{array}{rll} \text{öffentlicher Schlüssel} & \text{PK} = (n, e) & \text{(an Alice)} \\ \text{geheimer Schlüssel} & \text{SK} = (n, d) & \text{(von Bob)} \end{array}$$

[3] Der letzte Rekord in einem Körper $\mathbb{Z}_p$ wurde am 16. Juni 2016 aufgestellt; es wurde ein DLP in $\mathbb{Z}_p^*$ für eine Primzahl p mit 768 Bits gelöst, mit einem Hochleistungscluster und einer Rechenzeit von ca. 60 Millionen Core-Stunden. Siehe: `en.wikipedia.org/wiki/Discrete_logarithm_records`

Ist $m \in \mathbb{Z}_n$ eine geheime Nachricht für Bob, so schickt Alice den Chiffretext $c := m^e \in \mathbb{Z}_n$ an Bob. Diesen entschlüsselt Bob durch Berechnen von $c^d \in \mathbb{Z}_n$, denn in der Tat gilt

$$c^d = (m^e)^d = m^{ed} = m\,.$$

Beweis. Wenn $m \in \mathbb{Z}_n^*$ ist (was fast immer der Fall ist), so gilt $m^{\varphi(n)} = 1$ nach Corollar 5.10, a). Wegen $ed \equiv 1 \pmod{\varphi(n)}$ folgt daher $m^{ed} = m$. Der allgemeine Fall wird sich später leicht aus dem chinesischen Restsatz ergeben. □

Die Sicherheit des RSA-Verfahrens basiert auf der Schwierigkeit, zu gegebenen n die Faktoren p und q zu bestimmen, was praktisch äquivalent dazu ist, die Eulerfunktion $\varphi(n) = (p-1)(q-1)$ auszurechnen (Übung). Ist dann $\varphi(n)$ bekannt, so kann man aus dem öffentlichen Schlüssel e leicht den geheimen Schlüssel d als Inverses $e^{-1} \in \mathbb{Z}_{\varphi(n)}^*$ mit dem euklidischen Algorithmus bestimmen. Eine notwendige Voraussetzung ist somit die Schwierigkeit der Faktorisierung großer Zahlen, welche bis heute gegeben ist.[4]

Schließlich sei wieder darauf hingewiesen, dass einige sicherheitsrelevante Aspekte bei dieser Grundversion noch fehlen. Insbesondere müsste der öffentliche Schlüssel PK authentisiert werden, um sicher zu stellen, dass nur der rechtmäßige Besitzer (Bob) die Nachrichten entschlüsseln kann.

5.3 Chinesischer Restsatz

Unser Ziel ist nun, die Struktur des Restklassenrings $(\mathbb{Z}_n, +, \cdot)$ für zusammengesetzte Zahlen n besser zu verstehen. Hierfür ist das Konzept der Isomorphie, also die Präzisierung der Idee „gleich bis auf Umbenennung“, sehr nützlich.

Definition 5.8. Seien $(G, *)$ und $(H, \circ)$ Gruppen. Eine Abbildung $f\colon G \to H$ heißt *(Gruppen-)Homomorphismus* falls

$$f(x * y) \;=\; f(x) \circ f(y)$$

für alle $x, y \in G$ gilt. Wie man leicht nachprüft, fixiert ein Gruppenhomomorphismus $f\colon G \to H$ stets das neutrale Element und es gilt $f(x^{-1}) = f(x)^{-1}$ für alle $x \in G$.

Ein bijektiver Homomorphismus $f\colon G \to H$ heißt *(Gruppen-)Isomorphismus*, und in diesem Fall ist auch die Umkehrabbildung $f^{-1}\colon H \to G$ ein Homomorphismus. Die Gruppen $(G, *)$ und $(H, \circ)$ heißen *isomorph* ($G \cong H$), falls ein Isomorphismus $G \to H$ existiert.

Beispiel 5.5. Die Gruppen $(\mathbb{Z}_5^*, \cdot)$ und $(\mathbb{Z}_4, +)$ sind isomorph. Dies wird deutlich, wenn wir die Verknüpfungstafeln wie folgt aufschreiben:

$(\mathbb{Z}_5^*, \cdot)$

$\cdot$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

$(\mathbb{Z}_4, +)$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

In der Tat ist $f\colon \mathbb{Z}_5^* \to \mathbb{Z}_4$ definiert durch $f(1) = 0$, $f(2) = 1$, $f(3) = 3$ und $f(4) = 2$ ein Gruppenisomorphismus.

[4] Der aktuelle Faktorisierungsrekord wurde am 12. Dez. 2009 aufgestellt, als eine RSA-Zahl n mit 768 Bits unter Verwendung von ca. 20 Millionen Core-Stunden faktorisiert wurde.

Zu Gruppen $(G,\cdot),(H,\cdot)$ sei das *direkte Produkt* $(G\times H,\cdot)$ von G und H definiert durch

$$(x_1,x_2)\cdot(y_1,y_2) := (x_1\cdot y_1, x_2\cdot y_2)$$

für alle $x_1,y_1\in G$ und $x_2,y_2\in H$. Dann ist $(G\times H,\cdot)$ wieder eine Gruppe.

Beispiel 5.6. Die Gruppen $(\mathbb{Z}_8^*,\cdot)$ und $(\mathbb{Z}_2\times\mathbb{Z}_2,+)$ sind isomorph.

$(\mathbb{Z}_8^*,\cdot)$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$(\mathbb{Z}_2\times\mathbb{Z}_2,+)$

$+$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Zyklische Gruppen haben bis auf Isomorphie eine sehr einfache Struktur. In der Tat ist jede zyklische Gruppe $G=\langle g\rangle$ isomorph zur additiven Gruppe von $\mathbb{Z}$ oder von $\mathbb{Z}_n$ für ein $n\in\mathbb{N}_{>0}$, das heißt $(G,\cdot)\cong(\mathbb{Z},+)$ oder $(G,\cdot)\cong(\mathbb{Z}_n,+)$.

Beweis. Betrachte den surjektiven Homomorphismus $f\colon\mathbb{Z}\to G$, $x\mapsto g^x$. Entweder ist die Abbildung f auch injektiv und somit $\mathbb{Z}\cong G$, oder es folgt, dass G endlich ist. In diesem Fall sei $n:=\operatorname{ord}(g)\in\mathbb{N}_{>0}$. Nach Lemma 5.7 gilt $[x]_n=[x']_n \Leftrightarrow g^x=g^{x'}$, also ist durch $\tilde{f}\colon\mathbb{Z}_n\to G$, $[x]\to g^x$ ein Isomorphismus definiert. □

Wir können das Konzept der Isomorphie wie folgt auf Ringe verallgemeinern.

Definition 5.9. Seien $(R,+,\cdot)$ und $(S,+,\cdot)$ Ringe. Eine Abbildung $f\colon R\to S$ heißt *(Ring-)Homomorphismus* falls

$$f(x+y)=f(x)+f(y)\,,\quad f(x\cdot y)=f(x)\cdot f(y)\,,\ f(1)=1$$

für alle $x,y\in R$ gilt (und dann folgt $f(0)=0$ und $f(-x)=-f(x)$ für alle $x\in R$).

Ein bijektiver Homomorphismus $f\colon R\to S$ heißt *Isomorphismus* (und in diesem Fall ist auch $f^{-1}\colon S\to R$ ein Homomorphismus). Die Ringe R und S heißen *isomorph* ($R\cong S$), falls ein Isomorphismus $f\colon R\to S$ existiert.

Zum Beispiel ist für jedes $n\in\mathbb{N}_{>0}$ die natürliche Abbildung

$$f\colon\mathbb{Z}\to\mathbb{Z}_n\,,\quad x\mapsto[x]$$

ein Ringhomomorphismus, denn in der Tat gilt $[x+y]=[x]+[y]$ und $[x\cdot y]=[x]\cdot[y]$ für alle $x,y\in\mathbb{Z}$, und $[1]$ ist die Eins in $\mathbb{Z}_n$.

Man definiert nun das direkte Produkt $(R\times S,+,\cdot)$ von Ringen R und S ganz analog wie im Fall von Gruppen. Aus dem chinesischen Restsatz wird beispielsweise folgen, dass der Ring $\mathbb{Z}_6$ isomorph zum direkten Produkt $\mathbb{Z}_2\times\mathbb{Z}_3$ ist. Der Beweis benutzt folgende Aussage über das kleinste gemeinsame Vielfache teilerfremder Zahlen.

Lemma 5.11. *Seien $n_1,\dots,n_r\in\mathbb{N}_{>0}$ paarweise teilerfremd und sei $n:=\prod_{i=1}^r n_i$. Für $x\in\mathbb{Z}$ gilt dann:*

$$\forall i:\ n_i\mid x \quad\Leftrightarrow\quad n\mid x\,.$$

Der Beweis basiert auf Primfaktorzerlegung. Seien zum Beispiel $n_1=9=3^2$, $n_2=10=2\cdot5$ und $n_3=11$ gegeben, also $n=990=2\cdot3^2\cdot5\cdot11$, dann ist eine Zahl genau dann durch 9, 10 und 11 teilbar, wenn sie durch 990 teilbar ist.

Beweis. Die Richtung „$\Leftarrow$“ ist klar, denn es gilt $n_i \mid n$ für alle i. Um „$\Rightarrow$“ zu zeigen, dürfen wir ohne Einschränkung $x \in \mathbb{N}_{>0}$ annehmen.

Zu $a \in \mathbb{N}_{>0}$ und $p \in \mathbb{P}$ bezeichne $\nu_p(a) := e_p$ den Exponenten von a in der Primfaktorzerlegung $a = \prod p^{e_p}$. Offenbar gilt $\nu_p(a \cdot b) = \nu_p(a) + \nu_p(b)$ für alle $a, b \in \mathbb{N}_{>0}$.

Wir zeigen nun $\nu_p(n) \leq \nu_p(x)$ für alle $p \in \mathbb{P}$, woraus $n \mid x$ folgt. Für jede Primzahl p ist in der Tat

$$\nu_p(n) = \sum_{i=1}^{r} \nu_p(n_i) = \max \nu_p(n_i) \leq \nu_p(x)\,,$$

denn wegen der Teilerfremdheit ist $\nu_p(n_i) \neq 0$ für höchstens ein Index i, und es gilt $\nu_p(n_i) \leq \nu_p(x)$, da nach Voraussetzung $n_i \mid x$. □

Nun können wir den folgenden wichtigen Satz über simultane Kongruenzen und der Struktur des Restklassenrings $\mathbb{Z}_n$ beweisen.

Satz 5.12 (Chinesischer Restsatz)**.** *Seien $n_1, \ldots, n_r \in \mathbb{N}_{>0}$ paarweise teilerfremd und sei $n = \prod_{i=1}^{r} n_i$. Dann gilt:*

a) Für alle $a_1, \ldots, a_r \in \mathbb{Z}$ gibt es genau ein $x \in \{0, \ldots, n-1\}$ mit $x \equiv a_i \pmod{n_i}$.

b) $\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$.

Beweis. Die Abbildung

$$f\colon \mathbb{Z} \to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}\,, \quad x \mapsto ([x]_{n_1}, \ldots, [x]_{n_r})$$

ist ein Ringhomomorphismus. Und es ist $f(x) = 0$ genau dann, wenn $[x]_{n_i} = 0$, also $n_i \mid x$ für alle i gilt, was nach Lemma 5.11 äquivalent ist zu $n \mid x$. Somit gilt $[x]_n = [x']_n$, das heißt $n \mid x - x'$, genau dann, wenn $f(x - x') = 0$, also $f(x) = f(x')$ ist.

Wir definieren nun eine Abbildung

$$\tilde{f}\colon \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}\,, \quad [x] \mapsto f(x)\,.$$

Diese ist dann wohldefiniert, denn wie oben gezeigt gilt $[x]_n = [x']_n \Rightarrow f(x) = f(x')$, sowie injektiv, da $f(x) = f(x') \Rightarrow [x]_n = [x']_n$. Mit Proposition 5.6, b) folgt, dass $\tilde{f}$ auch surjektiv ist, denn $|\mathbb{Z}_n| = n = |\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}|$.

Daraus folgt a) unter Betrachtung von $([a_1]_{n_1}, \ldots, [a_r]_{n_r}) \in \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$. Schließlich ist $\tilde{f}$ ebenfalls (wie f) ein Homomorphismus, denn

$$\tilde{f}([x] + [y]) = \tilde{f}([x + y]) = f(x + y) = f(x) + f(y) = \tilde{f}([x]) + \tilde{f}([y])\,,$$

sowie entsprechend $\tilde{f}([x] \cdot [y]) = \tilde{f}([x]) \cdot \tilde{f}([y])$ und $\tilde{f}([1])$ ist die Eins in $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$. □

Um die Umkehrabbildung $\tilde{f}^{-1}$ zu berechnen, kann man wie folgt vorgehen.

1. Für jedes $j \in \{1, \ldots, r\}$ sei $m_j := \frac{n}{n_j} = \prod_{i \neq j} n_i$, so dass also m_j und n_j teilerfremd sind; dann finde $s, t \in \mathbb{Z}$ mit $sm_j + tn_j = 1$ mit dem eukldisichen Algorithmus (Lemma 4.12) und setze $x_j := sm_j$.

2. Dann löst $x := \sum_j a_j x_j$ die simultane Kongruenz von Satz 5.12, a).

Denn in der Tat ist $x_j \equiv 0 \pmod{n_i}$ für $i \neq j$, sowie $x_j = 1 - tn_j \equiv 1 \pmod{n_j}$. Daraus folgt $x = \sum_j a_j x_j \equiv a_i \pmod{n_i}$ für alle i, weil man in der Summe nur den Index $j = i$ betrachten muss.

Wir können nun die Struktur eines allgemeinen Restklassenrings $\mathbb{Z}_n$ angeben.

Corollar 5.13. *Sei $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ die Primfaktorzerlegung, so gilt*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \ldots \times \mathbb{Z}_{p_r^{e_r}} .$$

Für die Eulersche Phi-Funktion folgt $\varphi(n) = |\mathbb{Z}_n^*| = |\mathbb{Z}_{p_1^{e_1}}^*| \cdot \ldots \cdot |\mathbb{Z}_{p_r^{e_r}}^*| = \prod_i (p_i - 1) p_i^{e_i - 1}$.

Schließlich können wir noch die Korrektheit der RSA-Entschlüsselung für alle Nachrichten in $\mathbb{Z}_n$ zeigen.

Corollar 5.14. *Sei $n = p \cdot q$ mit verschiedenen Primzahlen $p, q \in \mathbb{P}$. Dann gilt $a^{k\varphi(n)+1} \equiv a \pmod{n}$ für alle $a, k \in \mathbb{Z}$.*

Dies begründet etwa die Beobachtung, dass die letzte Ziffer von a^5 stets gleich der letzten Ziffer von a ist (für $a \in \mathbb{N}$), betrachte $n = 10$.

Beweis. Sei $f \colon \mathbb{Z}_n \to \mathbb{Z}_p \times \mathbb{Z}_q$ ein Isomorphismus und sei $(b_1, b_2) := f([a]) \in \mathbb{Z}_p \times \mathbb{Z}_q$. Mit $r := k\varphi(n) + 1 = k(p-1)(q-1) + 1$ gilt $p-1 \mid r-1$ und $q-1 \mid r-1$, also folgt $b_1^r = b_1$ und $b_2^r = b_2$ mit Corollar 5.10, b). Dies bedeutet $f([a])^r = f([a])$, woraus $[a]^r = [a]$ folgt. □

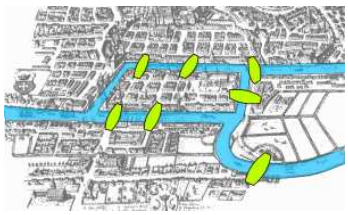
6 Graphentheorie

La mathématique est l'art de donner le même nom à des choses différentes.

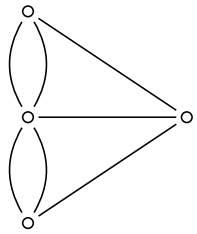
— Henri Poincaré (1908)

Algorithmen auf Graphen oder Netzwerken sind in der Informatik allgegenwärtig. In der Tat erweisen sich Graphen als überaus nützliches Hilfsmittel, sobald man eine Menge von Objekten und deren Beziehungen untereinander modellieren möchte. Wir beginnen mit zwei historischen Beispielen dazu.

Euler betrachtete 1736 das „Königsberger Brückenproblem“, also das Problem, alle sieben Brücken der damaligen Stadt Königsberg genau einmal zu überqueren.



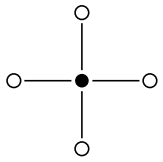
Brücken von Königsberg



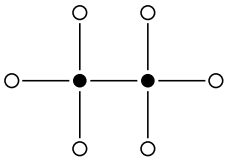
zugehöriger Graph

Nach geeigneter Modellierung betrachtet man einen Graphen, und die Frage lautet, ob es einen „Eulerweg“ darin gibt, d. h. einen Kantenzug, der jede Kante genau einmal durchläuft (nein, wie wir sehen werden).

Im Jahre 1857 untersuchte Cayley Kohlenwasserstoff-Verbindungen der Form C_kH_{2k+2}, beispielsweise:



Methan CH_4



Ethan C_2H_6

Es sind demnach alle Graphen mit $n = k + (2k + 2)$ Knoten zu klassifizieren, wobei k Knoten Grad 4 und die anderen Grad 1 haben.

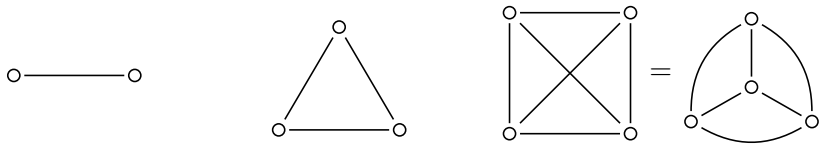
Definition 6.1. Ein *Graph* $G = (V, E)$ besteht aus einer Menge V von *Knoten* (auch *Ecken*, engl. „vertices“) und einer Menge $E \subseteq \binom{V}{2} := \{\{v, w\} \mid v, w \in V, v \neq w\}$ von *Kanten* (engl. „edges“).

Genauer bezeichnet man solche Graphen als einfache ungerichtete Graphen (ohne Schleifen); Graphen mit Mehrfachkanten und/oder gerichtete Kanten werden wir später behandeln. Die Knotenmenge V ist üblicherweise nicht-leer und endlich, dies sei hier fortan generell vorausgesetzt.

Wir definieren nun zwei Familien spezieller Graphen. Zu $n \in \mathbb{N}_{>0}$ sei

$$K_n := \left([n], \tbinom{[n]}{2}\right),$$

wobei $[n] := \{1, \ldots, n\}$, der *vollständige* (engl. „complete“) Graph mit n Knoten; dieser Graph besitzt $\binom{n}{2} = \frac{1}{2}n(n-1)$ Kanten. Zum Beispiel ist $K_4 = (V, E)$ mit $V = \{1, 2, 3, 4\}$ und den 6 Kanten $E = \big\{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\big\}$.



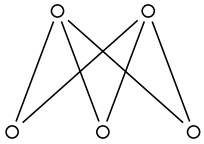
K_2 K_3 K_4

Wie wir am Beispiel K_4 sehen, kann der gleiche Graph durch unterschiedliche Diagramme dargestellt werden.

Weiterhin sei zu $m, n \in \mathbb{N}_{>0}$ der *vollständig bipartite* Graph definiert als

$$K_{m,n} := \left(A \dot\cup B,\ \big\{\{a,b\} \mid a \in A,\, b \in B\big\}\right),$$

wobei A, B disjunkte Mengen mit $|A| = m$ und $|B| = n$ seien; der Graph $K_{m,n}$ hat also $m+n$ Knoten und mn Kanten.

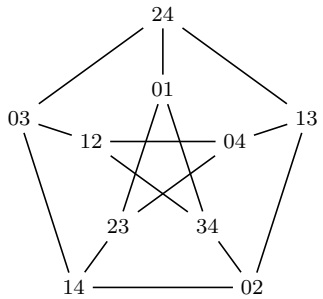


$K_{2,3}$

Beispiel 6.1. Sei $X = \mathbb{Z}_5 = \{0,1,2,3,4\}$. Der *Petersen-Graph* ist der Graph

$$G := \left(\tbinom{X}{2},\ \{\{A,B\} \mid A, B \in \tbinom{X}{2},\ A \cap B = \varnothing\}\right),$$

bestehend aus den 10 Knoten $\binom{X}{2} = \{01, 02, 03, 04, 12, 13, 14, 23, 24, 34\}$ (Kurzschreibweise ab für $\{a,b\}$) und 15 Kanten. Dieser Graph wird oft als Beispiel oder Gegenbeispiel verwendet, um graphentheoretische Aussagen zu illustrieren.



Sei $G = (V, E)$ ein Graph. Wir bezeichnen zwei Knoten $v, w \in V$ als *benachbart* (oder *adjazent*), falls $\{v, w\} \in E$. Zu einem Knoten $v \in V$ sei der *Grad* von v definiert als

$$\deg(v) := |\{e \in E \mid v \in e\}| = |\{w \in V \mid \{v,w\} \in E\}|,$$

d. h. als die Anzahl angrenzender Kanten bzw. als Anzahl benachbarter Knoten.

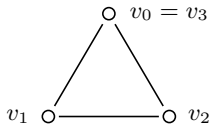
Lemma 6.1. *Für jeden Graphen $G = (V, E)$ gilt $\sum_{v \in V} \deg(v) = 2|E|$.*

Beweis. Wir zählen die „Inzidenzen“ $\{(v, e) \in V \times E \mid v \in e\}$ auf zwei Arten: jeder Knoten $v \in V$ hat $\deg(v)$ anliegende Kanten, und jede Kante $e = \{v, w\} \in E$ hat zwei Knoten. □

6.1 Bäume

Zusammenhängende Graphen ohne zyklische Strukturen sind von besonderer Bedeutung. Wir werden sie Bäume nennen und in diesem Abschnitt untersuchen.

Definition 6.2. Ein *Weg* (auch „Pfad“ oder „Kantenzug“) in einem Graphen $G = (V, E)$ ist eine Folge $v_0, \dots, v_s \in V$ von Knoten derart, dass $\{v_i, v_{i+1}\} \in E$ für alle $0 \leq i < s$ ist. Man spricht dann von einem Weg von $a := v_0$ nach $b := v_s$ der Länge $s \in \mathbb{N}$. Ein Weg heißt *Kreis*, falls $v_s = v_0$ und $s \geq 3$, sowie $v_i \neq v_j$ für alle $0 \leq i < j < s$ gilt.



Kreis der Länge 3

Ein Graph heißt *zusammenhängend* falls je zwei Knoten durch einen Weg verbunden sind, sowie *kreisfrei* falls keine Kreise existieren. Einen zusammenhängenden kreisfreien Graphen nennt man einen *Baum*.

Lemma 6.2. *Ist $G = (V, E)$ mit $\deg(v) \geq 2$ für alle $v \in V$, so besitzt G einen Kreis.*

Beweis. Wir konstruieren induktiv einen Weg wie folgt. Starte mit $v_0 \in V$ beliebig; wegen $\deg(v_0) \geq 1$ existiert dann ein Nachbar v_1 von v_0. Und ist bereits ein Weg $v_0, \dots, v_j \in V$ konstruiert (wobei $j \geq 1$), so gibt es wegen $\deg(v_j) \geq 2$ einen Nachbarn v_{j+1} von v_j mit $v_{j+1} \neq v_{j-1}$.

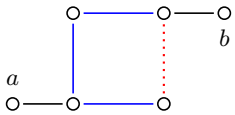
Sei nun $n := |V|$, dann folgt aus dem Schubfachprinzip, dass die Knoten $v_0, \dots, v_n$ nicht paarweise verschieden sind, also gibt es $0 \leq i < j \leq n$ mit $v_i = v_j$. Nach Konstruktion der Folge ist dann notwendig $j - i \geq 3$, und ist j minimal gewählt (mit $j > i$ und $v_i = v_j$), so ist die (Teil-)Folge $v_i, \dots, v_j$ ein Kreis in G. □

Mit diesem Lemma können wir die folgende Charakterisierung von Bäumen beweisen.

Satz 6.3. *Ein zusammenhängender Graph $G = (V, E)$ ist genau dann kreisfrei, also ein Baum, wenn $|E| = |V| - 1$ gilt.*

Beweis. „⇒“. Vollständige Induktion über $n := |V|$. Im Fall $n = 1$ ist $E = \varnothing$, also die Aussage wahr. Sei nun $G = (V, E)$ ein Baum mit $|V| = n > 1$ Knoten. Da G kreisfrei ist, existiert nach Lemma 6.2 ein Knoten v mit $\deg(v) \leq 1$, und da G zusammenhängend ist, muss $\deg(v) = 1$ sein. Sei w der eindeutige Nachbar von v und $e := \{v, w\} \in E$ die zugehörige Kante. Wenn wir v und e aus G entfernen, erhalten wir einen Graphen $\tilde{G} := (V \setminus \{v\}, E \setminus \{e\})$, welcher wieder zusammenhängend und kreisfrei, also ein Baum ist. Wegen $|V \setminus \{v\}| = n-1$ gilt nach Induktionsvoraussetzung $|E \setminus \{e\}| = |V \setminus \{v\}| - 1$, also $|E| - 1 = (|V| - 1) - 1$ und somit $|E| = |V| - 1$.

„⇐“. Wenn es einen Kreis gibt, so kann eine (beliebige) Kante im Kreis entfernt werden, wobei der Graph zusammenhängend bleibt.



„Umleitung“

Man iteriere diesen Vorgang solange, bis ein kreisfreier Graph $\tilde{G} = (V, \tilde{E})$ entsteht. Werden dabei $t \in \mathbb{N}$ Kanten entfernt, so gilt $|E| - t = |\tilde{E}| = |V| - 1$ nach „⇒“. Nach Voraussetzung ist $|V| - 1 = |E|$, also muss $t = 0$ gelten, das heißt, der Graph war bereits kreisfrei. □

Für den Graphen $G = (V, E)$ einer Kohlenwasserstoffverbindung der Form $C_k H_\ell$ gilt

$$4k + \ell \;=\; \sum_{v \in V} \deg(v) \;=\; 2|E|$$

nach Lemma 6.1, also ist nach Satz 6.3 der Graph G genau dann ein Baum, wenn $4k + \ell = 2(k + \ell) - 2$, also $\ell = 2k + 2$ gilt.

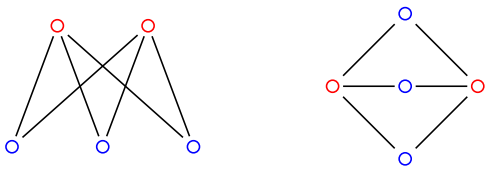
Bäume zählen Wir erweitern zunächst den Begriff der Isomorphie auf Graphen.

Definition 6.3. Seien $G = (V, E)$ und $\tilde{G} = (\tilde{V}, \tilde{E})$ Graphen. Eine Abbildung $f\colon V \to \tilde{V}$ heißt *Homomorphismus*, falls

$$\{v, w\} \in E \quad \Rightarrow \quad \{f(v), f(w)\} \in \tilde{E}$$

für $v, w \in V$ gilt. Ein bijektiver Homomorphismus $f\colon V \to \tilde{V}$, für den auch $f^{-1}\colon \tilde{V} \to V$ ein Homomorphismus ist (also $\{v, w\} \in E \;\Leftrightarrow\; \{f(v), f(w)\} \in \tilde{E}$ gilt), heißt *Isomorphismus*, und in diesem Fall nennt man die Graphen G und $\tilde{G}$ *isomorph* ($G \cong \tilde{G}$).

Beispielsweise sind die folgenden Graphen isomorph:



Das Problem, die Anzahl der Bäume bis auf Isomorphie zu bestimmen, erweist sich als zu schwierig. Stattdessen werden wir eine Formel für die Anzahl der markierten Bäume zeigen. Wir bezeichnen einen Graphen $G = (V, E)$ als „markiert“, falls die Knoten mit $1, \ldots, n$ markiert sind; wir können dann einfach $V = [n] = \{1, \ldots, n\}$ annehmen.

Es erweist sich als sinnvoll, als Knoten endliche Teilmengen von $\mathbb{N}$ (oder allgemeiner „total geordnete Mengen“) zu betrachten. In einem Baum bezeichnen wir einen Knoten v mit genau einer angrenzenden Kante, das heißt mit $\deg(v) = 1$, als *Blatt*.

Definition 6.4. Zu einem Baum $T = (V, E)$ mit $V \subset \mathbb{N}$ und $|V| = n \geq 2$ definieren wir den *Prüfer-Code* $(a_1, \ldots, a_{n-2}) \in V^{n-2}$ wie folgt:

1) $a_1 := w$, wobei $v \in V$ das kleinste Blatt und w der Nachbarknoten von v sei,

2) $(a_2, \ldots, a_{n-2})$ sei der Prüfer-Code des Baums $(V \setminus \{v\},\, E \setminus \{\{v, w\}\})$.

Das heißt, wir notieren den Nachbarknoten des kleinsten Blattes, entfernen das Blatt und die zugehörige Kante, und wiederholen den Vorgang bis eine Kante übrig bleibt.

Abbildung 4 listet alle markierten Bäume bis vier Knoten und deren Prüfer-Codes auf. Deren Isomorphieklassen sind in Abbildung 5 zusammengefasst.

Satz 6.4 (Cayley)**.** *Die Anzahl markierter Bäume mit n Knoten ist genau n^{n-2}.*

Beweis. Sei $f(T) := \underline{a} = (a_1, \ldots, a_{n-2})$ der Prüfer-Code eines Baums $T = (V, E)$ mit $|V| = n$. Wir beweisen zuerst folgende Hilfsbehauptung:

$$\deg(v) \geq 2 \quad \Leftrightarrow \quad \exists i :\, v = a_i\,,$$

das heißt die Blätter von T sind genau $V \setminus \{a_1, \ldots, a_{n-2}\}$.

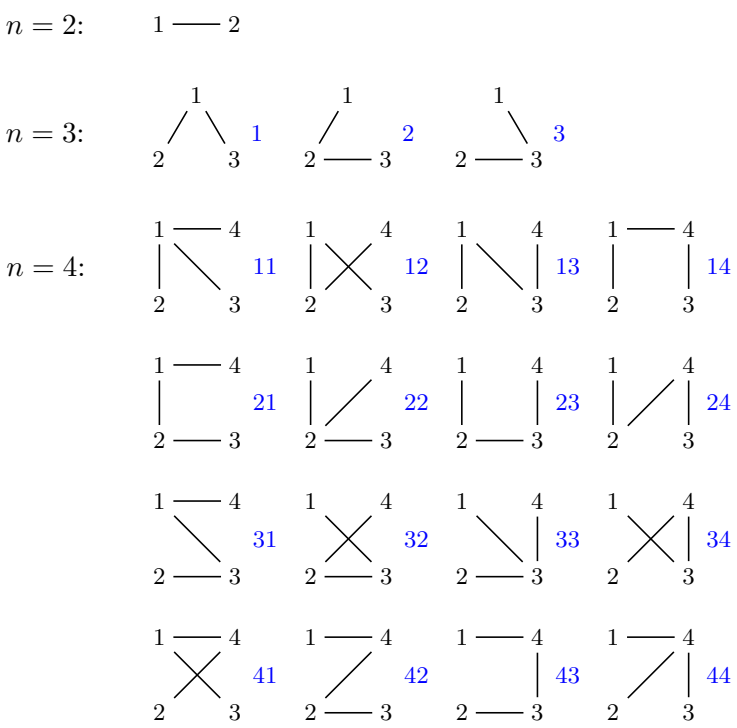


Abbildung 4: Markierte Bäume und ihre Prüfer-Codes

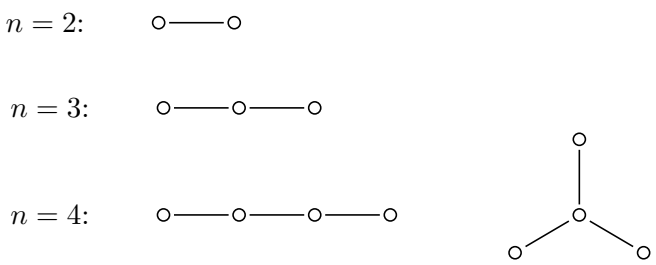


Abbildung 5: Isomorphieklassen von Bäumen

„⇐“. Ist $n > 2$ und $v \in V$ ein Blatt, sowie w der Nachbarknoten zu v, so ist w kein Blatt, also gilt $\deg(w) \geq 2$.

„⇒“. Beim Prüfer-Code werden schrittweise Kanten entfernt, bis nur eine übrig bleibt. Wegen $\deg(v) \geq 2$ wird also mindestens eine an v angrenzende Kante entfernt, und da v kein Blatt ist, wird dabei v notiert.

Nun zeigen wir, dass für alle Prüfer-Codes $\underline{a} = (a_1, \ldots, a_{n-2}) \in V^{n-2}$ genau ein Baum $T = (V, E)$ existiert mit $f(T) = \underline{a}$. Daraus folgt der Satz, denn $|V^{n-2}| = n^{n-2}$.

Wir verwenden vollständige Induktion über n, wobei $n \geq 2$. Bei $n = 2$ Knoten gibt es offenbar genau einen Baum. Nun sei $n \geq 3$ und $\underline{a} = (a_1, \ldots, a_{n-2}) \in V^{n-2}$ gegeben. Sei

$$b_1 := \min(V \setminus \{a_1, \ldots, a_{n-2}\})$$

und betrachte $\underline{a}' := (a_2, \ldots, a_{n-2}) \in (V \setminus \{b_1\})^{n-3}$. Nach Induktionsvoraussetzung mit $|V \setminus \{b_1\}| = n - 1$ existiert genau ein Baum $T' = (V \setminus \{b_1\}, E')$ mit $f(T') = \underline{a}'$, und nach der Hilfsbehauptung sind seine Blätter gerade $V \setminus \{b_1, a_2, \ldots, a_{n-2}\}$. Dann ist

$$T := (V, E' \cup \{\{a_1, b_1\}\})$$

ebenfalls ein Baum, und zwar mit Blättern $V \setminus \{a_1, \ldots, a_{n-2}\}$, also ist b_1 sein kleinstes Blatt. Daraus folgt $f(T) = \underline{a}$.

Sei nun $\tilde{T} = (V, \tilde{E})$ ein weiterer Baum mit $f(\tilde{T}) = \underline{a}$, so folgt wiederum mit der Hilfsbehauptung, dass b_1 das kleinste Blatt in $\tilde{T}$ ist, und mit

$$\tilde{T}' := (V \setminus \{b_1\},\, \tilde{E} \setminus \{\{a_1, b_1\}\})$$

ist $f(\tilde{T}') = \underline{a}'$, also gilt $\tilde{T}' = T'$ nach Induktionsvoraussetzung und somit $\tilde{T} = T$. □

Wir fassen die obige Rekonstruktion eines Baums aus einem Prüfer-Code zusammen. Sei ein Prüfer-Code $(a_1, \ldots, a_{n-2}) \in [n]^{n-2}$ gegeben, so definieren wir zunächst $(b_1, \ldots, b_{n-2}) \in [n]^{n-2}$ induktiv durch

$$b_i := \min([n] \setminus \{b_1, \ldots, b_{i-1}, a_i, \ldots, a_{n-2}\})$$

für $i = 1, \ldots, n-2$, sowie die Kante $e := [n] \setminus \{b_1, \ldots, b_{n-2}\}$; dann ist

$$T := \big([n],\, \{\{a_1, b_1\}, \ldots, \{a_{n-2}, b_{n-2}\}, e\}\big)$$

der zugehörige Baum mit $f(T) = (a_1, \ldots, a_{n-2})$.

6.2 Planare Graphen

Jene Graphen, die ein ebenes Diagramm ohne Kantenüberschneidungen besitzen, werden planar genannt. Wir werden zunächst diesen Begriff präzisieren. Ein (ebener) *Streckenzug* ist die Vereinigung von Verbindungsstrecken einer endlichen Folge von Punkten des $\mathbb{R}^2$. Der erste und der letzte Punkt in dieser Folge heißen die *Endpunkte* des Streckenzugs, und dessen *Inneres* ist der Streckenzug ohne die Endpunkte.

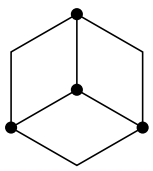
Definition 6.5. Ein *ebenes Diagramm* (V, E) besteht aus einer (nicht-leeren, endlichen) Menge $V \subset \mathbb{R}^2$ von *Knoten* und einer Menge E von Streckenzügen, den *Kanten*, wobei

1) die Kanten jeweils zwei Knoten miteinander verbinden,

2) je zwei Knoten durch höchstens eine Kante verbunden sind,

3) das Innere der Kanten keine Knoten und keine Punkte anderer Kanten enthält.

Ein ebenes Diagramm (V, E) definiert auf natürliche Weise einen Graphen $(V, \tilde{E})$ mit $\tilde{E} \subseteq \binom{V}{2}$, wobei jeder Streckenzug mit dessen Menge der Endpunkte identifiziert wird.



ein ebenes Diagramm des K_4

Definition 6.6. Ein Graph heißt *planar*, falls er ein ebenes Diagramm besitzt, d. h. falls er isomorph zum Graphen eines ebenen Diagramms ist.

Man kann zeigen, dass jeder planare Graph sogar ein ebenes Diagramm besitzt, dessen Kanten gerade Strecken sind (Satz von Wagner-Fáry).

Die Eulersche Polyederformel liefert eine grundlegende Aussage über die Anzahl der wie folgt definierten Flächen eines ebenen Diagramms. Für eine Menge $X \subseteq \mathbb{R}^2$ sei zunächst eine Äquivalenzrelation $R \subseteq X \times X$ definiert durch

$$(a, b) \in R \quad :\Leftrightarrow \quad \exists\,\text{Streckenzug in } X, \text{ der } a \text{ und } b \text{ verbindet.}$$

Die Äquivalenzklassen von R werden die *Gebiete* von X genannt.

Definition 6.7. Sei (V, E) ein ebenes Diagramm. Als dessen *Flächen* bezeichnet man die Gebiete der Menge $\mathbb{R}^2 \setminus \bigcup_{e \in E} e$.

Beispielsweise sind Bäume planar und jedes ebene Diagramm hat nur eine Fläche. Ein Kreisgraph $C_n := (\mathbb{Z}_n, \{\{i, i+1\} \mid i \in \mathbb{Z}_n\})$ mit n Knoten ist ebenfalls planar. Für einen elementaren Beweis der nachfolgenden Aussage siehe z. B. R. Courant, H. Robbins, *Was ist Mathematik?*, 5. Auflage, Springer, 2001.

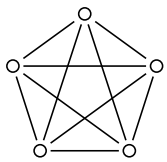
Lemma 6.5 (Jordanscher Kurvensatz für Polygone)**.** *Jedes ebene Diagramm von C_n hat genau zwei Flächen, deren gemeinsamer Rand die Vereinigung der Kanten ist.*

Satz 6.6 (Eulersche Polyederformel)**.** *Sei (V, E) ein zusammenhängendes ebenes Diagramm mit n Knoten, m Kanten und ℓ Flächen. Dann gilt*

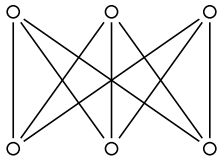
$$n - m + \ell \;=\; 2\,.$$

Beweis. Vollständige Induktion über die Zahl m der Kanten. Für $m = 0$ gibt es nur ein einen Knoten und eine Fläche, also gilt $1 - 0 + 1 = 2$. Sei nun ein zusammenhängendes ebenes Diagram mit $m \geq 1$ Kanten gegeben. Falls ein Kreis existiert, so entferne man eine beliebige Kante in diesem Kreis; da diese nach Lemma 6.5 an verschiedenen Flächen grenzt, wird dabei die Anzahl der Flächen ebenfalls um eins verringert und die Anzahl der Knoten bleibt gleich. Falls dagegen das Diagramm kreislos ist, so gibt es wegen Lemma 6.2 und des Zusammenhangs ein Blatt; entfernt man diesen Knoten und die zugehörige Kante, so ändert sich die Anzahl der Flächen nicht. In beiden Fällen schließen wir daher aus der Induktionsvoraussetzung die Behauptung. □

Der Satz von Kuratowski stellt eine genaue Charakterisierung der planaren Graphen dar. Der vollständige Graph K_5 und der vollständig bipartite Graph $K_{3,3}$ erweisen sich dabei als die „Prototypen“ nicht-planarer Graphen.



K_5



$K_{3,3}$

Lemma 6.7. *Die Graphen K_5 und $K_{3,3}$ sind nicht planar.*

Beweis. Betrachte ein ebenes Diagramm mit n Knoten, m Kanten und ℓ Flächen. Da jede Kante an höchstens zwei Flächen grenzt und jede Fläche mindestens drei Kanten hat, gilt

$$3\ell \;\leq\; 2m\,,$$

mit der Eulerschen Polyederformel also $2 = n - m + \ell \leq n - \frac{1}{3}m$. Der Graph K_5 hat jedoch $n = 5$ Knoten und $m = 10$ Kanten, also wäre $n - \frac{1}{3}m < 2$, ein Widerspruch.

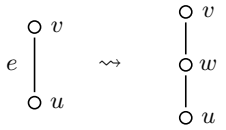
Im Fall des bipartiten Graphen $K_{3,3}$ hat jede Fläche sogar mindestens vier Kanten, und somit gilt

$$4\ell \leq 2m\,,$$

woraus $2 = n - m + \ell \leq n - \frac{1}{2}m$ folgt; dies führt mit $n = 6$ Knoten und $m = 9$ Kanten wegen $n - \frac{1}{2}m < 2$ ebenfalls zu einem Widerspruch. □

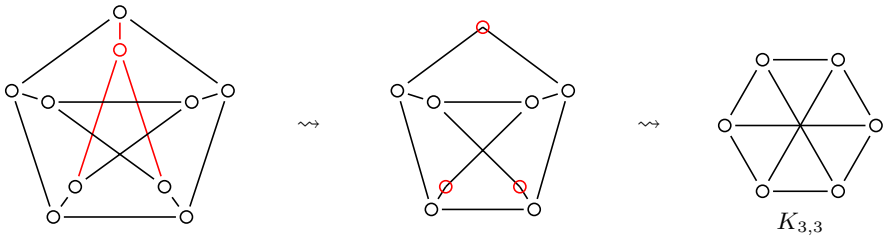
Sei $G = (V, E)$ ein Graph. Ein *Teilgraph* von G ist ein Graph $H = (W, F)$ mit $W \subseteq V$ und $F \subseteq E$ (also $F \subseteq \binom{W}{2} \cap E$). Das heißt, H entsteht aus G durch Entfernen von Kanten und/oder Knoten (wobei dann die angrenzenden Kanten auch entfernt werden).

Eine *Unterteilung* von G ist ein Graph, bei welchem schrittweise Kanten durch zwei inzidente Kanten ersetzt werden, d. h. ist $e = \{u, v\} \in E$ eine Kante, so sei in einem Schritt $\tilde{G} = (V \cup \{w\},\, E \setminus \{e\} \cup \{\{u, w\}, \{w, v\}\})$ mit neuem Knoten $w \notin V$.



Satz 6.8 (Kuratowski)**.** *Ein Graph ist genau dann planar, wenn er keine Unterteilung des K_5 oder des $K_{3,3}$ als Teilgraphen enthält.*

Aus Lemma 6.7 folgt leicht die notwendige Bedingung, also dass ein Graph nicht planar sein kann, wenn er als Teilgraph eine Unterteilung von K_5 oder $K_{3,3}$ enthält. Die hinreichende Bedingung ist schwieriger; wir können sie hier aus Zeitgründen nicht beweisen.



der Petersen-Graph ist nicht planar

Platonische Körper Wir betrachten nun planare Graphen $G = (V, E)$ mit $n = |V|$ Knoten, $m = |E|$ Kanten und ℓ Flächen derart, dass jede Fläche genau r Knoten hat und jeder Knoten Grad s besitzt. Durch Zählen von Inzidenzen erhalten wir somit

$$sn = 2m = r\ell\,,$$

woraus mit der Eulerschen Polyederformel $n - m + \ell = 2$ die Gleichung $n - \frac{s}{2}n + \frac{s}{r}n = 2$ resultiert. Es ergeben sich die folgenden Möglichkeiten:

r	s	n	m	ℓ	
3	3	4	6	4	Tetraeder
4	3	8	12	6	Hexaeder, Würfel
3	4	6	12	8	Oktaeder
5	3	20	30	12	Dodekaeder
3	5	12	30	20	Ikosaeder

Diese Graphen entsprechen gerade den fünf Platonischen Körpern, siehe Abb. 6. Beim Tetraeder, Würfel und Dodekaeder ist dabei jeweils eine Außenfläche gezeichnet, während beim Oktaeder und Ikosaeder jeweils ein „Außenpunkt“ dargestellt ist; durch Austauschen von Punkten und Flächen erhält man eine Dualität zwischen Würfel und Oktaeder, sowie zwischen Dodekaeder und Ikosaeder.

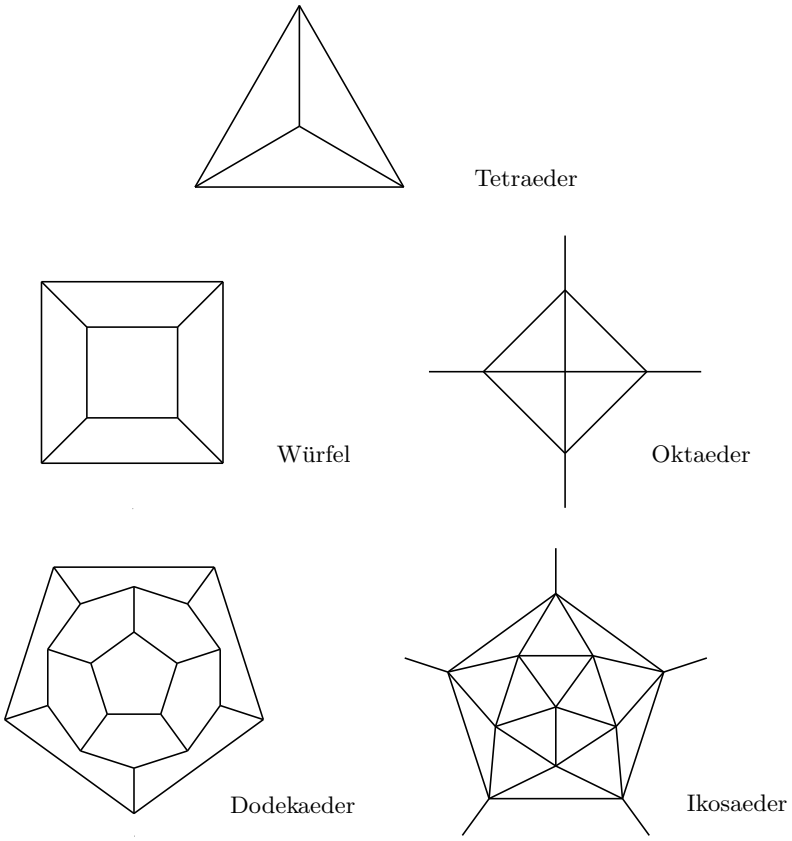
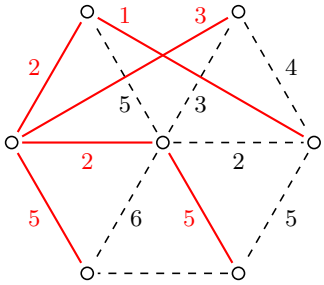


Abbildung 6: Die Platonischen Körper

6.3 Gewichtete Graphen

Ofmals lassen sich Situationen durch geeignete Graphen $G = (V, E)$ mit Kantengewichten $w\colon E \to \mathbb{R}_{\geq 0}$ modellieren, wobei die Gewichte beispielsweise Kosten oder Entfernungen ausdrücken können. Wir stellen zwei wichtige klassische Algorithmen für gewichtete Graphen vor, nämlich zur Berechnung eines minimalen Spannbaums und zur Bestimmung eines kürzesten Weges zwischen zwei Knoten.

Minimaler Spannbaum Sei $G = (V, E)$ ein zusammenhängender Graph. Unter einem *Spannbaum* (auch „Gerüst“) verstehen wir einen Baum (V, F) mit Kantenmenge $F \subseteq E$. Ein *minimaler Spannbaum* ist ein Spannbaum (V, F) derart, dass dessen Gesamtgewicht $\sum_{e \in F} w(e)$ minimal ist.



ein minimaler Spannbaum mit Gewicht 18

Wie wir sehen werden, konstruiert der folgende einfache „Greedy“-Algorithmus stets einen minimalen Spannbaum.

Algorithmus von Kruskal

$F_1 := \varnothing$

for $i := 1$ to $n-1$ do:

betrachte alle $e \in E \setminus F_i$ mit $F_i \cup \{e\}$ kreisfrei,
d. h. $e = \{v, w\}$ ohne Weg in F_i zwischen v und w

wähle davon e_i mit $w(e_i)$ minimal

$F_{i+1} := F_i \cup \{e_i\}$

Lemma 6.9 (Korrektheit)**.** *Im Kruskal-Algorithmus ist* (V, F_n) *minimaler Spannbaum.*

Beweis. Wir zeigen per Induktion, dass für alle $1 \leq i \leq n$ ein minimaler Spannbaum (V, F) mit $F_i \subseteq F$ existiert, woraus insbesondere $F_n = F$ folgt.

Der Fall $i = 1$ ist wegen $F_1 = \varnothing$ klar. Sei nun $1 \leq i \leq n-1$ und angenommen, dass es einen minimalen Spannbaum (V, F) mit $F_i \subseteq F$ gibt, so zeige die Behauptung für $i+1$. Im Fall $e_i \in F$ gilt $F_{i+1} \subseteq F$ und wir sind fertig. Andernfalls ist $e_i \notin F$, also gibt es einen Kreis in $F \cup \{e_i\}$. Wir wählen eine Kante $f \in F \setminus F_i$ in diesem Kreis, dann ist einerseits $F_i \cup \{f\}$ kreisfrei und somit nach dem Algorithmus $w(e_i) \leq w(f)$, und andererseits ist $F' := F \setminus \{f\} \cup \{e_i\}$ ebenfalls ein Spannbaum, welcher minimal ist und es gilt $F_{i+1} \subseteq F'$ wie gewünscht. □

Um den Aufwand des Kruskal-Algorithmus abschätzen zu können, sei $n := |V|$ die Anzahl Knoten und $m := |E|$ die Kantenzahl. Die algorithmischen Aufgaben sind:

1) die Kanten nach Gewicht sortieren: $O(m \log m)$,

2) jeweils entscheiden, ob $v, w \in V$ in der gleichen Zusammenhangskomponente liegen, d. h. ob ein Weg zwischen v und v existiert: dies ist mit sogenannten *union-find*-Strukturen “fast” linear in m möglich

Zusammen ergibt sich also eine Laufzeit von $O(m \log m)$. Neben dem Algorithmus von Kruskal existieren andere Algorithmen zum Auffinden minimaler Spannbäume, welche für bestimmte Graphen eine bessere Laufzeit haben.

Kürzeste Wege Für das Problem der kürzesten Wege ist es nun sinnvoll, Kanten mit einer Richtung zu versehen. Dabei kann ein (ungerichteter) Graph auch als ein gerichteter Graph aufgefasst werden, indem die ungerichteten Kanten durch jeweils zwei gerichtete Kanten ersetzt werden.

Ein *gerichteter Graph* $G = (V, E)$ besteht aus einer (nicht-leeren, endlichen) Menge V von Knoten, sowie einer Kantenmenge $E \subseteq V \times V$. Ein *Weg* von a nach b in G ist eine Folge $a = v_0, \ldots, v_s = b$ von Knoten mit $(v_i, v_{i+1}) \in E$ für alle $0 \leq i < s$.

Wie vorher betrachten wir nun Kantengewichte $w\colon E \to \mathbb{R}_{\geq 0}$. Das Gewichts eines Weges $P = (v_0, \ldots, v_s)$ ist dann definiert als die Summe $w(P) := \sum_{i=0}^{s-1} w((v_i, v_{i+1}))$. Zu Knoten $a, b \in V$ sei nun

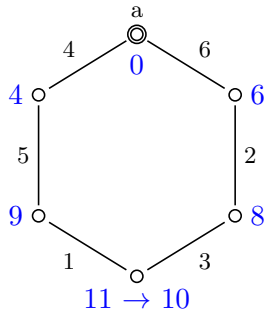
$$\operatorname{dist}(a, b) := \min\{w(P) \mid P \text{ Weg von } a \text{ nach } b\}$$

die *Distanz* von a zu b (wobei $\operatorname{dist}(a, b) := \infty$ falls kein Weg existiert).

Um die Distanzen und kürzesten Wege effizient zu berechnen, ist das folgende Verfahren sehr nützlich. Wir fixieren $a \in V$ und berechnen alle Distanzen $\operatorname{dist}(a, v)$ für $v \in V$.

Algorithmus von Dijkstra

$U_1 := \varnothing \qquad d(a) := 0$
für alle $v \in V \setminus \{a\}$ sei $d(v) := \infty$
for $i := 1$ to n do:
    wähle $u_i \in U_i$ mit $d(u_i)$ minimal
    $U_{i+1} := U_i \setminus \{u_i\}$
    für alle $e = (u_i, v) \in E$ mit $v \in U_{i+1}$
        setze $d(v) := \min(d(v),\, d(u_i) + w(e))$



Beispiel zum Dijkstra-Algorithmus

Lemma 6.10 (Korrektheit)**.** *Im Dijsktra-Algorithmus ist* $d(v) = \operatorname{dist}(a, v)$ *für alle* $v \in V$.

Beweis. Wir zeigen $d(u_i) = \operatorname{dist}(a, u_i)$ für alle $1 \leq i \leq n$ per Induktion. Der Fall $i = 1$, also $u_1 = a$ ist wegen $d(a) = 0 = \operatorname{dist}(a, a)$ klar. Betrachte nun $2 \leq i \leq n$. Entsprechend dem Algorithmus gibt es einen Weg von a nach u_i mit Gewicht $d(u_i)$, also gilt jedenfalls $\operatorname{dist}(a, u_i) \leq d(u_i)$.

Angenommen, es wäre $\operatorname{dist}(a, u_i) < d(u_i)$. Sei $P = (v_0, \ldots, v_s)$ ein kürzester Weg in G von a nach u_i, und sei j der maximale Index mit $v_j \in U_i^{\mathsf{c}} = \{u_1, \ldots, u_{i-1}\}$. Also gilt $d(v_j) = \operatorname{dist}(a, v_j)$ nach Induktionsvoraussetzung. Weiterhin ist $v_{j+1} \in U_i$, also wird die Kante $e = (v_j, v_{j+1})$ im Algorithmus betrachtet und es gilt

$$\begin{aligned} d(v_{j+1}) &\leq d(v_j) + w(e) = \operatorname{dist}(a, v_j) + w(e) \\ &= \operatorname{dist}(a, v_{j+1}) \leq \operatorname{dist}(a, u_i) < d(u_i)\,. \end{aligned}$$

Demnach wird v_{j+1} eher entfernt als u_i, was im Widerspruch zu $v_{j+1} \in U_i$ steht. □

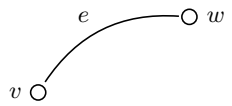
Der Dijkstra-Algorithmus hat offenbar eine Laufzeit von $O(n^2)$, wobei $n := |V|$ die Knotenanzhal ist. Für gewisse Graphen lässt sich diese Laufzeit wiederum verbessern.

Sind alle Distanzen $\mathrm{dist}(a, v) = d(v)$ bekannt, so findet man leicht einen kürzesten Weg P_{av} von a nach v via Rückwärtssuche. Denn für eine Kante $e = (u, v)$ mit $d(v) = d(u) + w(e)$ bildet ein kürzester Weg P_{au} nach u zusammen mit e einen kürzesten Weg P_{av}.

6.4 Wege in Multigraphen

Bei einem Multigraphen sind mehrere Kanten zwischen zwei Knoten möglich. Dabei wird jeder Kante die Menge ihrer Endpunkte zugeordnet, so dass also diverse Kanten die gleichen Endpunkte haben können.

Definition 6.8. Ein *Multigraph* $G = (V, E, \rho)$ besteht aus einer Knotenmenge V und einer Kantenmenge E, sowie einer Abbildung $\rho\colon E \to \binom{V}{2}$; jeder Kante $e \in E$ wird also eine zwei-elementige Knotenmenge $\rho(e) \in \binom{V}{2}$, die Menge ihrer Endpunkte, zugeordnet.



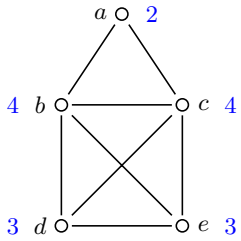
$\rho(e) = \{v, w\}$

Die Abbildung ρ ist genau dann injektiv, wenn zwischen je zwei Knoten höchstens eine Kante existiert. In diesem Fall kann die Kantenmenge E mit ihrem Bild $\rho(E) \subseteq \binom{V}{2}$ identifiziert werden und man erhält einen (einfachen) Graphen $(V, \rho(E))$.

Eulerwege Ein *Weg* in einem Multigraphen $G = (V, E, \rho)$ ist eine Folge $v_0, \ldots, v_s$ von Knoten mit $\{v_{i-1}, v_i\} \in \rho(E)$ für $1 \leq i \leq s$, d. h. es existiert jeweils eine Kante $e_i \in E$ mit Endpunkten $\rho(e_i) = \{v_{i-1}, v_i\}$. Im Folgenden wollen wir diejenigen Wege studieren, die dabei jede Kante genau einmal verwenden.

Definition 6.9. Ein *Eulerweg* ist ein Weg $v_0, \ldots, v_s$ in einem Multigraphen $G = (V, E, \rho)$, so dass jede Kante in E genau einmal durchlaufen wird; das heißt, es existiert eine Bijektion $e\colon [s] \to E$ mit $\{v_{i-1}, v_i\} = \rho(e(i))$ für alle $i \in [s] = \{1, \ldots, s\}$. Im Fall $v_s = v_0$ heißt ein solcher Weg *Eulerkreis*, ansonsten *offener* Eulerweg.

Beispiel 6.2. Beim „Haus vom Nikolaus“ ist der Weg $d, c, a, b, e, c, b, d, e$ ein Eulerweg.



Ob es zu einem gegebenen Multigraphen einen Eulerweg oder sogar einen Eulerkreis gibt, hängt tatsächlich nur von der Parität der Knotengrade ab. Der Grad eines Knotens $v \in V$ ist dabei wie vorher als Anzahl der angrenzenden Kanten definiert, also

$$\deg(v) := |\{e \in E \mid v \in \rho(e)\}|.$$

Satz 6.11 (Euler)**.** *Sei $G = (V, E, \rho)$ ein zusammenhängender Multigraph mit $n = |V|$ Knoten. Dann existiert ein Eulerkreis (bzw. ein offener Eulerweg) in G genau dann, wenn $|\{v \mid \deg(v)$ gerade$\}| = n$ (bzw. $n - 2$ ist).*

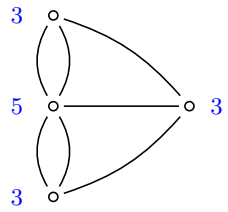
Beweis. „⇒“. Sei $v_0, \dots, v_s$ ein Eulerweg mit zugehöriger Bijektion $e\colon [s] \to E$. Bei den inneren Knoten v_i mit $1 \leq i < s$ werden jeweils die eingehende Kante $e(i)$ mit $\rho(e(i)) = \{v_{i-1}, v_i\}$ und die ausgehende Kante $e(i{+}1)$ mit $\rho(e(i{+}1)) = \{v_i, v_{i+1}\}$ gezählt. Außerdem wird beim Startknoten v_0 die Kante $e(1)$ mit $\rho(e(1)) = \{v_0, v_1\}$ und beim Endknoten v_s die Kante $e(s)$ mit $\rho(e(s)) = \{v_{s-1}, v_s\}$ gezählt. Daher sind im Fall $v_0 = v_s$ alle Knotengrade gerade und im Fall $v_0 \neq v_s$ genau die Knotengrade für $v \in V \setminus \{v_0, v_s\}$ gerade.

„⇐“. Wir zeigen, dass ein Eulerkreis existiert, falls alle Knotengrade $\deg(v)$ gerade sind. Betrachte hierfür einen maximalen Weg $v_0, \dots, v_s$ in G mit verschiedenen Kanten, d. h. es gibt eine Injektion $e\colon [s] \to E$ mit $\{v_{i-1}, v_i\} = \rho(e(i))$. Wäre $v_s \neq v_0$, so würden an beiden Enden eine ungerade Anzahl angrenzender Kanten verwendet (vgl. „⇒“), also bliebe, weil $\deg(v_0)$ und $\deg(v_s)$ gerade sind, an beiden Enden eine Kante übrig und der Weg könnte verlängert werden.

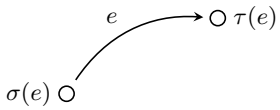
Also gilt $v_s = v_0$. Angenommen, es würden nicht alle Kanten verwendet, d. h. die Abbildung e wäre nicht surjektiv. Dann gibt es wegen des Zusammenhangs von G eine Kante $f \in E \setminus \mathrm{im}(e)$, die den Weg angrenzt, also mit Endpunkten $\rho(f) = \{v_i, w\}$ für ein $0 \leq i \leq s$. Indem wir von w starten, konstruieren wir so einen verlängerten Weg $w, v_i, \dots, v_s = v_0, \dots, v_i$ – Widerspruch! Also ist die Abbildung e bijektiv und der Weg ist ein Eulerkreis.

Ist der Grad gerade für alle Knoten bis auf genau zwei, also $\{v \in V \mid \deg(v) \text{ gerade}\} = V \setminus \{v, w\}$ für $\{v, w\} \in \binom{V}{2}$, dann füge eine Kante e mit Endpunkten $\rho(e) = \{v, w\}$ hinzu, so dass alle Knotengrade gerade sind. Wir haben dann bereits gezeigt, dass ein Eulerkreis existiert und dieser ergibt ohne die Kante e einen offenen Eulerweg von v nach w. □

Beispiel 6.3. Für den Graphen des „Königsberger Brückenproblems“ kann es nach diesem Satz also keinen Eulerweg geben.



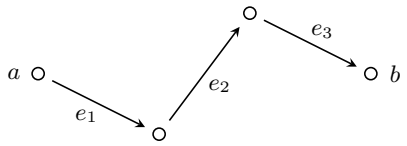
Adjazenzmatrix und Anzahl Kantenzüge Ein *gerichteter Multigraph* (auch „Netzwerk“) $G = (V, E, \rho)$ besteht aus Knoten V, Kanten E und einer Abbildung $\rho\colon E \to V \times V$, das heißt, jeder Kante $e \in E$ wird ein Knotenpaar $\rho(e) =: (\sigma(e), \tau(e)) \in V \times V$ zugeordnet, wobei $\sigma(e)$ der Startknoten und $\tau(e)$ der Zielknoten der Kante e sei.



Analog wie vorher ist die Abbildung ρ genau dann injektiv, wenn für jedes Knotenpaar (v, w) höchstens eine Kante von v nach w existiert. In diesem Fall kann die Kantenmenge E mit ihrem Bild $\rho(E) \subseteq V \times V$ identifiziert werden und man erhält einen (einfachen) gerichteten Graphen $(V, \rho(E))$.

In einem gerichteten Multigraphen $G = (V, E, \rho)$ ist ein *Weg* wie üblich als eine Knotenfolge $v_0, \dots, v_s$ mit $(v_{i-1}, v_i) \in \rho(E)$ definiert, d. h. es gibt jeweils eine Kante $e_i \in E$ mit $\rho(e_i) = (v_{i-1}, v_i)$, für alle $1 \leq i \leq s$. Um die Wahl der Verbindungskanten eines Wegs

zu spezifizieren, definieren wir nun einen *Kantenzug* (von $a \in V$ nach $b \in V$ der Länge $s \in \mathbb{N}_{>0}$) als eine Folge von Kanten $e_1, \ldots, e_s$ derart, dass $\sigma(e_1) = a$, $\tau(e_s) = b$ und $\tau(e_i) = \sigma(e_{i+1})$ für $1 \leq i < s$ gilt.



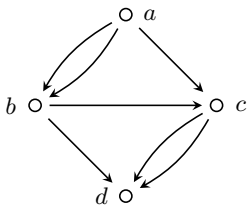
Die Anzahl der Kantenzüge hängt mit der wie folgt definierten Adjazenzmatrix eines gerichteten Multigraphen zusammen.

Definition 6.10. Zu einem Netzwerk $G = (V, E, \rho)$ sei die *Adjazenzmatrix* definiert durch

$$A \colon V \times V \to \mathbb{N}\,, \quad (v, w) \mapsto |\{e \in E \mid \rho(e) = (v, w)\}|\,,$$

d. h. der Eintrag $A(v, w)$ gibt die Anzahl der Kanten von v nach w in G an.

Beispiel 6.4. Betrachte das folgende Netzwerk mit $V = \{a, b, c, d\}$.



Für die Adjazenzmatrix A, sowie deren Matrixprodukt $A \cdot A$ erhalten wir

$$A = \begin{pmatrix} 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{und} \quad A^2 = \begin{pmatrix} 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Wir können Matrix-Potenzen induktiv definieren durch $A^0 := I$ (Einheitsmatrix), sowie $A^{i+1} := A^i \cdot A$ für $i \geq 0$. Die Einträge der Potenzen einer Adjazenzmatrix haben folgende interessante Interpretation.

Proposition 6.12. *Sei $A \colon V \times V \to \mathbb{N}$ die Adjazenzmatrix eines gerichteten Multigraphen $G = (V, E, \rho)$. Dann liefert der Eintrag $A^s(v, w)$ die Anzahl der Kantenzüge von v nach w der Länge s.*

Beweis. Wir zeigen die Behauptung per vollständiger Induktion über s. Im Fall $s = 1$ gibt $A(v, w)$ die Anzahl der Kanten von v nach w an, also die Anzahl der Kantenzüge der Länge 1. Um nun von s auf $s+1$ zu schließen, betrachte

$$A^{s+1}(v, w) \;=\; (A^s \cdot A)(v, w) \;=\; \sum_{u \in V} A^s(v, u) \cdot A(v, w)\,,$$

wobei nach Induktionsvoraussetzung $A^s(v, u)$ die Anzahl der Kantenzüge von v nach u der Länge s ist. Da über alle möglichen vorletzten Knoten $u \in V$ eines Kantenzugs summiert wird, ist diese Summe die Anzahl aller Kantenzüge von v nach w der Länge $s+1$. □

6.5 Flüsse in Transportnetzen

Wir betrachten schließlich gerichtete Graphen mit Kantengewichten, die wir als Kapazitäten interpretieren, und konstruieren hierfür einen maximalen Fluss. Zahlreiche graphentheoretische und kombinatorische Probleme lassen sich auf ein solches Problem des maximalen Flusses zurückführen.

Sei (V, E) ein gerichteter Graph, also mit Kanten $E \subseteq V \times V$. Falls $e = (v, w) \in E$ eine Kante ist, so heißt der Knoten v ein Vorgänger vom Knoten w bzw. der Knoten w ein Nachfolger vom Knoten v. Einen Knoten ohne jegliche Vorgänger nennt man „Quelle“, einen Knoten ohne Nachfolger „Senke“.

Definition 6.11. Ein *Transportnetz* $(V, E, q, s, \mathrm{wt})$ ist ein gerichteter Graph (V, E) mit Quelle q, Senke s (wobei $q \neq s$) und „Kapazitäten“ $\mathrm{wt}\colon E \to \mathbb{R}_{\geq 0}$.

Ein *Fluss* in diesem Transportnetz ist eine Kantenbewertung $f\colon E \to \mathbb{R}_{\geq 0}$ derart, dass für alle Knoten $v \in V \setminus \{q, s\}$ die Flussbedingung

$$\sum_{w,\,(w,v)\in E} f(w, v) \;=\; \sum_{w,\,(v,w)\in E} f(v, w)$$

erfüllt ist („was in v hinein fließt, fließt auch heraus“). Der Fluss f heißt *zulässig*, falls $f(e) \leq \mathrm{wt}(e)$ für alle $e \in E$ gilt.

Ist $T \subseteq V \setminus \{q, s\}$ eine Knotenmenge und f ein Fluss, so folgt

$$\sum_{(w,v)\in E\cap V\times T} f(w, v) \;=\; \sum_{(v,w)\in E\cap T\times V} f(v, w)\,.$$

Durch Subtraktion über alle Kanten in $T\times T$ ergibt sich daraus $\sum_{(w,v)\in E\cap T^{\mathrm{c}}\times T} f(w, v) = \sum_{(v,w)\in E\cap T\times T^{\mathrm{c}}} f(v, w)$. Für die größtmögliche Menge $T = V \setminus \{q, s\}$ folgt insbesondere

$$\sum_{v,\,(q,v)\in E} f(q, v) \;=\; \sum_{v,\,(v,s)\in E} f(v, s)$$

(„was aus q heraus fließt, fließt in s hinein“), und man bezeichnet $|f| := \sum_{(q,v)\in E} f(q, v) = \sum_{(v,s)\in E} f(v, s)$ als die *Stärke* des Flusses.

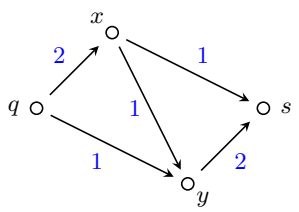
Eine Zerlegung des Transportnetzes in zwei Teile, welche die Quelle und die Senke voneinander trennen, bezeichnet man als Schnitt. Jeder zulässige Fluss kann durch den wie folgt definierten Wert eines Schnitts abgeschätzt werden.

Definition 6.12. Sei $(V, E, q, s, \mathrm{wt})$ ein Transportnetz. Ein *Schnitt* $\mathcal{C} = (Q, S)$ ist eine Zerlegung der Knotenmenge $V = Q \mathbin{\dot\cup} S$ mit $q \in Q$ und $s \in S$. Der *Wert* von $\mathcal{C}$ ist

$$|\mathcal{C}| \;:=\; \sum_{(v,w)\in E\cap Q\times S} \mathrm{wt}(v, w)\,,$$

wobei wir also über die Menge $E \cap Q \times S$ der „Schnittkanten“ summieren.

Beispiel 6.5. Betrachte das Transportnetz $(V, E, q, s, \mathrm{wt})$ mit $V = \{q, x, y, s\}$ und $E = \{(q, x), (q, y), (x, y), (x, s), (y, s)\}$, sowie folgenden Kapazitäten:



Für den Schnitt $\mathcal{C}_1 = (\{q, x\}, \{y, s\})$ sind die Schnittkanten $\{(q, y), (x, y), (x, s)\}$, also ist der Wert $|\mathcal{C}_1| = 3$. Für $\mathcal{C}_2 = (\{q, y\}, \{x, s\})$ mit den Schnittkanten $\{(q, x), (y, s)\}$ ergibt sich dagegen der Wert $|\mathcal{C}_2| = 4$.

Lemma 6.13. *Für jeden zulässigen Fluss f und jeden Schnitt $\mathcal{C}$ gilt $|f| \leq |\mathcal{C}|$.*

Beweis. Sei f ein zulässiger Fluss und $\mathcal{C} = (Q, S)$ ein Schnitt. Unter Benutzung der Flussbedingung erhalten wir für die Stärke

$$|f| = \sum_{(v,w) \in E \cap Q \times V} f(v, w) - \sum_{(w,v) \in E \cap V \times Q} f(w, v) = \sum_{(v,w) \in E \cap Q \times S} f(v, w) - \sum_{(w,v) \in E \cap S \times Q} f(w, v)$$

(„was von Q nach S fließt minus was zurück fließt“). Wegen $0 \leq f(e) \leq \mathrm{wt}(e)$ für alle $e \in E$ ergibt sich somit $|f| \leq \sum_{(v,w) \in E \cap Q \times S} \mathrm{wt}(v, w) = |\mathcal{C}|$. □

Dieses Lemma ist eine wichtige Vorbereitung für unser Hauptresultat über Flüsse in Transportnetzen, welches wir konstruktiv durch Angabe eines Algorithmus beweisen.

Satz 6.14 (Max-Flow-Min-Cut)**.** *Sei $(V, E, q, s, \mathrm{wt})$ ein Transportnetz. Die maximale Stärke eines zulässigen Flusses ist gleich dem minimalen Wert eines Schnitts, also*

$$\max_{f \text{ zul. Fluss}} |f| = \min_{\mathcal{C} \text{ Schnitt}} |\mathcal{C}| .$$

Beweis. Die Abschätzung „$\leq$“ folgt unmittelbar aus Lemma 6.13.

Um „$\geq$“ zu zeigen, finden wir einen zulässigen Fluss f und einen Schnitt $\mathcal{C}$ mit $|f| = |\mathcal{C}|$ mittels folgendem Verfahren.

Algorithmus von Ford und Fulkerson

---

start: leerer Fluss $f(e) := 0$ für alle $e \in E$

augmentiere: betrachte zu einem Fluss f den „Residualgraphen“ $G_f := (V, E_f)$
mit $E_f := E_1 \cup E_2$, wobei $E_1 := \{e \in E \mid f(e) < \mathrm{wt}(e)\}$ (nicht ausgelastete Kanten)
und $E_2 := \{(w, v) \mid (v, w) \in E \wedge f(w, v) > 0\}$ (Rückwärtskanten).

falls ein Weg $v_0, \ldots, v_t$ von q nach s in G_f existiert:

sei $e_i := (v_{i-1}, v_i) \in E_f$ und setze $c_i := \mathrm{wt}(e_i) - f(e_i)$ für $e_i \in E_1$,
sowie $c_i := f(v_i, v_{i-1})$ sonst

mit $c := \min_i c_i > 0$ setze dann $\tilde{f}(e_i) := f(e_i) + c$ für $e_i \in E_1$,
sowie $\tilde{f}(v_i, v_{i-1}) := f(v_i, v_{i-1}) - c$ sonst

augmentiere erneut mit $f := \tilde{f}$

sonst stop

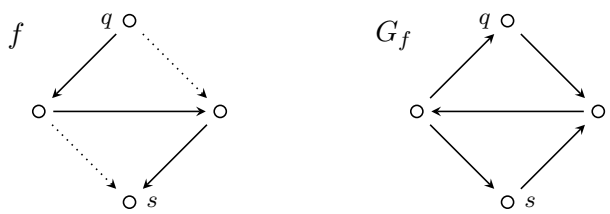


Abbildung 7: Beispiel zum Ford-Fulkerson-Algorithmus

Nach Beendigung des Algorithmus definieren wir einen Schnitt $\mathcal{C} = (Q, S)$ durch

$$Q := \{v \in V \mid \exists \text{ Weg von } q \text{ nach } v \text{ in } G_f\}$$

und $S := Q^{\mathsf{c}}$. Dann ist $q \in Q$, und nach der Abbruchbedingung existiert kein Weg von q nach s, also gilt $s \in S$ und (Q, S) ist ein Schnitt.

Für die Kanten $(v, w) \in E$ gilt nach der Definition von G_f dann $f(v, w) = \mathrm{wt}(v, w)$ falls $(v, w) \in Q \times S$, sowie $f(v, w) = 0$ falls $(w, v) \in Q \times S$. Daher folgt

$$|f| = \sum_{(v,w) \in E \cap Q \times S} f(v, w) - \sum_{(w,v) \in E \cap S \times Q} f(w, v) = \sum_{(v,w) \in E \cap Q \times S} \mathrm{wt}(v, w) = |\mathcal{C}|\,,$$

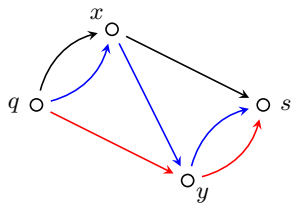
wie gewünscht. □

Gerichtete Multigraphen können als Transportnetze mit ganzzahligen Kapazitäten aufgefasst werden. Sei nämlich $G = (V, E, \rho)$ ein gerichteter Multigraph, wobei die Abbildung $\rho\colon E \to V \times V$ jeder Kante ihren Start- und Zielknoten zuordnet, sowie $q \in V$ eine Quelle und $s \in V$ eine Senke. Dadurch wird ein gerichteter Graph $(V, \tilde{E})$ mit $\tilde{E} := \rho(E) \subseteq V \times V$ definiert und für jede Kante $(v, w) \in \tilde{E}$ hat man eine „Kapazität“

$$\mathrm{wt}(v, w) \;:=\; \big|\{e \in E \mid \rho(e) = (v, w)\}\big|\,,$$

welche die Anzahl der Kanten in E von v nach w angibt.

Ist dann $f\colon \tilde{E} \to \mathbb{N}$ ein Fluss der Stärke r, so kann man leicht zeigen, dass es r kantendisjunkte Wege von q nach s gibt. Aus Satz 6.14 resultiert dann direkt der folgende Satz von Menger: Die maximale Anzahl kantendisjunkter Wege ist gerade gleich dem minimalen Wert eines Schnitts (Anzahl der Schnittkanten).



drei kantendisjunkte Wege

7 Geordnete Mengen

Ordnung ist das halbe Leben – woraus mag die andere Hälfte bestehen?

— Heinrich Böll

Neben den Äquivalenzrelationen stellen die Ordnungen die wichtigste Art von binären Relationen dar. Ordnungsrelationen sind nicht nur in der Mathematik allgegenwärtig, sondern begegnen einem häufig in der Informatik, etwa bei der Implementierung effizienter Such- und Sortierverfahren. Wir beginnen hier mit einem Beispiel aus dem „echten Leben“, welches dem Lehrbuch von B. Ganter, *Diskrete Mathematik: Geordnete Mengen*, Springer, 2013, entnommen ist.

Beispiel 7.1 (Ein Spiegelei zubereiten)**.** Betrachte eine Menge X von Arbeitsschritten:

HE Herd einschalten	EA Ei aufschlagen
PH Pfanne auf den Herd	EP Ei in die Pfanne
PE Pfanne heiß werden lassen	EB Ei braten
FP Fett in die Pfanne	ET Ei auf den Teller
FZ Fett zerlassen	ES Ei salzen

Wir können eine Reihe von Vorgänger-Bedingungen („precedence constraints“) formulieren, die für eine sinnvolle Reihenfolge von Arbeitsschritten zu berücksichtigen sind:

$$(\mathrm{HE},\mathrm{PE}),\ (\mathrm{PH},\mathrm{PE}),\ (\mathrm{PE},\mathrm{FZ}),\ (\mathrm{FP},\mathrm{FZ}),\ (\mathrm{FZ},\mathrm{EP}),$$
$$(\mathrm{EA},\mathrm{EP}),\ (\mathrm{EA},\mathrm{ES}),\ (\mathrm{EP},\mathrm{EB}),\ (\mathrm{EB},\mathrm{ET})\,.$$

Eine Vorgänger-Bedingung ist dabei ein geordnetes Paar $(a,b) \in X \times X$, mit der Interpretation, dass Schritt a vor Schritt b auszuführen sei. Die Menge dieser Bedingungen definiert somit eine Relation $R \subseteq X \times X$ auf X.

Nun lassen sich weitere Bedingungen aus den gegebenen herleiten, etwa $(\mathrm{HE},\mathrm{FZ})$ und $(\mathrm{PH},\mathrm{FZ})$. Dabei bilden wir den sogenannten transitiven Abschluss der Relation R.

Definition 7.1. Sei X eine Menge und $R \subseteq X \times X$ eine Relation auf X. Als *transitive Hülle* $\mathrm{trans}(R)$ von R bezeichnet man die Relation aller Paare $(a,b) \in X \times X$ für die eine Folge $x_0, \ldots, x_s \in X$ mit $x_0 = a$, $x_s = b$, sowie $(x_{i-1}, x_i) \in R$ für alle $1 \leq i \leq s$ existiert.

Graphentheoretisch bedeutet dies Folgendes. Ist R eine Relation auf X, so ist $G := (X,R)$ ein gerichteter Graph (wobei die Knotenmenge X ggfs. unendlich ist), und

$$\mathrm{trans}(R) \;=\; \{(a,b) \in X \times X \mid \exists \text{ Weg in } G \text{ von } a \text{ nach } b\}\,.$$

Es ist nützlich, ein Produkt von Relationen, in Analogie zur Verknüpfung von Abbildungen, wie folgt zu definieren. Seien $R, S \subseteq X \times X$ Relationen, dann bezeichne

$$R \circ S \;:=\; \{(a,c) \in X \times X \mid \exists b \in X : (a,b) \in R \wedge (b,c) \in S\}$$

das „Relationenprodukt“ von R und S. Somit ist eine Relation $R \subseteq X \times X$ transitiv, d. h. aus $(a,b) \in R$ und $(b,c) \in R$ folgt $(a,c) \in R$, genau dann, wenn $R \circ R \subseteq R$ gilt.

Bemerkung 7.1. *Die transitive Hülle* $\mathrm{trans}(R)$ *ist die kleinste transitive Relation, die* R *enthält. In der Tat gilt*

$$\mathrm{trans}(R) \;=\; \bigcup_{i \geq 1} R^i\,,$$

wobei $R^1 := R$ *und induktiv* $R^{i+1} := R^i \circ R$ *für* $i \in \mathbb{N}$ *sei.*

Eine effiziente Berechnung der transitiven Hülle $\text{trans}(R)$ einer Relation R ist indes für endliche Mengen X in $O(n^3)$ Schritten möglich, wobei $n = |X|$. Hierfür kann der Floyd-Warshall-Algorithmus verwendet werden.

Mitunter kann eine Menge von Vorgänger-Bedingungen zu zyklischen Abhängigkeiten führen, so dass eine gültige Ablaufplanung unmöglich ist. Wir beschränken uns daher auf solche Relationen, bei denen dieses Phänomen ausgeschlossen wird.

Definition 7.2. Eine Relation $R \subseteq X \times X$ auf X heißt *azyklisch*, falls $\text{trans}(R) \cap \Delta_X = \varnothing$ gilt, wobei $\Delta_X := \{(x, x) \mid x \in X\}$ die „Diagonale“ von X sei.

Die graphentheoretische Interpretation lautet, dass in G keine gerichteten Kreise, d. h. Wege $v_0, \ldots, v_s = v_0$ mit $s \geq 1$, existieren dürfen. Derartige Graphen sind auch als „directed acyclic graphs“ (DAG) bekannt.

7.1 Ordnungen

Eine Relation $R \subseteq X \times X$ auf einer Menge X wird *irreflexiv* genannt, falls $R \cap \Delta_X = \varnothing$ ist, d. h. falls $(x, x) \notin R$ für alle $x \in X$ gilt. Eine irreflexive, transitive Relation $R \subseteq X \times X$ bezeichnet man als *strikte Ordnung* auf X. Für jede azyklische Relation R ist also die transitive Hülle $\text{trans}(R)$ eine strikte Ordnung.

Für eine strikte Ordnung R kann es offenbar keine Elemente $a, b \in X$ mit $(a, b) \in R$ und $(b, a) \in R$ geben (denn sonst folgte $(a, a) \in R$ aus der Transitivität). Der zentrale Begriff der Ordnungsrelation (kurz Ordnung) ergibt sich nun aus den strikten Ordnungsrelationen, indem man die Diagonale hinzufügt, so dass die Relation reflexiv und *anti-symmetrisch* wird, d. h. $(a, b) \in R$ und $(b, a) \in R$ implizieren $a = b$.

Definition 7.3. Sei X eine Menge. Eine reflexive, anti-symmetrische, transitive Relation $R \subseteq X \times X$ heißt *Ordnung* auf X und (X, R) heißt dann *geordnete Menge*. Eine Ordnungsrelation R erfüllt also drei Eigenschaften:

1) R ist „reflexiv“, d. h. $\forall x \in X : (x, x) \in R$,

2) R ist „anti-symmetrisch“, d. h. $\forall x, y \in X : (x, y) \in R \ \wedge \ (y, x) \in R \ \Rightarrow \ x = y$,

3) R ist „transitiv“, d. h. $\forall x, y, z \in X : (x, y) \in R \ \wedge \ (y, z) \in R \ \Rightarrow \ (x, z) \in R$.

Für diesen Begriff wird auch manchmal die Bezeichnung „partielle Ordnung“ verwendet, um den Unterschied zu den linearen Ordnungen (siehe unten) zu betonen.

Bemerkung 7.2. *Ist R eine strikte Ordnung auf X, so ist $R \cup \Delta_X$ eine Ordnung. Ist umgekehrt R eine Ordnung auf X, so definiert $R \setminus \Delta_X$ eine strikte Ordnung.*

Für Ordnungen gilt das wichtige Dualitätsprinzip: Wenn R eine Ordnung ist, so ist $R^{-1} := \{(y, x) \mid (x, y) \in R\}$ ebenfalls eine Ordnung. So lassen sich etwa Aussagen über größte oder maximale Elemente in solche über kleinste/minimale Elemente überführen.

Wie bei den Äquivalenzrelationen wird für Ordnungen oft die Infix-Notation $a \, R \, b$ für $(a, b) \in R$ verwendet. Dies gilt insbesondere, wenn für R das übliche Symbol $\leq$ benutzt wird. Ist also $(X, \leq)$ eine geordnete Menge, so wird durch

$$a < b \quad :\Leftrightarrow \quad a \leq b \ \wedge \ a \neq b$$

eine strikte Ordnung $<$ definiert, sowie durch $a \geq b \ :\Leftrightarrow \ b \leq a$ die duale Ordnung $\geq$.

Beispiel 7.2. Wir sind bereits einigen Ordnungen in der Mathematik begegnet.

1) Sei $X \subseteq \mathbb{R}$ und sei $\leq$ die übliche Ordnung der reellen Zahlen, dann ist $(X, \leq)$ eine geordnete Menge.

2) Sei Y eine Menge und $X = \mathcal{P}(Y)$ die Potenzmenge von Y, sowie $\subseteq$ die Teilmengen-Relation. Dann ist auch $(X, \subseteq)$ eine geordnete Menge.

3) Auf der Menge $X = \mathbb{N}$ der natürlichen Zahlen ist die Teilbarkeitsrelation $|$, wobei $a \mid b \ :\Leftrightarrow\ \exists x \in \mathbb{N} : \ b = ax$, ebenfalls eine Ordnung.

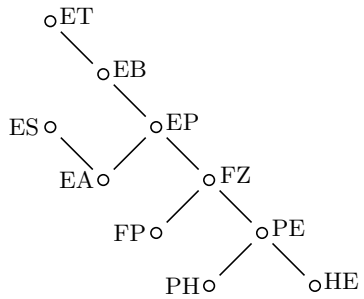
Diagramme Ordnungsrelationen auf endlichen Mengen X lassen sich übersichtlich graphisch darstellen. Wir brauchen dabei nur die „benachbarten" Elemente zu betrachten.

Definition 7.4. Sei $(X, \leq)$ eine geordnete Menge. Definiere die *Nachbarschaftsrelation* $\lessdot$ auf X durch $a \lessdot b$, falls $a < b$ gilt und es kein $c \in X$ mit $a < c < b$ gibt.

Bemerkung 7.3. *Ist X endlich, so gilt $\leq \ = \ \mathrm{trans}(\lessdot) \cup \Delta_X$, somit ist die Nachbarschaftsrelation $\lessdot$ die kleinste Relation aus der $\leq$ rekonstruiert werden kann.*

Diese Aussage kann für unendliche Mengen X falsch sein, denn für $(\mathbb{R}, \leq)$ beispielsweise ist $\lessdot \ = \ \varnothing$.

Unter einem *Ordnungsdiagramm* einer Ordnung $\leq$ auf einer endlichen Menge X verstehen wir nun eine Darstellung des Graphens $(X, \lessdot)$, wobei die gerichteten Kanten nach oben führen (und man somit die Richtungspfeile weglassen kann). Für die Spiegelei-Ordnung aus Beispiel 7.1 hat das Diagramm die Form:



Grundbegriffe Nachfolgend stellen wir die wichtigsten Grundbegriffe für den Umgang mit Ordnungen zusammen. Sei $(X, \leq)$ eine geordnete Menge.

Definition 7.5. Zwei Elemente $a, b \in X$ heißen *vergleichbar*, falls $a \leq b$ oder $b \leq a$ gilt, ansonsten *unvergleichbar*. Sind alle $a, b \in X$ vergleichbar, so heißt $\leq$ eine *lineare* (oder *totale*) Ordnung. Eine Teilmenge $Y \subseteq X$ heißt *Kette*, falls alle $a, b \in Y$ vergleichbar sind, falls also $(Y, \leq_Y)$ (wobei $\leq_Y := \leq \cap\, Y \times Y$) eine linear geordnete Menge ist.

Definition 7.6. Ein Element $a \in X$ heißt

- *maximal*, falls kein $x \in X$ mit $x > a$ existiert,
- *größtes* Element, falls $x \leq a$ für alle $x \in X$,
- *obere Schranke* einer Teilmenge $Y \subseteq X$, falls $y \leq a$ für alle $y \in Y$.

Entsprechend sind die Begriffe *minimal*, *kleinstes* Element und *untere Schrnake* durch Betrachtung der Dualordnung $\geq$ definiert.

Beispiel 7.3. In der Spiegelei-Ordnung von Beispiel 7.1 sind beispielsweise EB und FP vergleichbar, denn FP $\leq$ EB. Andererseits sind ES und PE unvergleichbar, also ist die Ordnung nicht linear. Ein Beispiel für eine Kette ist die Teilmenge $\{\mathrm{PH}, \mathrm{PE}, \mathrm{EP}\}$.

Die maximalen Elemente sind ET und ES, während die minimalen Elemente HE, PH, FP und EA sind. Die Ordnung hat jedoch weder größte noch kleinste Elemente. Für die Teilmenge $\{\mathrm{EA}, \mathrm{FZ}\}$ beispielsweise sind EP, EB und ET obere Schranken, aber es gibt keine untere Schranke.

Die Begriffe Äquivalenzrelation und Ordnung sind von komplementärer Natur (Übung: Welche Relationen $R \subseteq X \times X$ sind gleichzeitig Äquivalenzrelation und Ordnung auf X?). Die Quasiordnungen stellen eine Verallgemeinerung dar, die beide Begriffe umfasst.

Definition 7.7. Sei X eine Menge. Eine reflexive, transitive Relation $R \subseteq X \times X$ nennt man *Quasiordnung* auf X.

Jede Quasiordnung induziert eine Ordnung auf einer Menge von Äquivalenzklassen. Ist nämlich $R \subseteq X \times X$ eine Quasiordnung auf einer Menge X, so wird durch

$$x \sim y \quad :\Leftrightarrow \quad x\,R\,y \ \wedge \ y\,R\,x$$

eine Äquivalenzrelation definiert. Dann ist auf der Menge $X/\!\sim$ der Äquivalenzklassen eine Relation durch

$$[x] \leq [y] \quad :\Leftrightarrow \quad x\,R\,y$$

definiert; diese Vorschrift ist wohldefiniert, also unabhängig von der Repräsentantenwahl, und ergibt eine Ordnungsrelation. Es ist also $(X/\!\sim, \leq)$ eine geordnete Menge.

Beispiel 7.4. Betrachte auf der Menge $X := \mathbb{Z}$ der ganzen Zahlen die Teilbarkeitsrelation $a \mid b \ :\Leftrightarrow \ \exists x \in \mathbb{Z} : \, b = ax$. Die Relation „$\mid$“ ist eine Quasiordnung und es gilt

$$a \sim b \quad \Leftrightarrow \quad a \mid b \ \wedge \ b \mid a \quad \Leftrightarrow \quad b \in \{a, -a\}\,.$$

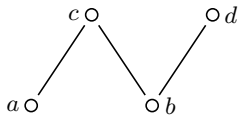
Auf den Äquivalenzklassen $\mathbb{Z}/\!\sim$ wird somit durch $\{a, -a\} \mid \{b, -b\} \ :\Leftrightarrow \ a \mid b$ eine Ordnung definiert. (Man kann die Menge $\mathbb{Z}/\!\sim$ mit den natürlichen Zahlen $\mathbb{N}$ identifizieren und dann ist dies die übliche Teilbarkeitsrelation auf $\mathbb{N}$.)

7.2 Lineare Erweiterungen

Schauen wir uns erneut die Spiegelei-Ordnung aus Beispiel 7.1 an. Praktisch muss man sich ja für eine konkrete Reihenfolge von Arbeitsschritten entscheiden, die alle Vorgänger-Bedingungen berücksichtigt. Es ist also im folgenden Sinne eine lineare Erweiterung einer Ordnung gesucht.

Definition 7.8. Sei (X, R) eine geordnete Menge. Unter einer *Ordnungserweiterung* von R verstehen wir eine Ordnung $S \subseteq X \times X$ mit $R \subseteq S$. Ist die Ordnung S linear, so spricht man von einer *linearen Erweiterung*.

Beispiel 7.5. Auf der Menge $X := \{a, b, c, d\}$ sei die Ordnung $R := \{(a, c), (b, c), (b, d)\} \cup \Delta_X$ betrachtet, also folgendes Diagramm:



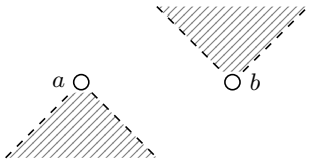
Diese Ordnung besitzt 5 lineare Erweiterungen, nämlich $a < b < c < d$, $a < b < d < c$, $b < a < c < d$, $b < a < d < c$ und $b < d < a < c$.

Ein einzelner Schritt einer Ordnungserweiterung wird im folgenden Lemma behandelt.

Lemma 7.4. *Seien (X, R) eine geordnete Menge und $a, b \in X$ unvergleichbar. Dann ist*

$$R_{a,b} := R \cup \{(x, y) \in X \times X \mid x\, R\, a \ \wedge\ b\, R\, y\}$$

eine Ordnungserweiterung von R mit $(a, b) \in R_{a,b}$.



Beweis. Zu zeigen ist lediglich, dass die Relation $R_{a,b}$ anti-symmetrisch und transitiv ist; der Rest ist klar. Um die Transitivität zu beweisen, gelte $(x, y) \in R_{a,b}$ und $(y, z) \in R_{a,b}$; zu zeigen ist $(x, z) \in R_{a,b}$, also dass $x\, R\, z$ oder $x\, R\, a \ \wedge\ b\, R\, z$ gilt.

Wegen $(x, y) \in R_{a,b}$ ist $x\, R\, y$ oder $x\, R\, a \ \wedge\ b\, R\, y$. Betrachte zuerst den Fall $x\, R\, y$. Wegen $(y, z) \in R_{a,b}$ gilt $y\, R\, z$, woraus $x\, R\, z$ folgt, oder $y\, R\, a \ \wedge\ b\, R\, z$, woraus $x\, R\, a$ folgt – also beiderseits $(x, z) \in R_{a,b}$. Nun sei der Fall $x\, R\, a \ \wedge\ b\, R\, y$ betrachtet. Wiederum ist $y\, R\, z$, woraus $b\, R\, z$ folgt, oder $y\, R\, a \ \wedge\ b\, R\, z$, was jedoch $b\, R\, a$ impliziert im Widerspruch zur Voraussetzung – also folgt wieder $(x, z) \in R_{a,b}$.

Der Beweis der Anti-Symmetrie, also $(x, y) \in R_{a,b}$ und $(y, x) \in R_{a,b}$ impliziert $x = y$, verläuft mit $z = x$ ganz analog wie oben. □

Nun können wir die Existenz von linearen Erweiterungen beweisen. Die nachfolgende Aussage zeigt außerdem, dass wir dabei die Reihenfolge von zwei unvergleichbaren Elementen willkürlich festlegen können.

Satz 7.5 (Lemma von Szpilrajn)**.** *Sei (X, R) eine geordnete Menge mit $(x, y) \notin R$. Dann existiert eine lineare Erweiterung L von R mit $(x, y) \notin L$.*

Beweis. Wir zeigen den Satz hier für endliche Mengen X.

Betrachte die Menge $\mathcal{A}$ aller Ordnungserweiterungen S von R mit $(x, y) \notin S$. Dann ist $(\mathcal{A}, \subseteq)$ eine endliche geordnete Menge, in der somit ein maximales Element $L \in \mathcal{A}$ existiert. Wir behaupten, dass L linear ist, womit der Satz bewiesen ist.

Angenommen, es wären zwei Elemente $a, b \in X$ unvergleichbar bezüglich L. Dann gibt es nach Lemma 7.4 die Ordnungserweiterungen $L_{a,b}$ und $L_{b,a}$. Wegen der Maximalität von L muss dann $L_{a,b} \notin \mathcal{A}$ und $L_{b,a} \notin \mathcal{A}$ gelten, also $(x, y) \in L_{a,b} \cap L_{b,a}$. Wegen $(x, y) \notin L$ folgt somit $x\, L\, a$ und $a\, L\, y$, woraus sich der Widerspruch $x\, L\, y$ ergibt. □

Corollar 7.6. *Jede Ordnung ist ein Durchschnitt von linearen Ordnungen.*

Die minimale Anzahl benötigter linearer Ordnungen bezeichnet man als *Ordnungsdimension* der Ordnung.

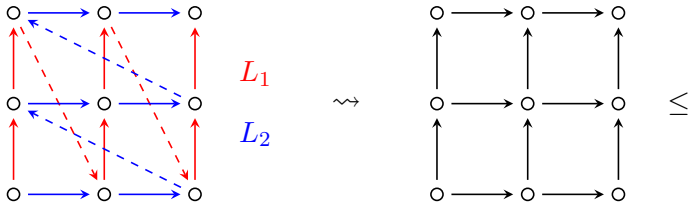
Beispiel 7.6. Für $m, n \geq 2$ betrachte die geordnete Menge $([m] \times [n], \leq)$, wobei

$$(x_1, x_2) \leq (y_1, y_2) \quad :\Leftrightarrow \quad x_1 \leq y_1 \ \wedge\ x_2 \leq y_2\,.$$

Dann hat $\leq$ die Ordnungsdimension 2, denn $\leq$ ist nicht linear, und es gilt $\leq \;=\; L_1 \cap L_2$, wobei die linearen Ordnungen L_i wie folgt definieren seien:

$$\begin{aligned}(x_1, x_2)\, L_1\, (y_1, y_2) \quad &:\Leftrightarrow \quad x_1 < y_1 \;\vee\; (x_1 = y_1 \wedge x_2 \leq y_2) \\ (x_1, x_2)\, L_2\, (y_1, y_2) \quad &:\Leftrightarrow \quad x_2 < y_2 \;\vee\; (x_2 = y_2 \wedge x_1 \leq y_1)\,.\end{aligned}$$

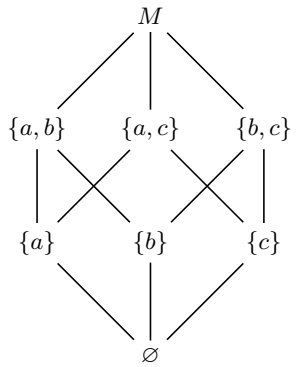
Das Beispiel $([3]\times[3], \leq)$ lässt sich wie folgt illustrieren:



7.3 Teilmengen-Ordnung

Sei M eine Menge und $X := \mathcal{P}(M)$ deren Potenzmenge. Wir wollen im Folgenden die geordnete Menge $(X, \subseteq)$ genauer studieren.

Beispiel 7.7. Betrachte eine drei-elementige Menge $M = \{a, b, c\}$. Die geordnete Menge $(\mathcal{P}(\{a, b, c\}), \subseteq)$ hat dann 8 Elemente und folgendes Ordnungsdiagramm:



Die Ordnung $\subseteq$ besitzt genau 48 lineare Erweiterungen, d. h. Folgen $A_0 < \cdots < A_7$ von Teilmengen von M derart, dass $A_i \subseteq A_j$ stets $i \leq j$ impliziert.

In der Tat ist notwendig $A_0 = \varnothing$ und $A_7 = M$; weiterhin sieht man, dass $|A_1| = |A_2| = 1$ und $|A_5| = |A_6| = 2$ gelten müssen. Daraus ergeben sich einerseits 36 Möglichkeiten mit $A_1, A_2, A_3 \in \binom{M}{1}$ und $A_4, A_5, A_6 \in \binom{M}{2}$ (jeweils in beliebiger Reihenfolge), sowie 12 weitere Möglichkeiten mit $A_3 = A_1 \cup A_2$ und $A_4 = A_5 \cap A_6$ (mit drei Möglichkeiten für $A_3 \in \binom{M}{2}$, sowie A_1, A_2 und A_5, A_6 in beliebiger Reihenfolge).

Die 12 linearen Erweiterungen der zweiten Art lassen sich (teilweise) als lexikographische Ordnungen auf der Potenzmenge auffassen.

Definition 7.9. Sei $(M, \leq)$ eine endliche, linear geordnete Menge. Die *lexikographische* Ordnung auf $X = \mathcal{P}(M)$ (bezüglich $\leq$) sei gegeben durch

$$A \preceq B \quad :\Leftrightarrow \quad A = B \;\vee\; \min\nolimits_{\leq}(A \mathbin{\triangle} B) \in B\,,$$

wobei $A \mathbin{\triangle} B := (A \setminus B) \cup (B \setminus A)$ die „symmetrische Differenz“ sei.

Es lässt sich zeigen, dass die Ordnung $\preceq$ eine lineare Ordnung definiert. Im Beispiel $M = \{a, b, c\}$ mit $a < b < c$ ergibt sich beispielsweise

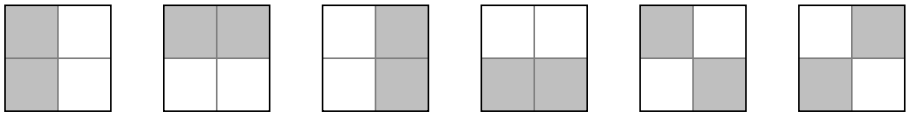
$$\varnothing \prec \{c\} \prec \{b\} \prec \{b, c\} \prec \{a\} \prec \{a, c\} \prec \{a, b\} \prec \{a, b, c\}\,,$$

was sich (bei naheliegender Identifikation) auch als Folge $000 \prec 001 \prec 010 \prec 011 \prec 100 \prec 101 \prec 110 \prec 111$ von Binärwörtern interpretieren lässt.

Die Ordnung $(\mathcal{P}(M), \subseteq)$ kann als Durchschnitt von drei lexikographischen Ordnungen beschrieben werden, etwa bezüglich $a < b < c$, $b < c < a$ und $c < a < b$. Andererseits ist sie kein Durchschnitt von nur zwei linearen Ordnungen (Übung), und somit ist die Ordnungsdimension 3.

Antiketten Ein klassisches kombinatorisches Problem lautet: Wie viele Teilmengen einer n-elementigen Menge kann man finden, so dass keine zwei sich gegenseitig enthalten?

Beispiel 7.8. Im Fall $n = 4$ kann man sich die Teilmengen als Figuren eines 2×2-Rechtecks vorstellen. Es gibt 6 Figuren, die sich gegenseitig nicht enthalten:



Ist dies eine optimale Lösung, oder kann man noch mehr Figuren finden?

Definition 7.10. Sei $(X, \leq)$ eine geordnete Menge. Eine *Antikette* ist eine Teilmenge $Y \subseteq X$ derart, dass alle $x, y \in Y$ mit $x \neq y$ unvergleichbar sind. Es gilt also $\leq_Y = \Delta_Y$.

Die obige Frage kann also wie folgt formuliert werden. Was ist die Kardinalität der größten Antikette in $(\mathcal{P}(M), \subseteq)$, wobei M eine n-elementige Menge ist? Die Antwort liefert der Satz von Sperner, welcher elegant mit folgendem Lemma bewiesen werden kann.

Lemma 7.7 (LYM-Ungleichung[5])**.** *Sei $|M| = n$ und sei $Y \subseteq \mathcal{P}(M)$ eine Antikette. Bezeichne $\alpha_k := |Y \cap \binom{M}{k}|$ die Anzahl der k-elementigen Mengen in Y, so gilt*

$$\sum_{k=0}^{n} \frac{\alpha_k}{\binom{n}{k}} \leq 1\,.$$

Beweis. Der Beweis erfolgt durch doppeltes Abzählen. Sei $\mathcal{C}$ die Menge aller maximalen Ketten in $\mathcal{P}(M)$, also Mengen der Form

$$Z = \{\varnothing, \{a_1\}, \{a_1, a_2\}, \ldots, M\}\,,$$

wobei $M = \{a_1, \ldots, a_n\}$. Dann gilt $|\mathcal{C}| = n \cdot (n-1) \cdot \ldots \cdot 1 = n!$.

Betrachte nun die Relation $R \subseteq \mathcal{C} \times Y$, definiert durch

$$(Z, A) \in R \quad :\Leftrightarrow \quad A \in Z\,.$$

Einerseits gibt es für jede Kette $Z \in \mathcal{C}$ höchstens ein $A \in Y$ mit $A \in Z$ (da Y eine Antikette ist). Andererseits ist jedes $A \in Y$ mit $|A| = k$ in genau $k! \cdot (n-k)!$ Ketten $Z \in \mathcal{C}$ enthalten. Somit folgt

$$\sum_{k=0}^{n} \alpha_k \cdot k! \cdot (n-k)! \leq n!\,,$$

und Teilen durch $n!$ ergibt die Behauptung. □

[5]Die Abkürzung LYM steht für die Autoren Lubell, Yamamoto und Meshalkin, welche das Resultat unabhängig voneinander herleiteten.

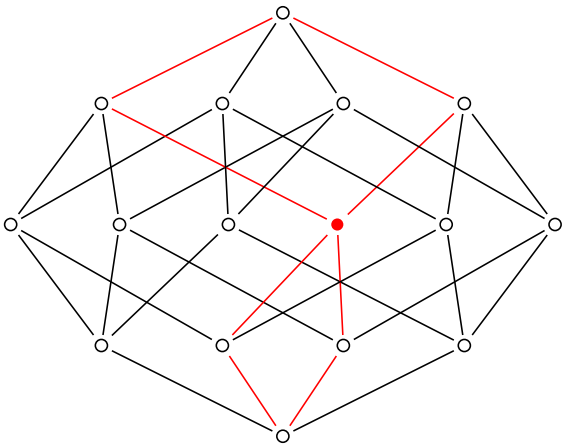


Illustration für $n = 4$: ein $A \in \binom{M}{2}$ und zugehörige vier Ketten

Aus der LYM-Ungleichung folgt leicht der folgende klassische Satz.

Satz 7.8 (Sperner)**.** *Sei M eine n-elementige Menge. Eine größte Antikette in $(\mathcal{P}(M), \subseteq)$ hat $\binom{n}{m}$ Elemente, wobei $m := \lfloor \frac{n}{2} \rfloor$ sei.*

Zusatz: Für n gerade ist nur $\binom{M}{m}$, die Menge aller m-elementigen Teilmengen, eine solche Antikette, während für n ungerade genau $\binom{M}{m}$ und $\binom{M}{m+1}$ die größten Antiketten sind.

Beweis. Sei $Y \subseteq \mathcal{P}(M)$ eine Antikette und sei $\alpha_k := |Y \cap \binom{M}{k}|$. Dann gilt $\binom{n}{k} \leq \binom{n}{m}$ für alle $0 \leq k \leq n$ (Übung), und somit folgt

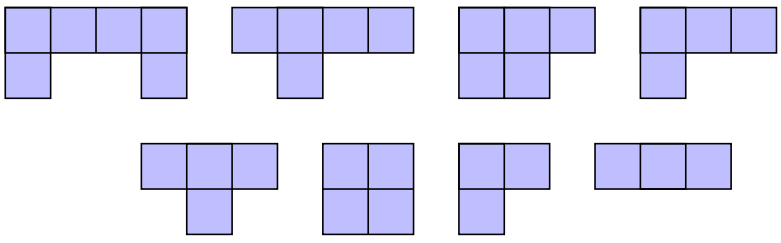
$$\sum_{k=0}^{n} \frac{\alpha_k}{\binom{n}{m}} \leq \sum_{k=0}^{n} \frac{\alpha_k}{\binom{n}{k}} \leq 1$$

mit Lemma 7.7. Dies impliziert $|Y| = \sum_{k=0}^{n} \alpha_k \leq \binom{n}{m}$. □

7.4 Antiketten, Matchings, Flüsse

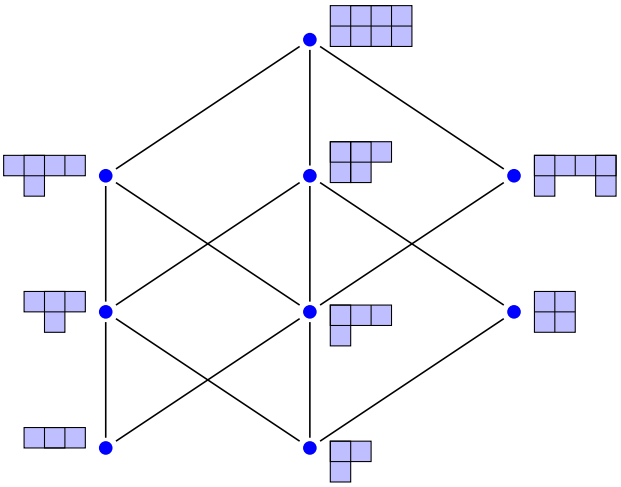
In diesem Abschnitt betrachten wir Antiketten allgemein in einer geordneten Menge und stellen einen Zusammenhang mit Flüssen in Transportnetzen her. Wir beginnen abermals mit einem Beispiel aus B. Ganter, *Diskrete Mathematik: Geordnete Mengen.*

Beispiel 7.9. Eine Firma produziert aus einem 2×4-Block acht verschiedene Formen:

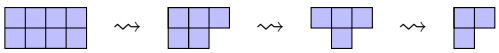


Jede dieser Formen wird nur einmal kurz benötigt. Wie viele Blöcke sind dann nötig?

Das Enthaltensein dieser Figuren ist eine Ordnungsrelation, welche durch das folgende Diagramm dargestellt werden kann.



Die folgende Kette wäre beispielsweise möglich, sie gehört allerdings nicht zu einer optimalen Lösung:



Das Problem lautet also, eine geordnete Menge mit möglichst wenigen geordneten Ketten zu überdecken. Hierfür ist der folgende Satz und sein Beweis von Interesse.

Satz 7.9 (Dilworth)**.** *Sei $(X, \leq)$ eine endliche geordnete Menge. Dann ist die maximale Größe einer Antikette gleich der minimalen Anzahl Ketten die X zerlegen. Es gilt also:*

$$\max_{Y \text{ Antikette}} |Y| = \min_{\mathcal{C} \text{ Kettenpartition}} |\mathcal{C}| .$$

Zum Beweis. Sei $Y \subseteq X$ eine Antikette und $\mathcal{C}$ eine Kettenpartition. Da jede Kette $Z \in \mathcal{C}$ höchstens ein Element $y \in Y$ der Antikette enthält (und jedes $y \in Y$ in ein $Z \in \mathcal{C}$ enthalten ist) folgt $|Y| \leq |\mathcal{C}|$. Also gilt jedenfalls $\max_Y |Y| \leq \min_{\mathcal{C}} |\mathcal{C}|$.

Nun müssen wir zeigen, dass eine Antikette Y und eine Kettenpartition $\mathcal{C}$ existieren mit gleicher Anzahl $|Y| = |\mathcal{C}|$. Dies zeigen wir mittels eines Satzes über Matchings, der wiederum aus dem Max-Flow-Min-Cut-Theorem folgt.

Matchings Ein Graph $G = (V, E)$ (mit $E \subseteq \binom{V}{2}$) heißt *bipartit*, falls es eine Zerlegung $V = U_1 \dot\cup U_2$ der Knotenmenge gibt, so dass keine Kanten innerhalb U_1 oder U_2 existieren, d. h. für alle Kanten $e \in E$ gilt $e \cap U_j \neq \varnothing$ für $j = 1, 2$.

Ein *Matching* in G ist eine Menge $M \subseteq E$ paarweise disjunkter Kanten, und eine *Knotenüberdeckung* ist eine Menge $C \subseteq V$ derart, dass $C \cap e \neq \varnothing$ für alle $e \in E$ gilt.

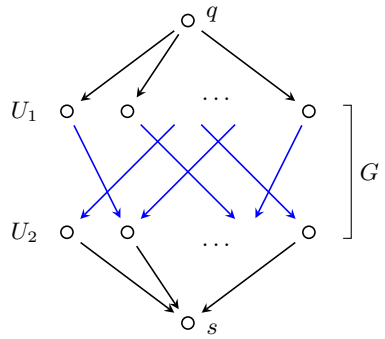
Satz 7.10 (Kőnig)**.** *In einem bipartiten Graphen ist die maximale Größe eines Matchings gleich der minimalen Größe einer Knotenüberdeckung.*

Beweis. Sei $G = (V, E)$ ein bipartiter Graph mit $V = U_1 \dot\cup U_2$. Ist M ein Matching und C eine Knotenüberdeckung, so berührt jede Matchingkante $e \in M$ einen Knoten $v \in C$. Umgekehrt ist jeder Knoten $v \in C$ Endpunkt höchstens einer Matchingkante $e \in M$. Folglich ist $|M| \leq |C|$ und somit gilt $\max_M |M| \leq \max_C |C|$. Wir zeigen nun, dass ein Matching M und eine Knotenüberdeckung C existieren mit $|M| = |C|$.

Dazu definieren wir ein Transportnetz $(\tilde V, \tilde E, q, s, \mathrm{wt})$ mit Knotenmenge $\tilde V := V \cup \{q, s\}$ (mit zwei neuen Knoten $q, s \notin V$) und Kantenmenge

$$\begin{aligned} \tilde E := {} & \{(q, u_1) \mid u_1 \in U_1\} \cup \{(u_2, s) \mid u_2 \in U_2\} \\ & \cup \{(u_1, u_2) \in U_1 \times U_2 \mid \{u_1, u_2\} \in E\} , \end{aligned}$$

sowie Gewichten $\mathrm{wt}(q, u_1) = \mathrm{wt}(u_2, s) = 1$ und $\mathrm{wt}(u_1, u_2) = |V| + 1$ für alle $u_1 \in U_1$, $u_2 \in U_2$ mit $\{u_1, u_2\} \in E$.

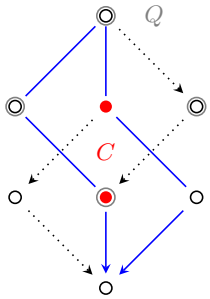


Nach dem Max-Flow-Min-Cut-Theorem Satz 6.14 existiert für dieses Transportnetz ein Fluss f und ein Schnitt $\mathcal{S}$ mit gleichen Werten $|f| = |\mathcal{S}|$. Der Fluss ist ganzzahlig und definiert somit eine Menge von $|f|$ kantendisjunkten Wegen von q nach s. Die dabei benutzten Kanten in E bilden dabei nach Konstruktion des Transportnetzes ein Matching M, und es gilt $|M| = |f|$.

Zum minimalen Schnitt $\mathcal{S} = (Q, S)$ betrachte die Schnittkanten $\tilde{E}_{\mathcal{S}} := \tilde{E} \cap Q \times S$ von Q nach S (also gilt $|\mathcal{S}| = |\tilde{E}_{\mathcal{S}}|$). Wegen des hohen Gewichts $|V| + 1$ der Kanten von U_1 nach U_2 müssen alle Schnittkanten die Quelle q oder die Senke s berühren. Dann ist

$$C := (U_1 \cap S) \cup (U_2 \cap Q)$$

eine Knotenüberdeckung, denn jede Kante $e = \{u_1, u_2\} \in E$ (wobei $u_1 \in U_1$ und $u_2 \in U_2$) gehört nicht zum Schnitt, folglich gilt $(u_1, u_2) \notin Q \times S$, das heißt $u_1 \in S$ oder $u_2 \in Q$. Wegen $|C| = |\tilde{E}_{\mathcal{S}}| = |\mathcal{S}|$ folgt schließlich $|M| = |f| = |\mathcal{S}| = |C|$, wie gewünscht. □



Graph mit Fluss, Schnitt und Knotenüberdeckung

Schließlich können wir mittels des Satzes von Kőnig über Matchings den Satz von Dilworth über Antiketten beweisen.

Beweis von Satz 7.9. Zur gegebenen endlichen geordneten Menge $(X, \leq)$ (mit $|X| = n$ Elementen) betrachte einen bipartiten Graphen $G = (V, E)$ mit Knotenmenge $V = X^- \dot\cup X^+$ und Kantenmenge

$$E := \left\{\{x^-, y^+\} \mid x < y\right\}.$$

Nach Satz 7.10 existiert in G ein Matching $M \subseteq E$ und eine Knotenüberdeckung $C \subseteq V$ mit $|M| = |C|$. Wir definieren nun eine Antikette und eine Kettenpartition wie folgt. Die Teilmenge

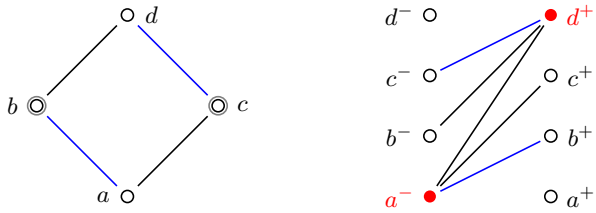
$$Y := \{x \in X \mid x^- \notin C \wedge x^+ \notin C\}$$

ist eine Antikette, denn wäre $x < y$ für $x, y \in Y$, also $\{x^-, y^+\} \in E$, so wäre x^- oder y^+ in der Knotenüberdeckung C. Weiterhin gilt $|Y| \geq n - |C|$.

Nun benutzen wir die Matchingkanten, um Elemente von X zu Ketten zu verbinden. Genauer betrachten wir die symmetrische Relation R auf X, gegeben durch

$$x \, R \, y \;:\Leftrightarrow\; \{x^-, y^+\} \in M \;\vee\; \{y^-, x^+\} \in M \,.$$

und definieren eine Zerlegung $\mathcal{C}$ durch die Äquivalenzrelation $\sim := \operatorname{trans}(R) \cup \Delta_X$. Aus der Matching-Eigenschaft folgt dann, dass jede Klasse eine Kette ist. Weiterhin gilt für die Anzahl der Klassen $|\mathcal{C}| = n - |M|$, und somit folgt $|\mathcal{C}| = n - |M| = n - |C| \leq |Y|$, wie gewünscht. □



Antikette und Kettenpartition, sowie Matching und Knotenüberdeckung

Als eine vielleicht überraschende Anwendung des Satzes von Dilworth präsentieren wir einen kurzen Beweis eines klassischen Resultats von Erdős und Szekeres.

Corollar 7.11. *Sei $a_1, \ldots, a_n$ eine Folge verschiedener reeller Zahlen, wobei $n \geq k\ell + 1$. Dann findet sich darin eine aufsteigende Teilfolge*

$$a_{i_1} < \cdots < a_{i_{k+1}}$$

(mit $i_1 < \cdots < i_{k+1}$) der Länge $k + 1$, oder eine absteigende Teilfolge

$$a_{j_1} > \cdots > a_{i_{\ell+1}}$$

(mit $j_1 < \cdots < j_{\ell+1}$) der Länge $\ell + 1$.

Beweis. Wir benutzen Satz 7.9. Betrachte auf der Menge $X = [n]$ die durch

$$i \, R \, j \;:\Leftrightarrow\; i \leq j \;\wedge\; a_i \leq a_j$$

definierte Ordnung; dann entspricht einer Kette offenbar eine aufsteigende Teilfolge und einer Antikette eine absteigende. Wenn die größte Antikette höchstens ℓ Elemente hat, muss demnach eine Kette mit mehr als k Elementen existieren. □

8 Unendlichkeit

Mach dir keine Sorgen wegen deiner Schwierigkeiten mit der Mathematik. Ich kann dir versichern, dass meine noch größer sind.

— Albert Einstein

Die moderne Sprache der Mathematik, welche auf den Begriffen der Menge und der Abbildung basiert, erlaubt auch den Umgang mit unendlichen Mengen. Wir setzen dabei ein weiteres Axiom voraus, und zwar eine der äquivalenten Formulierungen des sogenannten Auswahlaxioms, welches zwar naheliegend erscheinen mag, jedoch (etwa wegen seiner weitreichenden Konsequenzen) unter Mathematikern nicht ganz unumstritten ist.

Axiom 7 (Auswahl)**.** Jede surjektive Abbildung ist rechtsinvertierbar. Das heißt, zu jeder Surjektion $f\colon X \to Y$ existiert eine (injektive) Abbildung $g\colon Y \to X$ mit $f \circ g = \mathrm{id}_Y$.

Die rechtsinverse Abbildung g wählt also für jedes $y \in Y$ ein Urbild aus der nichtleeren Menge $f^{-1}(\{y\}) = \{x \in X \mid f(x) = y\}$ aus. Jede Rechtsinverse ist injektiv.

Es sei daran erinnert, dass eine Menge X endlich heißt, falls eine Bijektion $X \to [n]$ für ein $n \in \mathbb{N}$ besteht. Die natürliche Zahl n ist dann eindeutig und wird als Kardinalität von X bezeichnet. Eine Menge, die nicht endlich ist, nennen wir *unendlich*.

Man kann zeigen, dass eine Menge X genau dann unendlich ist, wenn es eine Abbildung $X \to X$ gibt, die injektiv, aber nicht surjektiv ist; diese Eigenschaft wird auch „Dedekind-unendlich“ genannt.

Abzählbarkeit Mittels Abbildungen können wir verschiedene „Arten von Unendlichkeit“ unterscheiden. Eine grundlegende Klassifikation liefert der Begriff der Abzählbarkeit. Die folgende Definition präzisiert die Idee, dass sich eine abzählbare Menge X als eine Folge $X = \{x_1, x_2, x_3, \dots\}$ darstellen lässt.

Definition 8.1. Eine Menge X heißt *abzählbar*, falls eine Surjektion $\mathbb{N} \to X$ existiert. Andernfalls heißt X *überabzählbar*.

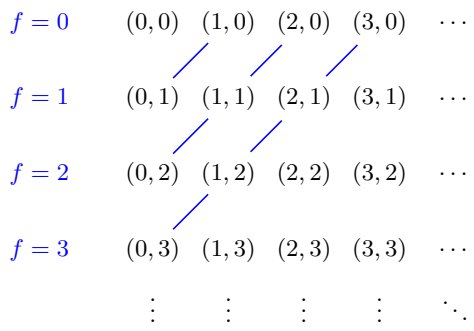
Eine Menge X ist genau dann abzählbar, wenn eine Injektion $X \to \mathbb{N}$ besteht. Und die Menge X ist genau dann abzählbar unendlich, wenn eine Bijektion $X \to \mathbb{N}$ existiert.

Falls eine Bijektion $X \to Y$ zwischen zwei Mengen X und Y besteht, so nennt man diese Mengen *gleichmächtig*; man sagt auch, dass X die „Mächtigkeit“ (oder „Kardinalität“) Y hat. Somit hat jede abzählbar unendliche Menge die Mächtigkeit $\mathbb{N}$.

Welche Mengen sind abzählbar? Es ist nützlich zu bemerken, dass eine Menge X bereits dann abzählbar ist, wenn es eine Abbildung $f\colon X \to \mathbb{N}$ gibt derart, dass jedes Urbild $f^{-1}(\{n\})$ für $n \in \mathbb{N}$ endlich ist. (In diesem Fall können wir nämlich die endlichen Urbildmengen „der Reihe nach“ aufzählen.)

Beispiel 8.1. Folgende Mengen sind abzählbar.

1) $X = \mathbb{N} \times \mathbb{N}$, etwa via $f(m, n) := m + n$. Diese Begründung ist als Cantors erstes Diagonalargument bekannt:



2) $X = \mathbb{Z}$, via $f(x) := |x|$.

3) $\mathbb{Q}$, denn $X = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ ist abzählbar und $\mathbb{Q} = X/\!\sim$.

Dass auch (sehr viele) überabzählbare Mengen existieren, ergibt sich aus dem folgenden allgemeinen Resultat.

Satz 8.1 (Cantors zweites Diagonalargument)**.** *Für jede Menge X ist die Potenzmenge $\mathcal{P}(X)$ nicht gleichmächtig zu X.*

Beweis. Angenommen, es gäbe es eine Surjektion $X \to \mathcal{P}(X)$, $x \mapsto A_x$. Betrachte die Menge $B := \{x \in X \mid x \notin A_x\} \in \mathcal{P}(X)$. Also existiert $y \in X$ mit $B = A_y$. Dann gilt

$$y \in A_y \quad \Leftrightarrow \quad y \in B \quad \Leftrightarrow \quad y \notin A_y\,,$$

dies ist offenbar ein Widerspruch. □

Hieraus folgt, dass die Mengen $\mathcal{P}(\mathbb{N})$ und somit auch $\{0,1\}^{\mathbb{N}} = \{f\colon \mathbb{N} \to \{0,1\}\}$ überabzählbar sind. Ein ganz ähnliches Diagonalargument zeigt auch, dass die Menge der reellen Zahlen (unendlich viele Nachkommastellen) überabzählbar ist.

Das Lemma von Zorn Ein wichtige, starke Aussage im Umgang mit unendlichen Mengen stellt das folgende Resultat über geordnete Mengen dar, welches oft in (nicht-konstruktiven) Existenzbeweisen zur Anwendung kommt.

Satz 8.2 (Lemma von Zorn)**.** *Eine geordnete Menge, in der jede Kette eine obere Schranke hat, besitzt stets ein maximales Element.*

Es sei bemerkt, dass dieses Resultat für lineare Ordnungen, wie $(X, \leq)$ für $X \subseteq \mathbb{R}$, nicht interessant ist, weil in diesem Fall die Menge X selbst eine Kette ist. Anders verhält es sich für den Fall $(\mathcal{A}, \subseteq)$ von Teilmengen $\mathcal{A} \subseteq \mathcal{P}(M)$ einer Potenzmenge von M; meistens wird das Lemma in diesem Kontext angewandt.

Das Lemma von Zorn bildet eine Grundlage für ganze mathematische Theorien (beispielsweise Funktionalanalysis). Der Beweis ist allerdings recht anspruchsvoll und verwendet das Auswahlaxiom; umgekehrt lässt sich das Auswahlaxiom aus dem Lemma von Zorn folgern. Wir stellen schließlich zwei Anwendungen vor.

Das „Lemma von Szpilrajn“, Satz 7.5, besagt, dass jede geordnete Menge (X, R) mit $(x, y) \notin R$ eine lineare Erweiterung L von R besitzt mit $(x, y) \notin L$.

Beweis für beliebige Mengen X. Betrachte die Menge $\mathcal{A} \subseteq \mathcal{P}(X \times X)$ aller Ordnungserweiterungen S von R mit $(x, y) \notin S$. Dann erfüllt die geordnete Menge $(\mathcal{A}, \subseteq)$ die Voraussetzung des Lemmas von Zorn.

Denn sei $\mathcal{C} \subseteq \mathcal{A}$ eine Kette, so ist $T := \bigcup_{S \in \mathcal{C}} S$ eine obere Schranke von $\mathcal{C}$. Hierzu ist lediglich $T \in \mathcal{A}$ zu zeigen, also dass auch T eine Ordnung ist. Sicherlich ist T reflexiv und symmetrisch. Für die Transitivität seien $x, y, z \in X$ mit $x \mathrel{T} y$ und $y \mathrel{T} z$ gegeben, also gibt es $S_1, S_2 \in \mathcal{C}$ mit $x \mathrel{S_1} y$ und $y \mathrel{S_2} z$. Weil $\mathcal{C}$ eine Kette ist, gilt $S_1 \subseteq S_2$ oder $S_2 \subseteq S_1$. Ohne Einschränkung sei $S_1 \subseteq S_2$, also $x \mathrel{S_2} y$ und $y \mathrel{S_2} z$; dann folgt $x \mathrel{S_2} z$, weil S_2 transitiv ist, und somit ist $x \mathrel{T} z$, wie gewünscht.

Nach Satz 8.2 existiert nun ein maximales Element $L \in \mathcal{A}$, und der Beweis, dass L die gesuchte lineare Erweiterung ist, kann wie vorher geführt werden. □

„Jeder Vektorraum hat eine Basis.“

Hierzu müssen wir zunächst den Begriff der Basis auf unendliche Mengen erweitern. Sei V ein beliebiger K-Vektoraum. Eine Teilmenge $B \subseteq V$ heißt *linear unabhängig*, falls jede endliche Teilmenge $B_0 \subseteq B$ linear unabhängig ist. Und die Menge B heißt *Basis*, falls sie linear unabhängig und erzeugend ist, das heißt, falls jedes $x \in V$ eine eindeutige Darstellung $x = \sum_{v \in B} \lambda_v v$ mit endlich vielen $\lambda_v \neq 0$ hat.

Beweis. Sei $\mathcal{A} \subseteq \mathcal{P}(V)$ die Menge aller linear unabhängigen Teilmengen und betrachte die geordnete Menge $(\mathcal{A}, \subseteq)$. Ist $\mathcal{C} \subseteq \mathcal{A}$ eine Kette, so ist die Menge $B := \bigcup_{A \in \mathcal{C}} A$ linear unabhängig. Denn ist $B_0 = \{v_1, \ldots, v_n\} \subseteq B$ eine endliche Teilmenge, so gibt es $A_1, \ldots, A_n \in \mathcal{C}$ mit $v_i \in A_i$ für alle i. Weil die A_i eine Kette bilden, gibt es j mit $A_i \subseteq A_j$ für alle i, also $B_0 = \{v_1, \ldots, v_n\} \subseteq A_j$. Die lineare Unabhängigkeit von A_j impliziert nun, dass B_0 linear unabhängig ist.

Nach Satz 8.2 existiert also ein maximales Element $B \in \mathcal{A}$. Dies ist in der Tat eine Basis von V. Denn wäre B nicht erzeugend, so gäbe es $w \notin \operatorname{span}(B)$, und in diesem Fall wäre auch $B \cup \{w\}$ linear unabhängig, im Widerspruch zur Maximalität. □

Die Aussage, dass jeder Vektorraum eine Basis besitzt, ist im Grunde genommen ganz erstaunlich. Als Beispiel betrachten wir den $\mathbb{R}$-Vektorraum

$$\mathbb{R}^{\mathbb{N}} := \{(a_n)_{n \in \mathbb{N}} \mid \forall n \in \mathbb{N} : a_n \in \mathbb{R}\}$$

aller reellen Folgen. Dieser besitzt also eine Basis. Man beachte hierbei, dass die Menge der „Einheitsfolgen“ $\{e^{(k)} \mid k \in \mathbb{N}\}$ (wobei $e^{(k)}_k = 1$ und $e^{(k)}_n = 0$ für $n \neq k$) keine Basis ist, weil sie den Vektorraum $\mathbb{R}^{\mathbb{N}}$ nicht erzeugt (sondern nur die Folgen mit endlich vielen Komponenten $\neq 0$); tatsächlich ist eine Basis notwendig überabzählbar.

Index