Diskrete Strukturen

Vorlesung (entspricht 3V+1Ü SWS)

Prof. Dr. Nicole Schweikardt

Lehrstuhl Theoretische Informatik / Logik in der Informatik
Institut für Informatik
Humboldt-Universität zu Berlin

Version vom 19. Oktober 2023

Vorwort

Dieses Vorlesungsskript ist im Laufe des Wintersemesters 2022/2023 und des Sommersemesters 2023 entstanden. Es enthält das Material, das im Wintersemester 2022/2023 in den Vorlesungen und Übungen der Veranstaltung „Diskrete Strukturen“ behandelt wurde. Diese Veranstaltung richtet sich an Studierende im ersten Semester des Bachelor-Studiengangs Informatik.

Am Ende jedes einzelnen Kapitels findet sich eine Sammlung von Übungsaufgaben, die zum Ziel haben, die Inhalte des Kapitels zu wiederholen und zu vertiefen. Einige Aufgaben sind mit einem $*$ markiert um anzudeuten, dass die Lösung dieser Aufgabe evtl. etwas kniffliger ist als die Lösung der meisten anderen Aufgaben.

Ich bedanke mich sehr herzlich bei allen, die zum Entstehen dieses Vorlesungsskripts beigetragen haben – insbesondere bei Benjamin Scheidt, der mit mir zusammen den Übungsbetrieb organisiert und viele der hier enthaltenen Übungsaufgaben entworfen hat, bei Charlotte Lenz, die die im Skript enthaltenen Zeichnungen und Skizzen gestaltet hat, und bei Max Wehmeier, der die Übungsaufgaben ins Vorlesungsskript eingearbeitet hat.

Berlin, im Oktober 2023 Nicole Schweikardt

Inhaltsverzeichnis

Kapitel 1

Einführung ins Thema

1.1 Ziele der Veranstaltung „Diskrete Strukturen“

Folie 1

Auszug aus der Studien- und Prüfungsordnung

Lern- und Qualifikationsziele dieser Veranstaltung:

> Studierende erlernen die zum fundierten Verständnis der Informatik notwendigen Grundlagen der diskreten mathematischen Strukturen.
>
> Sie erwerben die Fähigkeit, mathematische Aussagen zu verstehen und Beweise selbst zu führen, sowie Probleme präzise zu formulieren und durch Methoden der diskreten Mathematik zu lösen.

Themen und Inhalte der Veranstaltung:

- Mathematische Grundbegriffe;
  Mathematische Beweise verstehen und selbst formulieren
- Graphen und Bäume
- Algebraische Strukturen
- Kombinatorik
- Diskrete Stochastik

Folie 2

Verortung der Begriffe „diskret“ und „Struktur“

Auszug aus DUDEN Fremdwörterbuch *(6. Auflage, 1997):*

diskret 1.a) so unauffällig behandelt, ausgeführt o.Ä., dass es von anderen kaum od. gar nicht bemerkt wird; vertraulich

b) taktvoll, rücksichtsvoll; Ggs. ↑ indiskret.

2.a) (von sprachlichen Einheiten) abgegrenzt, abgetrennt, abgrenzbar, z.B. durch Substitution (Sprachw.);

b) *in einzelne Punkte zerfallend, vereinzelt, abzählbar (bezogen auf eine Folge von Ereignissen od. Symbolen; Techn.)*

Struktur 1. [unsichtbare] *Anordnung der Teile eines Ganzen zueinander, gegliederter Aufbau, innere Gliederung.*

2. Gefüge, das aus Teilen besteht, die wechselseitig voneinander abhängen.

3. (ohne Plural) erhabene Musterung bei Textilien, Tapeten o.Ä.

4. geologische Bauform (z.B. Falte, Salzstock u.a.).

Folie 3

Auszug aus dem Vorwort des Buchs [Ste07]:

> Um was aber geht es in einem Buch über diskrete Strukturen? Natürlich nicht etwa um geheime Strukturen, das Wort „diskret“ steht hier vielmehr für das Gegenteil von „analog“.
>
> Die Bedeutung der diskreten Strukturen für die Informatik ist vor allem darin begründet, dass die Arbeitsweise moderner Computer auf den binären Zuständen 0 und 1 basiert. Aber nicht nur der logische Aufbau eines Computers ist diskreter Natur, diskrete Strukturen spielen auch bei der Modellierung und Lösung von Problemen aus der Informatik eine wichtige Rolle.

1.2 Wozu „Diskrete Strukturen“ im Informatik-Studium?

Folie 4

Modellierung mittels diskreter Strukturen

In der Informatik wird das Modellieren mittels diskreter Strukturen als typische Arbeitsmethode in vielen Bereichen angewandt. Es dient der präzisen Beschreibung von Problemen durch geeignete formale Modelle und ist damit Voraussetzung für die systematische Lösung eines Problems (siehe Abbildung 1.1).

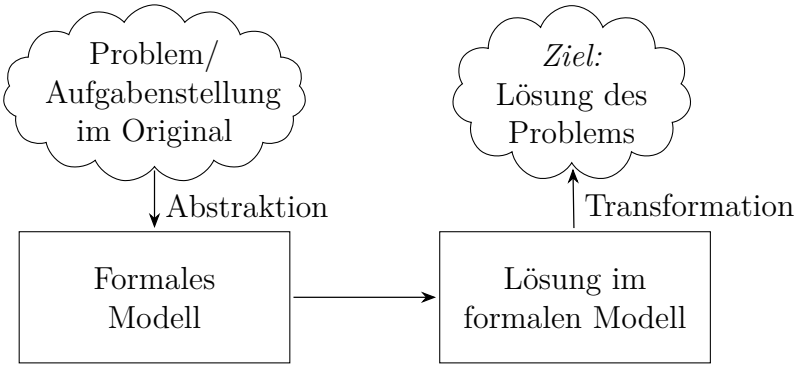


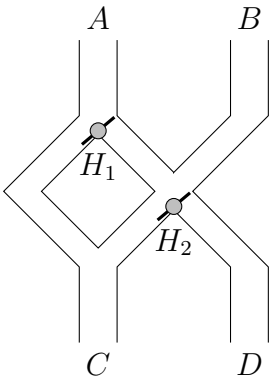
Abbildung 1.1: Generelle Vorgehensweise in der Informatik.

Folie 5

In den verschiedenen Gebieten der Informatik werden unterschiedliche, jeweils an die Art der Probleme und Aufgaben angepasste diskrete Modellierungsmethoden verwendet. Ziel ist jeweils, (nur) die zur Lösung des Problems *relevanten* Aspekte präzise zu beschreiben.
In der Veranstaltung „Diskrete Strukturen“ werden die Grundlagen von verschiedenen diskreten Modellierungsmethoden behandelt und anhand von anschaulichen Beispielen verdeutlicht.

Folie 6

Beispiel 1.1 (Problem „Murmeln“)**.**
Die nachfolgende Abbildung zeigt ein Spiel, in dem Murmeln bei A oder B in die Spielbahn fallen gelassen werden.



Folie 7

Je nach Stellung der Hebel H_1 und H_2 rollen die Murmeln in der Spielbahn nach links oder rechts. Sobald eine Murmel auf einen dieser Hebel trifft, wird der Hebel nach dem Passieren der Murmel umgestellt, so dass die nächste Murmel in die andere Richtung rollt. Zu Beginn ist jeder der beiden Hebel so eingestellt, dass die nächste Murmel, die auf den Hebel trifft, nach links rollt. Wenn beispielsweise nacheinander drei Murmeln fallen gelassen werden, wobei die erste und dritte Murmel bei A und die zweite Murmel bei B fallen gelassen wird, dannkommen die ersten beiden Murmeln an der Öffnung C und die letzte Murmel an der Öffnung D heraus.

Frage: Aus welcher Öffnung fällt die letzte Murmel, wenn sieben Murmeln fallen gelassen werden, wobei die erste, zweite, vierte und letzte Murmel bei A und alle anderen Murmeln bei B fallen gelassen werden?

Folie 8

Lösungsansätze:

1. Knobeln, um eine Lösung per „Geistesblitz“ zu erhalten

2. Systematisches Vorgehen unter Verwendung von Informatik-Kalkülen

Hier wird der 2. Ansatz verfolgt.

Erste Analyse des Problems:

- *relevante Objekte:*
  Spielbahn, Eingänge A und B, Ausgänge C und D, Hebel H_1 und H_2, Murmeln

- *Tätigkeit:*
  Einwerfen von Murmeln an Eingängen A und/oder B
- *Start:*
  Hebel H_1 und H_2 zeigen nach links
- *Ziel:*
  Herausfinden, aus welchem Ausgang die letzte Murmel rollt, wenn nacheinander Murmeln an folgenden Eingängen eingeworfen werden:
  A, A, B, A, B, B, A

Folie 9

- *Eigenschaften/Beziehungen:*
  - Hebelpositionen: H_1 zeigt entweder nach links oder nach rechts, H_2 zeigt entweder nach links oder nach rechts.
  - Für jeden der beiden Hebel H_1 bzw. H_2 gilt: Wenn er nach links (bzw. rechts) zeigt, so rollt die nächste an ihm vorbeirollende Murmel nach links (bzw. nach rechts) weiter.
  - Jeder der beiden Hebel H_1 bzw. H_2 ändert bei jedem Kontakt mit einer Murmel seine Richtung.
  - Eine bei A eingeworfene Murmel rollt zu Hebel H_1.
    Eine bei B eingeworfene Murmel rollt direkt zu Hebel H_2, ohne Hebel H_1 zu passieren.
  - Zeigt H_1 nach links, so rollt eine bei A eingeworfene Murmel direkt zu Ausgang C.
    Zeigt H_1 nach rechts, so rollt eine bei A eingeworfene Murmel zu Hebel H_2.
  - Zeigt H_2 nach links, so rollt eine diesen Hebel passierende Murmel zu Ausgang C.
    Zeigt H_2 nach rechts, so rollt eine diesen Hebel passierende Murmel zu Ausgang D.

Folie 10

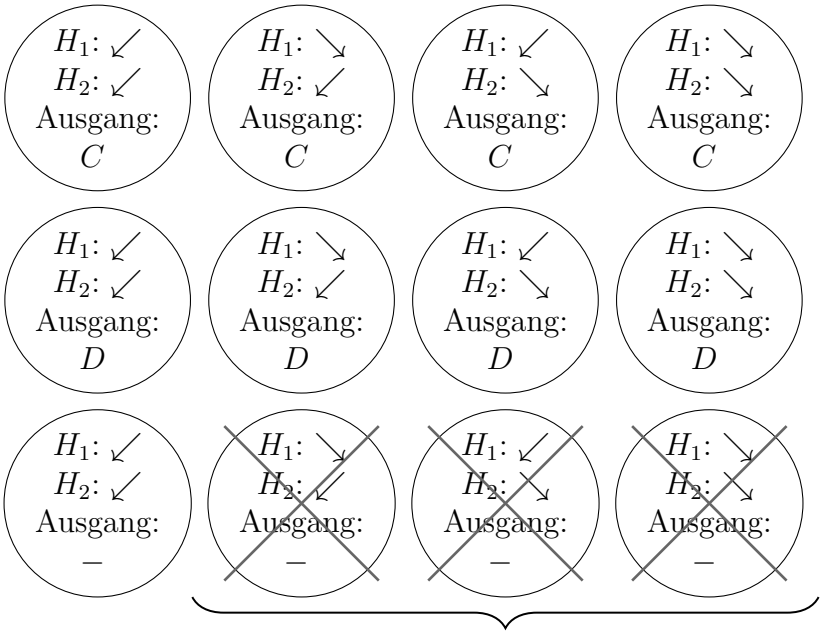
Abstraktionen:

1. Nutze Abkürzungen:

$H_1 : \swarrow$	$\widehat{=}$	Hebel H_1 zeigt nach links
$H_1 : \searrow$	$\widehat{=}$	Hebel H_1 zeigt nach rechts
$H_2 : \swarrow$	$\widehat{=}$	Hebel H_2 zeigt nach links
$H_2 : \searrow$	$\widehat{=}$	Hebel H_2 zeigt nach rechts
Ausgang: C	$\widehat{=}$	die zuvor fallen gelassene Murmel ist an Ausgang C herausgerollt
Ausgang: D	$\widehat{=}$	die zuvor fallen gelassene Murmel ist an Ausgang D herausgerollt
Ausgang: $-$	$\widehat{=}$	es wurde noch keine Murmel eingeworfen

Folie 11

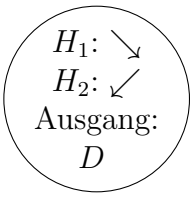
2. Betrachte die möglichen „Zustände“, die auftreten dürfen:



Diese Zustände sind unzulässig, da vor dem Einwurf der ersten Murmel beide Hebel nach links zeigen müssen.

Folie 12

3. Formale Modellierung der „Zustände“: Repräsentiere den „Zustand“



durch das Tupel (R, L, D).

Allgemein wird ein Zustand durch ein Tupel (x, y, z) repräsentiert mit $x \in \{L, R\}$, $y \in \{L, R\}$ und $z \in \{C, D, -\}$, für das folgende Bedingung erfüllt ist: *falls* $z = -$, *so ist* $x = y = L$.

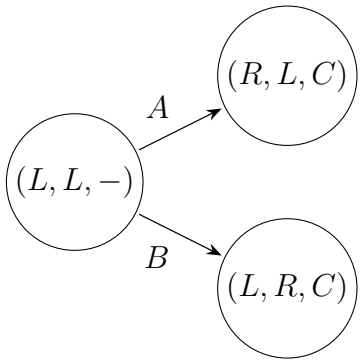
Folie 13

Übergänge von einem Zustand in einen anderen Zustand:

Vom Zustand $(L, L, -)$ aus kann man durch Einwerfen einer einzelnen Murmel in folgende Zustände gelangen:

- (R, L, C), indem die Murmel bei A eingeworfen wird,
- (L, R, C), indem die Murmel bei B eingeworfen wird.

Graphische Darstellung:



Insgesamt ergibt sich das in Abbildung 1.2 dargestellte Bild aus Zuständen und Zustandsübergängen.

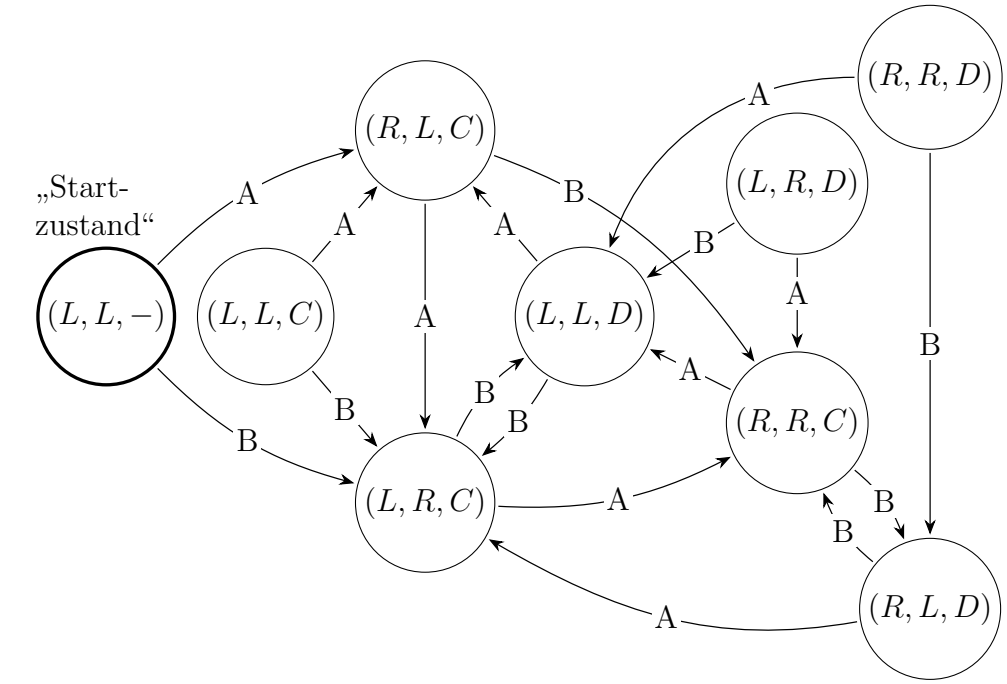


Abbildung 1.2: Übergänge zwischen Zuständen beim Problem „Murmeln“.

Folie 14

Folie 15

Lösung des Problems „Murmeln“:

An diesem Bild lässt sich unser ursprüngliches Problem „Murmeln“ (Frage: Aus welchem Ausgang rollt die letzte Murmel, wenn nacheinander Murmeln an den Eingängen A, A, B, A, B, B, A eingeworfen werden?) leicht lösen, indem man einfach einen Weg vom „Startzustand“ sucht, bei dem die Pfeile nacheinander mit

$$A, A, B, A, B, B, A$$

beschriftet sind. In Abbildung 1.2 gibt es genau einen solchen Weg; er endet mit dem Zustand (L, R, C). Die Antwort auf die ursprünglich gestellte Frage lautet also:

> Wenn nacheinander Murmeln an den Eingängen A, A, B, A, B, B, A eingeworfen werden, so rollt die letzte Murmel durch Ausgang C.

Folie 16

Weiterer Nutzen von Abbildung 1.2

Anhand von Abbildung 1.2 kann auch die folgende Frage beantworten werden:

> Ist es möglich, vom Startzustand aus durch geschicktes Einwerfen von Murmeln zu erreichen, dass die letzte Murmel aus Ausgang D herausrollt und danach beide Hebel nach rechts zeigen?

Um diese Frage zu beantworten muss man einfach nachprüfen, ob es in Abbildung 1.2 einen Weg vom Startzustand zum Zustand (R, R, D) gibt. Man sieht leicht, dass es in Abbildung 1.2 keinen solchen Weg gibt. Folglich lautet die korrekte Antwort auf obige Frage „nein“.

□Ende Bsp. 1.1

Folie 17

Transitionssysteme

Bemerkung 1.2.
Wir haben hier den Kalkül der *Transitionssysteme* (auch bekannt als *endliche Automaten* bzw. *Zustandsübergangsdiagramme* oder *Statecharts*) benutzt. Dieser Kalkül eignet sich besonders gut, wenn Abläufe in Systemen mit Übergängen zwischen verschiedenen Zuständen beschrieben werden sollen.

1.3 Literaturhinweise

Quellennachweis: Das „Murmelproblem“ aus Bsp. 1.1 ist eine vereinfachte Variante von Aufgabe 2.3 in [HU79].

1.4 Übungsaufgaben

Aufgabe 1.1. Der Polizist John McClane steht in einem Brunnen und soll in zwei anfangs leere Gefäße jeweils genau einen Liter füllen. Das eine Gefäß fasst einen Liter, das andere drei. Da sich an den Gefäßen keine Markierungen befinden, kann John nur die folgenden Aktionen durchführen:

Er kann eines der Gefäße vollständig mit Wasser aus dem Brunnen befüllen, eines der Gefäße komplett auskippen oder Wasser eines Gefäßes in das andere kippen bis eines der Gefäße voll oder leer ist. Da John es hasst, von vorne zu beginnen, wird er außerdem niemals in den Startzustand mit zwei leeren Gefäßen zurückkehren.

(a) Kann John McClane sein Ziel erreichen?

(b) Ist es möglich, dass John sich durch eine ungeschickte Abfolge von Schritten (aber unter Berücksichtigung der Regeln) in eine Situation bringt, aus der er das Ziel nicht mehr erreichen kann?

(c) Nehmen Sie nun an, dass John keine Aktion direkt wieder rückgängig macht und ansonsten (unter Berücksichtigung der Regeln) wahllos vorgeht. Wird er dann zwangsläufig irgendwann in den Zustand kommen, in dem er sein Ziel erreicht hat?

Aufgabe 1.2. In dieser Aufgabe betrachten wir das Spiel Dinn, das wie folgt definiert ist: Zwei Personen, Alice und Bob, spielen gegeneinander. Zu Beginn des Spiels liegen neun Hölzer auf dem Tisch, zusätzlich besitzen Alice und Bob jeweils noch eine unbegrenzte Anzahl von Hölzern. Die beiden Spieler sind abwechselnd am Zug, Alice beginnt. In jedem Zug i kann der Spieler, der gerade an der Reihe ist, entweder i Hölzer zusätzlich auf den Tisch legen oder i Hölzer vom Tisch entfernen, wenn dort noch mindestens i Hölzer liegen. So kann Alice im ersten Zug ein Holz zu den Hölzern auf dem Tisch hinzufügen oder davon entfernen. Im zweiten Zug kann Bob entscheiden, ob er zwei Hölzer entfernt oder zwei hinzufügt und so fort. Es gewinnt der Spieler, der eine Anzahl von Hölzern auf dem Tisch hinterlässt, die eine Primzahl ist. *Vorsicht*: 1 ist keine Primzahl.

Modellieren Sie zur Beantwortung der folgenden Fragen das Spiel analog zu Beispiel 1.1 durch ein Transitionssystem. Überlegen Sie sich zunächst, welche Zustände und Zustandsübergänge auftreten können.

(a) Ist es eine gute Idee für Alice, im ersten Zug ein Holz auf den Tisch zu legen?

(b) Eine Gewinnstrategie für einen Spieler in diesem Spiel ist eine Vorschrift, die ihm sagt, welchen Zug er als nächstes tätigen soll. Hält sich der Spieler an diese Vorschrift, so gewinnt er auf jeden Fall. Existiert in diesem Spiel eine Gewinnstrategie für Alice?

(c) Existiert eine Gewinnstrategie für Bob?

Kapitel 2

Mathematische Grundbegriffe und Beweistechniken

Folie 18

Symbol	Bedeutung
$:=$	Definition eines Wertes, z.B. $x := 5$, $M := \{1, 2, 3\}$
$:\Longleftrightarrow$	Definition einer Eigenschaft oder einer Schreibweise z.B. $m \in M :\Longleftrightarrow m$ ist Element von M
ex.	Abkürzung für „es gibt“, „es existiert“
f.a.	Abkürzung für „für alle“, „für jedes“
s.d.	Abkürzung für „so, dass“
$\Longrightarrow$	Abkürzung für „impliziert“ z.B.: Regen $\Longrightarrow$ nasse Straße
$\Longleftrightarrow$	Abkürzung für „genau dann, wenn“ z.B.: Übungsschein erhalten $\Longleftrightarrow$ mindestens 40% der erreichbaren Übungspunkte erreicht
$\square$	markiert das Ende eines Beweises

Folie 19

Modellierung und Wertebereiche

In der Modellierung von Systemen, Aufgaben, Problemen oder Lösungen kommen *Objekte unterschiedlicher Art und Zusammensetzung* vor. Für Teile des Modells wird angegeben, aus welchem Wertebereich sie stammen, es wird zumeist aber offen gelassen, welchen konkreten Wert sie annehmen.

Ein *Wertebereich* ist eine Menge gleichartiger Werte. Wertebereiche werden aus Mengen und Strukturen darüber gebildet.

Folie 20

Beispiel 2.1 (Modellierung der Karten eines (Skat-)Kartenspiels)**.**
Die Karten eines Skat-Kartenspiels lassen sich durch folgende Wertebereiche darstellen:

$$\begin{aligned}
\text{KartenArten} &:= \{\ \text{Kreuz}, \text{Pik}, \text{Herz}, \text{Karo}\ \} \\
\text{KartenSymbole} &:= \{\ 7, 8, 9, 10, \text{Bube}, \text{Dame}, \text{König}, \text{Ass}\ \} \\
\text{Karten} &:= \{\ (\text{Kreuz}, 7), (\text{Kreuz}, 8), \ldots, (\text{Kreuz}, \text{Ass}), \\
&\quad\ (\text{Pik}, 7), (\text{Pik}, 8), \ldots, (\text{Pik}, \text{Ass}), \\
&\quad\ (\text{Herz}, 7), (\text{Herz}, 8), \ldots, (\text{Herz}, \text{Ass}), \\
&\quad\ (\text{Karo}, 7), (\text{Karo}, 8), \ldots, (\text{Karo}, \text{Ass})\ \}.
\end{aligned}$$

□Ende Beispiel 2.1

Folie 21

Wertebereiche sind u.a. wichtig

- zur Modellierung von Strukturen und Zusammenhängen,
- als Grundlage für alle anderen formalen Kalküle und
- als *abstrakte Grundlage für Typen in Programmiersprachen.*

Folie 22

Der grundlegende Kalkül zur Handhabung von Wertebereichen ist die *Mengenlehre*, bei der Mengen und Mengenoperationen betrachtet werden. Zur Modellierung von „zusammengesetzten Wertebereichen“ kann man z.B.

- Potenzmengen,

- kartesische Produkte und Tupel,
- Relationen,
- Folgen bzw. Wörter und
- Funktionen

nutzen. Ziel dieses Kapitels ist, diese Begriffe zu präzisieren und darüber hinaus auch einige wichtige mathematische Grundlagen und Beweistechniken zu erklären.

2.1 Mengen

Was ist eine Menge?

Folie 23

Cantors naiver Mengenbegriff

Cantors naiver Mengenbegriff besagt Folgendes: *(Georg Cantor, 1845–1918)*

> Eine Menge M ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens, welche *Elemente der Menge M* genannt werden, zu einem Ganzen.

Wir schreiben

$$m \in M$$

um auszusagen, dass M eine Menge ist und dass m ein Element in der Menge M ist.

Wir schreiben

$$m \notin M$$

um auszusagen, dass m kein Element in der Menge M ist.

Künftig werden wir solche Notationen festlegen, indem wir kurz Folgendes schreiben:

Notation.

$m \in M \quad :\Longleftrightarrow \quad m$ ist Element der Menge M.

$m \notin M \quad :\Longleftrightarrow \quad m$ ist kein Element der Menge M.

Folie 24

Die Russellsche Antinomie

Cantors Mengenbegriff ist problematisch und führt zu Widersprüchen.
Russell gab folgendes Beispiel:

Die Russellsche Antinomie: *(Bertrand Russell, 1872–1970)*

Sei X die Menge aller Mengen M, die sich nicht selbst als Element enthalten (d.h.: $M \in X \ :\Longleftrightarrow\ M$ ist eine Menge, für die gilt: $M \notin M$).

Frage: Enthält X sich selbst — d.h. gilt $X \in X$?

Klar ist: Entweder es gilt $X \in X$ oder es gilt $X \notin X$.

Fall 1: $X \notin X$.
Gemäß Definition der Menge X gilt dann, dass $X \in X$.
Das ist ein Widerspruch.

Fall 2: $X \in X$.
Gemäß Definition der Menge X gilt dann, dass $X \notin X$.
Das ist ein Widerspruch.

Somit führen beide Fälle zu einem Widerspruch, obwohl wir wissen, dass einer der beiden Fälle zutreffen müsste.

Fazit: *Irgendetwas stimmt nicht mit Cantors naivem Mengenbegriff!*

Folie 25

Der Barbier von Sonnenthal

Um Russells Beispiel und den daraus resultierenden Widerspruch besser zu verstehen, betrachte man folgende Geschichte vom Barbier von Sonnenthal.

> *Der Barbier von Sonnenthal:*
>
> Im Städtchen Sonnenthal (in dem bekanntlich viele seltsame Dinge passieren) wohnt ein Barbier, der genau diejenigen männlichen Einwohner von Sonnenthal rasiert, die sich nicht selbst rasieren.
>
> *Frage:* Rasiert der Barbier sich selbst?

Folie 26

Um die Russellsche Antinomie zu vermeiden, muss man die Mengenlehre sehr sorgfältig axiomatisch aufbauen (siehe z.B. [Ebb03]) — dies sprengt allerdings den Rahmen dieser Vorlesung.
Sofern man sich der Problematik bewusst ist, kann man sie im „täglichen Gebrauch“, den Informatiker*innen von Mengen machen, vermeiden.
Wir arbeiten daher weiter mit einem naiven Mengenbegriff, den wir nach den im Folgenden beschriebenen Grundsätzen verwenden werden.

Folie 27

Beschreibung bzw. Definition von Mengen

Wir beschreiben bzw. definieren Mengen

- *extensional*, durch Aufzählen der Elemente, z.B.

$$M_1 \;:=\; \{0,1,2,3,4,5\} \qquad\qquad \text{oder}$$

- *intensional*, durch Angabe von charakteristischen Eigenschaften der Elemente der Menge, z.B.

$$\begin{aligned} M_2 \;&:=\; \{x \,:\, x \in M_1 \text{ und } x \text{ ist gerade}\} \\ &=\; \{x \in M_1 \,:\, x \text{ ist gerade}\} \\ &=\; \{x \,:\, x \text{ ist eine natürliche Zahl und } x \text{ ist gerade und } 0 \leqslant x \leqslant 5\}. \end{aligned}$$

Extensional lässt sich die Menge M_2 folgendermaßen beschreiben:

$$M_2 \;=\; \{0,2,4\}.$$

Oft schreibt man statt „:“ auch „|“ und statt „und“ einfach ein Komma, also

$$M_2 \;=\; \{x \mid x \in M_1,\, x \text{ gerade}\}.$$

Folie 28

Vorsicht.

- $\{x \,:\, 0 \leqslant x \leqslant 5\}$ definiert nicht eindeutig eine Menge, weil nicht festgelegt ist, ob x beispielsweise eine ganze Zahl oder eine reelle Zahl ist.
- $\{M \,:\, M \text{ ist eine Menge, } M \notin M\}$ führt zur Russellschen Antinomie.

Fazit: *Um solche Probleme zu vermeiden, müssen wir bei intensionalen Mengendefinitionen immer angeben, aus welcher anderen Menge die ausgewählten Elemente kommen sollen*, also:

$$\{x \in M \ : \ x \text{ hat Eigenschaft(en) } E\},$$

wobei M eine Menge und E eine Eigenschaft oder eine Liste von Eigenschaften ist, die jedes einzelne Element aus M haben kann oder nicht.

Folie 29

Wichtige grundsätzliche Eigenschaften von Mengen

- Alle Elemente einer Menge sind verschieden. D.h. ein Wert ist entweder Element der Menge oder eben nicht — aber er kann nicht „mehrfach“ in der Menge vorkommen.
- Die Elemente einer Menge haben keine feste Reihenfolge.
- Dieselbe Menge kann auf verschiedene Weisen beschrieben werden, z.B.
$$\begin{aligned}\{1,2,3\} &= \{1,2,2,3\} = \{2,1,3\} \\ &= \{i \ : \ i \text{ ist eine ganze Zahl, } 0 < i \leqslant 3\}.\end{aligned}$$
- Mengen können aus „atomaren“ oder aus „zusammengesetzten“ Elementen gebildet werden. Eine Menge kann auch „verschiedenartige“ Elemente enthalten. *Beispiel:* Die Menge
$$M \ := \ \{\ 1,\ (\text{Pik}, 8),\ \{\text{rot}, \text{blau}\},\ 5,\ 1\ \}$$
besteht aus 4 Elementen: dem atomaren Wert 1, dem Tupel $(\text{Pik}, 8)$, der Menge $\{\text{rot}, \text{blau}\}$ und dem atomaren Wert 5.

Folie 30

Einige konkrete Zahlenmengen

$\mathbb{N}$	:=	die Menge der natürlichen Zahlen := $\{0, 1, 2, 3, ...\}$
$\mathbb{N}_{\geqslant 1}$	:=	die Menge der positiven natürlichen Zahlen := $\{1, 2, 3, ...\}$
$\mathbb{Z}$	:=	die Menge der ganzen Zahlen := $\{0, 1, -1, 2, -2, 3, -3, ...\}$
$\mathbb{Q}$	:=	die Menge der rationalen Zahlen := $\{\frac{a}{b} \ : \ a, b \in \mathbb{Z},\ b \neq 0\}$
$\mathbb{R}$	:=	die Menge der reellen Zahlen

Folie 31

Die leere Menge und die „Menge aller Mengen“

Beobachtung. Es gibt genau eine Menge, die kein(e) Element(e) enthält.

Definition 2.2 (leere Menge)**.**
Die *leere Menge* ist die (eindeutig bestimmte) Menge, die kein(e) Element(e) enthält. Wir bezeichnen sie mit $\emptyset$.

Frage 2.3. Gibt es eine „Menge aller Mengen“?

Antwort: Nein! Denn wäre U die Menge aller Mengen, so wäre auch $X := \{M \in U : M \notin M\}$ eine Menge. Dies führt aber wieder zur Russellschen Antinomie, da die Frage „Ist $X \in X$?“ nicht geklärt werden kann.

Mengenalgebra

Folie 32

In diesem Abschnitt werden einige grundlegende Operationen auf Mengen betrachtet. Nebenbei werden auch einige (sehr einfache) Beispiele von mathematischen Beweisen gegeben.

Folie 33

Definition 2.4 (Gleichheit von Mengen)**.**
Zwei Mengen X und Y sind gleich (kurz: $X = Y$), falls sie dieselben Elemente enthalten, d.h. falls gilt:

- f.a. $z \in X$ gilt $z \in Y$, und
- f.a. $z \in Y$ gilt $z \in X$.

Beachte.
$\emptyset \neq \{\emptyset\}$, denn $\emptyset$ ist die Menge, die keine Elemente enthält, während $\{\emptyset\}$ eine Menge ist, die ein Element (nämlich $\emptyset$) enthält.

Definition 2.5 (Teilmengen)**.** Seien X, Y Mengen.

(a) X ist eine *Teilmenge* von Y (kurz: $X \subseteq Y$), wenn jedes Element von X auch ein Element von Y ist.

(b) X ist eine *echte Teilmenge* von Y (kurz: $X \subsetneq Y$), wenn $X \subseteq Y$ und $X \neq Y$.

(c) X ist eine *Obermenge* von Y (kurz: $X \supseteq Y$), wenn $Y \subseteq X$.

(d) X ist eine *echte Obermenge* von Y (kurz: $X \supsetneq Y$), wenn $X \supseteq Y$ und $X \neq Y$.

Satz 2.6. *Seien X, Y, Z Mengen. Dann gilt:*

(a) $X = Y \iff X \subseteq Y$ *und* $X \supseteq Y$.

(b) $X \subseteq Y$ *und* $Y \subseteq Z \implies X \subseteq Z$.

Beweis. (a) Es gilt:

$$
\begin{aligned}
X = Y \quad &\overset{\text{Def. 2.4}}{\iff} \quad \text{f.a. } z \in X \text{ gilt } z \in Y \text{ und} \\
&\qquad\qquad\quad \text{f.a. } z \in Y \text{ gilt } z \in X \\
&\iff \quad \text{jedes Element von } X \text{ ist auch ein Element von } Y \text{ und} \\
&\qquad\qquad\quad \text{jedes Element von } Y \text{ ist auch ein Element von } X \\
&\overset{\text{Def. 2.5(a)}}{\iff} \quad X \subseteq Y \text{ und } Y \subseteq X \\
&\overset{\text{Def. 2.5(c)}}{\iff} \quad X \subseteq Y \text{ und } X \supseteq Y.
\end{aligned}
$$

(b) Es gelte $X \subseteq Y$ und $Y \subseteq Z$.

Behauptung: $X \subseteq Z$, d.h. f.a. $x \in X$ gilt $x \in Z$.

Beweis: Sei $x \in X$ beliebig. Wir zeigen, dass $x \in Z$:

$$x \in X \quad \overset{\text{nach Vor.: } X \subseteq Y}{\implies} \quad x \in Y \quad \overset{\text{nach Vor.: } Y \subseteq Z}{\implies} \quad x \in Z.$$

□

Definition 2.7. Seien X und Y Mengen.

(a) Der *Durchschnitt* von X und Y ist die Menge

$$X \cap Y \;:=\; \{z \,:\, z \in X \text{ und } z \in Y\}.$$

(b) Die *Vereinigung* von X und Y ist die Menge

$$X \cup Y \;:=\; \{z \,:\, z \in X \text{ oder } z \in Y\}.$$

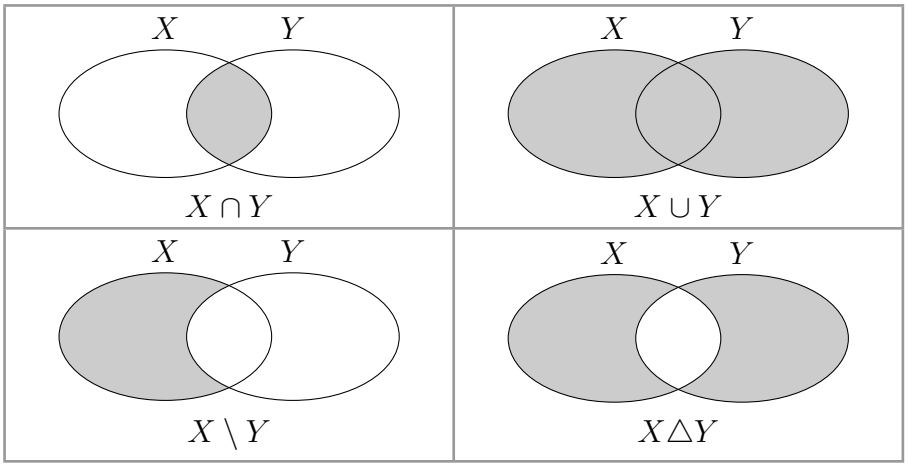
(c) Die *Differenz* von X und Y ist die Menge

$$X \setminus Y \;:=\; X - Y := \{z \,:\, z \in X \text{ und } z \notin Y\}.$$

(d) Die *symmetrische Differenz* von X und Y ist die Menge

$$X \triangle Y \;:=\; (X \setminus Y) \cup (Y \setminus X).$$

Veranschaulichung durch Venn-Diagramme



Notation 2.8 (disjunkt)**.**
Zwei Mengen X und Y heißen *disjunkt*, falls $X \cap Y = \emptyset$, d.h. falls sie keine gemeinsamen Elemente besitzen.Manchmal schreiben wir

$$X \dot\cup Y,$$

um die Menge $X \cup Y$ zu bezeichnen und gleichzeitig auszudrücken, dass $X \cap Y = \emptyset$.

Rechenregeln für Durchschnitt und Vereinigung

Satz 2.9. *Seien X, Y, Z Mengen. Dann gelten:*

(a) Idempotenz:

$$X \cap X \;=\; X \qquad \textit{und} \qquad X \cup X \;=\; X.$$

(b) Kommutativität:

$$X \cap Y \;=\; Y \cap X \qquad \textit{und} \qquad X \cup Y \;=\; Y \cup X.$$

(c) Assoziativität:

$$X \cap (Y \cap Z) \;=\; (X \cap Y) \cap Z \qquad \textit{und} \qquad X \cup (Y \cup Z) \;=\; (X \cup Y) \cup Z.$$

(d) Absorption:

$$X \cap (X \cup Y) \;=\; X \qquad \textit{und} \qquad X \cup (X \cap Y) \;=\; X.$$

(e) Distributivität:

$$X \cap (Y \cup Z) \;=\; (X \cap Y) \cup (X \cap Z) \qquad \textit{und} \qquad X \cup (Y \cap Z) \;=\; (X \cup Y) \cap (X \cup Z).$$

Beweis. (a)

$$\begin{array}{rcl} X \cap X & \overset{\text{Def. 2.7(a)}}{=} & \{x \,:\, x \in X \text{ und } x \in X\} \\ & = & \{x \,:\, x \in X\} \\ & = & X. \end{array}$$

Analog: $X \cup X = X$.

(b)

$$\begin{aligned} X \cap Y &\overset{\text{Def. 2.7(a)}}{=} \{z : z \in X \text{ und } z \in Y\} \\ &= \{z : z \in Y \text{ und } z \in X\} \\ &\overset{\text{Def. 2.7(a)}}{=} Y \cap X. \end{aligned}$$

Analog: $X \cup Y = Y \cup X$.

(c)

$$\begin{aligned} X \cap (Y \cap Z) &\overset{\text{Def. 2.7(a)}}{=} \{x : x \in X \text{ und } x \in Y \cap Z\} \\ &\overset{\text{Def. 2.7(a)}}{=} \{x : x \in X \text{ und } (x \in Y \text{ und } x \in Z)\} \\ &= \{x : (x \in X \text{ und } x \in Y) \text{ und } x \in Z\} \\ &\overset{\text{Def. 2.7(a)}}{=} \{x : x \in X \cap Y \text{ und } x \in Z\} \\ &\overset{\text{Def. 2.7(a)}}{=} (X \cap Y) \cap Z. \end{aligned}$$

Analog: $X \cup (Y \cup Z) = (X \cup Y) \cup Z$.

(d) Wir beweisen, dass $X \cap (X \cup Y) = X$ in zwei Schritten:

Schritt 1: Zeige, dass $X \cap (X \cup Y) \supseteq X$.

Schritt 2: Zeige, dass $X \cap (X \cup Y) \subseteq X$.

Aus Satz 2.6(a) folgt dann, dass $X \cap (X \cup Y) = X$.

Zu Schritt 1:

Behauptung: $X \cap (X \cup Y) \supseteq X$, d.h. f.a. $x \in X$ gilt $x \in X \cap (X \cup Y)$.

Beweis: Sei $x \in X$ beliebig. Zu zeigen: $x \in X \cap (X \cup Y)$. Wegen $x \in X$ gilt auch $x \in X \cup Y$ (gemäß Definition 2.7(b)). Wegen $x \in X$ und $x \in X \cup Y$ gilt gemäß Definition 2.7(a), dass $x \in X \cap (X \cup Y)$.

Zu Schritt 2:

Behauptung: $X \cap (X \cup Y) \subseteq X$, d.h. f.a. $z \in X \cap (X \cup Y)$ gilt $z \in X$.

Beweis: Sei $z \in X \cap (X \cup Y)$ beliebig. Zu zeigen: $z \in X$. Wegen $z \in X \cap (X \cup Y)$ gilt gemäß Definition 2.7(a), dass $z \in X$ und $z \in X \cup Y$. Insbesondere ist also $z \in X$.

Insgesamt haben wir damit gezeigt, dass $X \cap (X \cup Y) = X$.

Analog: $X \cup (X \cap Y) = X$.

(e) Analog; Details: Übungsaufgabe.

□

Das Komplement einer Menge

Folie 39

Das *Komplement* einer Menge M (kurz: $\overline{M}$) soll die Menge aller Elemente sein, die *nicht* zu M gehören. Bei der präzisen Definition von $\overline{M}$ ist allerdings wieder Vorsicht geboten. Denn wenn wir einfach

$$\overline{M} \;:=\; \{x \,:\, x \notin M\}$$

setzen, so gilt für die leere Menge $\emptyset$, dass ihr Komplement $\overline{\emptyset}$ einfach *alles* enthält — und dann wäre

$$\{M \,:\, M \in \overline{\emptyset} \text{ und } M \text{ ist eine Menge}\}$$

die „Menge aller Mengen“ — und dass es die nicht geben kann, haben wir bereits bei der Beantwortung von Frage 2.3 gesehen.
Daher betrachten wir Mengen stets innerhalb eines festen Universums U, das selbst eine Menge ist (die wir jeweils im Kontext angeben müssen). Für $M \subseteq U$ setzen wir dann $\overline{M} := U \setminus M$ und bezeichnen $\overline{M}$ als das Komplement von M in U.

Folie 40

Rechenregeln für Komplemente

Satz 2.10.
Sei U unser festes Universum, das selbst eine Menge ist, und seien $M, N \subseteq U$. Dann gelten:

(a) Doppelte Negation:

$$\overline{(\overline{M})} \;=\; M.$$

(b) De Morgansche Regeln:

$$\overline{M \cap N} \;=\; \overline{M} \cup \overline{N} \qquad \textit{und} \qquad \overline{M \cup N} \;=\; \overline{M} \cap \overline{N}.$$

(c) Inversionsregeln:

$$M \cap \overline{M} \;=\; \emptyset \qquad \textit{und} \qquad M \cup \overline{M} \;=\; U.$$

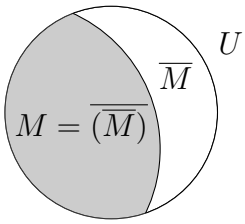
(d) Identitätsregeln:

$$M \cap U \;=\; M \qquad \textit{und} \qquad M \cup \emptyset \;=\; M.$$

Beweis. Übungsaufgabe. □

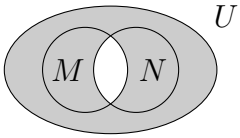
Veranschaulichung durch Venn-Diagramme:

- Doppelte Negation:

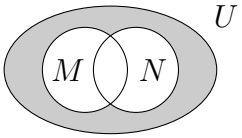


- De Morgansche Regeln:

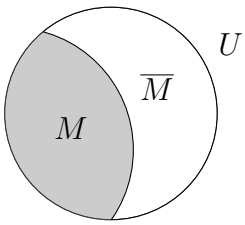
$\overline{M \cap N} = \overline{M} \cup \overline{N}$



$\overline{M \cup N} = \overline{M} \cap \overline{N}$



- Inversionsregel:



Mächtigkeit bzw. Kardinalität einer Menge

Folie 41

Definition 2.11.

(a) Eine Menge heißt *endlich*, wenn sie nur endlich viele Elemente enthält, d.h. wenn es eine Zahl $n \in \mathbb{N}$ gibt, so dass die Menge genau n verschiedene Elemente enthält.

(b) Die *Mächtigkeit* (oder *Kardinalität*) einer Menge M ist

$$|M| := \begin{cases} \text{Anzahl der Elemente in } M, & \text{falls } M \text{ endlich ist} \\ \infty \text{ (unendlich)}, & \text{sonst.} \end{cases}$$

Man beachte, dass „∞“ keine natürliche Zahl ist (d.h. $\infty \notin \mathbb{N}$), sondern lediglich eine Abkürzung für das Wort „unendlich“.

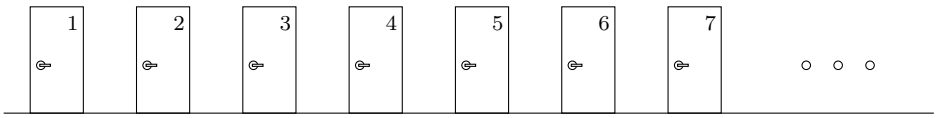
Beispiel 2.12.

$$\begin{array}{lllllllll} |\{2,4,6\}| & = & 3\,, & |\mathbb{N}| & = & \infty\,, & |\emptyset| & = & 0\,, \\ |\{2,4,6,4\}| & = & 3\,, & |\mathbb{Z}| & = & \infty\,, & |\{\emptyset\}| & = & 1\,. \\ |\{2,\{a,b\}\}| & = & 2\,, & & & & & & \end{array}$$

Folie 42

Vorsicht beim Vergleich der Mächtigkeit unendlicher Mengen

Hilberts Hotel (David Hilbert, 1862–1943)
Hilberts Hotel hat unendlich viele Zimmer, die fortlaufend mit $1, 2, 3, \ldots$ (also mit allen Zahlen aus $\mathbb{N}_{\geqslant 1}$) nummeriert sind.



Obwohl alle Zimmer belegt sind, schafft der Angestellte an der Rezeption es, für jeden neuen Gast Platz zu schaffen.

Wie? — Er bittet alle Gäste, in das Zimmer mit der nächsthöheren Nummer umzuziehen und gibt dem neuen Gast das Zimmer mit der Nummer 1.

Fügt man also zu einer unendlichen Menge ein Element hinzu, so erhält man keine „wirklich größere“ Menge.

Es ist nicht schwer, zu sehen, dass im vollbesetzten Hotel sogar unendlich viele neue Gäste, die mit den Zahlen 1, 2, 3, ... durchnummeriert sind, einquartiert werden können. Dazu muss einfach jeder der bisherigen Gäste in das Zimmer umziehen, dessen Nummer das Doppelte der bisherigen Zimmernummer ist. Danach sind alle „alten“ Gäste in den Zimmern mit geraden Zimmernummern untergebracht, und die neuen Gäste können in die Zimmer mit ungeraden Zimmernummern einziehen.

Die Potenzmenge

Definition 2.13.
Die *Potenzmenge* (engl.: power set) einer Menge M (kurz: $\mathcal{P}(M)$) ist die Menge aller Teilmengen von M. D.h.:

$$\mathcal{P}(M) \quad = \quad \{X \,:\, X \subseteq M\}.$$

Beispiel 2.14.

- $\mathcal{P}(\{a,b\}) = \{\, \emptyset, \{a\}, \{b\}, \{a,b\} \,\}$.
- $\mathcal{P}(\{1,2,3\}) = \{\, \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\} \,\}$.
- $\mathcal{P}(\emptyset) = \{\, \emptyset \,\}$.
  Insbesondere gilt: $\mathcal{P}(\emptyset) \neq \emptyset$.

Notation 2.15.
In manchen Büchern wird $\mathcal{P}(M)$ auch mit *Pow(M)* (für „power set“) oder mit 2^M bezeichnet.
Später, in Folgerung 2.39, werden wir nachweisen, dass für jede endliche Menge M gilt:

$$|\mathcal{P}(M)| \quad = \quad 2^{|M|}.$$

2.2 Kartesische Produkte und Relationen

Paare, Tupel und kartesische Produkte

Definition 2.16 (Paare und Tupel)**.**

(a) Für beliebige Objekte a und b bezeichnet (a,b) das geordnete *Paar* mit Komponenten a und b.

(b) Für $k \in \mathbb{N}$ und beliebige Objekte $a_1, \ldots, a_k$ bezeichnet $(a_1, \ldots, a_k)$ das *k-Tupel* mit Komponenten $a_1, \ldots, a_k$.

(c) Die *Gleichheit* zweier Tupel ist wie folgt definiert:
F.a. $k, \ell \in \mathbb{N}$ und $a_1, \ldots, a_k, b_1, \ldots, b_\ell$ gilt:

$$\begin{aligned} & (a_1, \ldots, a_k) = (b_1, \ldots, b_\ell) \\ :\Longleftrightarrow \quad & k = \ell \text{ und } a_1 = b_1 \text{ und } a_2 = b_2 \text{ und } \cdots \text{ und } a_k = b_k. \end{aligned}$$

Bemerkung 2.17.

(a) Für $k = 0$ gibt es genau ein k-Tupel, nämlich das *leere Tupel* (), das keine Komponente(n) hat.

(b) Man beachte den Unterschied zwischen Tupeln und Mengen: z.B.

- $(1, 2) \neq (2, 1)$, aber $\{1, 2\} = \{2, 1\}$.
- $(1, 1, 2) \neq (1, 2)$, aber $\{1, 1, 2\} = \{1, 2\}$.

Folie 45

Definition 2.18.

(a) Sei $k \in \mathbb{N}$ und sei M eine Menge. Die *k-te Potenz* von M ist die Menge

$$M^k \;:=\; \{(m_1, ..., m_k) \,:\, m_1 \in M, \ldots, m_k \in M\}.$$

Insbesondere gilt: $M^0 = \{()\}$ besteht genau aus einem Element, dem leeren Tupel.

(b) Das *kartesische Produkt* (bzw. *Kreuzprodukt*) zweier Mengen X, Y ist die Menge

$$X \times Y \;:=\; \{(x, y) \,:\, x \in X,\, y \in Y\}.$$

(c) Sei $k \in \mathbb{N}_{\geqslant 1}$ und seien $M_1, \ldots, M_k$ Mengen. Das kartesische Produkt von $M_1, \ldots, M_k$ ist die Menge

$$M_1 \times \cdots \times M_k \;:=\; \{(m_1, \ldots, m_k) \,:\, m_1 \in M_1, \ldots, m_k \in M_k\}.$$

Folie 46

Beispiel 2.19. Sei $X = \{a, b\}$ und $Y = \{1, 2, 3\}$. Dann gilt:

- $X \times Y = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$.
- $X \times \{1\} = \{(a, 1), (b, 1)\}$.
- $X \times \emptyset = \emptyset$.
- $X^2 = \{(a, a), (a, b), (b, a), (b, b)\}$.
- $X^1 = \{(a), (b)\}$.
- $X^0 = \{()\}$.
- $\emptyset^2 = \emptyset$.
- $\emptyset^1 = \emptyset$.
- $\emptyset^0 = \{()\}$.

Folie 47

- In Beispiel 2.1 hatten wir die *Karten eines Skat-Kartenspiels* durch folgende Wertebereiche modelliert:

$$\begin{aligned} \text{KartenArten} &= \{\text{Kreuz}, \text{Pik}, \text{Herz}, \text{Karo}\}, \\ \text{KartenSymbole} &= \{7, 8, 9, 10, \text{Bube}, \text{Dame}, \text{König}, \text{Ass}\}, \\ \text{Karten} &= \text{KartenArten} \times \text{KartenSymbole}. \end{aligned}$$

- *Uhrzeiten* kann man repräsentieren durch Elemente der Menge

$$\text{Uhrzeiten} := \text{Stunden} \times \text{Minuten} \times \text{Sekunden},$$

wobei

$$\begin{aligned} \text{Stunden} &:= \{0, 1, 2, ..., 23\}, \\ \text{Minuten} &:= \{0, 1, 2, ..., 59\}, \\ \text{Sekunden} &:= \{0, 1, 2, ..., 59\}. \end{aligned}$$

Das Tupel $(9, 45, 0)$ repräsentiert dann die Uhrzeit „9 Uhr, 45 Minuten und 0 Sekunden“.

Folie 48

Notation 2.20.

- Ist $k \in \mathbb{N}_{\geqslant 1}$ und sind $z_1, \ldots, z_k$ Zahlen, so schreiben wir

$$\sum_{i=1}^{k} z_i \qquad \text{bzw.} \qquad \sum_{i \in \{1,\ldots,k\}} z_i$$

um die Summe der Zahlen $z_1, \ldots, z_k$ zu bezeichnen (d.h. die Zahl $z_1 + \cdots + z_k$).

Wir schreiben

$$\prod_{i=1}^{k} z_i \qquad \text{bzw.} \qquad \prod_{i \in \{1,\ldots,k\}} z_i$$

um das Produkt der Zahlen $z_1, \ldots, z_k$ zu bezeichnen (d.h. die Zahl $z_1 \cdot \cdots \cdot z_k$).

Folie 49

- Sind $M_1, \ldots, M_k$ Mengen, so schreiben wir

$$\bigcup_{i=1}^{k} M_i \qquad \text{bzw.} \qquad \bigcup_{i \in \{1,\ldots,k\}} M_i$$

um die Vereinigung der Mengen $M_1, \ldots, M_k$ zu bezeichnen (d.h. die Menge $M_1 \cup \cdots \cup M_k$).

Wir schreiben

$$\bigcap_{i=1}^{k} M_i \qquad \text{bzw.} \qquad \bigcap_{i \in \{1,\ldots,k\}} M_i$$

um den Durchschnitt der Mengen $M_1, \ldots, M_k$ zu bezeichnen (d.h. die Menge $M_1 \cap \cdots \cap M_k$).

Folie 50

- Ist K eine Menge, deren Elemente Teilmengen einer Menge U sind (d.h.: $K \subseteq \mathcal{P}(U)$), so ist

$$\bigcup_{M \in K} M \quad := \quad \{x \in U \,:\, \text{ex. } M \in K \text{ s.d. } x \in M\}$$

die Vereinigung aller Mengen $M \in K$ (d.h. die Menge aller Elemente x, die in mindestens einer Menge $M \in K$ liegen).

Analog ist

$$\bigcap_{M \in K} M \quad := \quad \{x \in U \,:\, \text{f.a. } M \in K \text{ gilt } x \in M\}$$

der Durchschnitt aller Mengen $M \in K$ (d.h. die Menge aller Elemente x, die in jeder Menge $M \in K$ liegen).

Folie 51

Die Mächtigkeit von kartesischen Produkten

Satz 2.21.

(a) Seien A und B zwei endliche Mengen. Dann gilt:

$$|A \times B| \;=\; |A| \cdot |B|.$$

(b) Sei $k \in \mathbb{N}_{\geqslant 1}$ und seien $M_1, \ldots, M_k$ endliche Mengen. Dann gilt:

$$|M_1 \times \cdots \times M_k| \;=\; \prod_{i=1}^{k} |M_i|.$$

(c) Sei $k \in \mathbb{N}$ und sei M eine endliche Menge. Dann gilt:

$$\left|M^k\right| \;=\; |M|^k.$$

Beweis. (a) Es gilt:

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

Außerdem gilt für alle $a, a' \in A$ mit $a \neq a'$, dass die Mengen $\{a\} \times B$ und $\{a'\} \times B$ disjunkt sind. Ferner gilt für beliebige disjunkte endliche Mengen X und Y, dass $|X \cup Y| = |X| + |Y|$ ist. Insgesamt folgt daraus, dass

$$\begin{aligned} |A \times B| \;&=\; \left|\bigcup_{a \in A} (\{a\} \times B)\right| \;=\; \sum_{a \in A} |\{a\} \times B| \\ &=\; \sum_{a \in A} |B| \;=\; \underbrace{|B| + \cdots + |B|}_{|A|\text{-mal}} \;=\; |A| \cdot |B|. \end{aligned}$$

(b) Analog; Details: Übungsaufgabe.

(c) $\left|M^k\right| \;=\; \underbrace{|M \times \cdots \times M|}_{k\text{-mal}} \overset{\text{(b)}}{=} \prod_{i=1}^{k} |M| \;=\; \underbrace{|M| \cdot \cdots \cdot |M|}_{k\text{-mal}} \;=\; |M|^k.$

□

Folie 52

Bemerkung. Satz 2.21(c) besagt, dass

$$\left|M^k\right| \;=\; |M|^k \tag{2.1}$$

für jedes $k \in \mathbb{N}$ und jede endliche Menge M gilt.

Speziell für $M := \emptyset$ gilt:
$|M| = |\emptyset| = 0$. Aus Beispiel 2.19 wissen wir, dass $M^0 = \emptyset^0 = \{()\}$, also $|M^0| = |\emptyset^0| = 1$; und für alle $k \in \mathbb{N}$ mit $k \geqslant 1$ ist $M^k = \emptyset^k = \emptyset$, also $\left|\emptyset^k\right| = 0$.
Gemeinsam mit (2.1) rechtfertigt dies die Konvention, dass

$$0^0 \;=\; 1 \qquad \text{und} \qquad 0^k \;=\; 0 \quad \text{f.a. } k \in \mathbb{N} \text{ mit } k \geqslant 1.$$

Worte bzw. endliche Folgen

Folie 53

Bemerkung 2.22. Sei A eine Menge.

- Gelegentlich fassen wir ein Tupel $(a_1, \ldots, a_k) \in A^k$ als *Wort* auf, dessen „Buchstaben“ $a_1, \ldots, a_k$ sind. Um diese Sichtweise zu betonen, schreiben wir $a_1 \cdots a_k$ statt $(a_1, \ldots, a_k)$.

  Beispiel: Das Tupel $(\mathrm{S}, \mathrm{t}, \mathrm{r}, \mathrm{u}, \mathrm{k}, \mathrm{t}, \mathrm{u}, \mathrm{r})$ identifizieren wir mit dem Wort Struktur.

- A ist dann das *Alphabet*, über dem die Worte gebildet werden, und $a_1 \cdots a_k$ wird „Wort über A“ genannt.

- Das *leere Tupel* $() \in A^0$ heißt auch *leeres Wort* und wird oft als ε (epsilon, für „empty word“) bezeichnet.

- Die *Länge* eines Wortes $a_1 \cdots a_k$ ist die Zahl

  $$|a_1 \cdots a_k| \;:=\; k.$$

  Insbesondere ist $|\varepsilon| = 0$, d.h. das leere Wort hat die Länge 0.

- Sind $v = a_1 \cdots a_k$ und $w = b_1 \cdots b_\ell$ zwei Worte über A, so ist die *Konkatenation* von v und w das Wort

  $$vw \;:=\; a_1 \cdots a_k b_1 \cdots b_\ell.$$

- Manchmal wird ein Wort $a_1 \cdots a_k$ auch als *Folge* der Länge k aufgefasst.

Definition 2.23 (A^*, A^+, Sprache)**.**
Sei A ein Alphabet (d.h. eine Menge).

(a) Die *Menge aller Worte über A* (von beliebiger endlicher Länge) bezeichnen wir mit A^*. Es gilt also:

$$A^* \;=\; \bigcup_{k\in\mathbb{N}} A^k \;=\; \{\, a_1 \cdots a_k \,:\, k \in \mathbb{N},\, a_1, \ldots, a_k \in A \,\}.$$

Beachte: Wegen $0 \in \mathbb{N}$ und $A^0 = \{()\} = \{\varepsilon\}$ enthält A^* insbesondere das leere Wort.

(b) Die Menge aller *nicht-leeren* Worte über A (von beliebiger endlicher Länge) bezeichnen wir mit A^+. Es gilt:

$$A^+ \;=\; A^* \setminus \{\varepsilon\} \;=\; \{\, a_1 \cdots a_k \,:\, k \in \mathbb{N}_{\geqslant 1},\, a_1, \ldots, a_k \in A \,\}.$$

(c) Eine *Sprache* über A ist eine Teilmenge von A^*.

Bemerkung: In vielen Büchern werden Sprachen mit dem Buchstaben L (für *L*anguage) oder mit Varianten wie L' oder L_1 bezeichnet.

Beispiel 2.24 (Natürliche Sprachen)**.**
Wir betrachten das Alphabet

$$\begin{aligned} A_{deutsch} \;:=\; \{\; & \mathrm{A},\ \mathrm{B},\ \ldots,\ \mathrm{Z},\ \ddot{\mathrm{A}},\ \ddot{\mathrm{O}},\ \ddot{\mathrm{U}},\\ & \mathrm{a},\ \mathrm{b},\ \ldots,\ \mathrm{z},\ \ddot{\mathrm{a}},\ \ddot{\mathrm{o}},\ \ddot{\mathrm{u}},\ \ss,\\ & .,\ ,,\ :,\ ;,\ !,\ ?,\ \text{-},\ \_\ \}. \end{aligned}$$

Beispiele für Sprachen über $A_{deutsch}$ sind:

- $L_1 :=$ Menge aller grammatikalisch korrekten Sätze der, deutschen Sprache (aufgefasst als Zeichenketten über $A_{deutsch}$)
- $L_2 :=$ Menge aller Wörter der deutschen Sprache.

Folie 56

Beispiel 2.25 (Programmiersprachen)**.**
Wir betrachten das Alphabet

$$\text{ASCII} \;:=\; \text{die Menge aller ASCII-Symbole}$$

Beispiele für Sprachen über Alphabet ASCII sind:

- $L_1 :=$ die Menge aller JAVA-Schlüsselwörter,
- $L_2 :=$ die Menge aller erlaubten Variablennamen in JAVA,
- $L_3 :=$ die Menge aller syntaktisch korrekten JAVA-Programme.

Relationen

Folie 57

Relationen sind Teilmengen von kartesischen Produkten. Präzise:

Definition 2.26.

(a) Seien A, B Mengen. Eine *Relation* von A nach B ist eine Teilmenge von $A \times B$.

(b) Sei $k \in \mathbb{N}_{\geqslant 1}$ und seien $M_1, \ldots, M_k$ Mengen. Eine *Relation auf* $M_1, \ldots, M_k$ ist eine Teilmenge von $M_1 \times \cdots \times M_k$. Die *Stelligkeit* einer solchen Relation ist k.

(c) Sei M eine Menge und sei $k \in \mathbb{N}$. Eine *k-stellige Relation über M* ist eine Teilmenge von M^k.

Folie 58

Beispiel 2.27. Um Datumsangaben im Format (Tag, Monat, Jahr) anzugeben, nutzen wir die Wertebereiche

$$\begin{aligned} \text{TagWerte} &:= \{1, 2, \ldots, 31\} \\ \text{MonatsWerte} &:= \{1, 2, \ldots, 12\} \\ \text{JahresWerte} &:= \mathbb{Z}. \end{aligned}$$

Die Menge „Gültig“ aller *gültigen* Daten ist dann eine *Teilmenge* von

$$\text{TagWerte} \times \text{MonatsWerte} \times \text{JahresWerte},$$

d.h. eine *Relation* auf TagWerte, MonatsWerte, JahresWerte, zu der beispielsweise das Tupel $(23, 6, 1912)$ gehört,[1] nicht aber das Tupel $(30, 2, 1912)$.

Folie 59

Notation 2.28.

- Ist R eine Relation von A nach B (für zwei Mengen A, B), so schreiben wir oft
$$a\,R\,b \quad \text{statt} \quad (a, b) \in R.$$
Beispiel:
  - $a \leqslant b$, für natürliche Zahlen a und b
  - $a \neq b$, für ganze Zahlen a und b
- Ist R eine Relation auf $M_1, \ldots, M_k$, so schreiben wir manchmal
$$R(m_1, \ldots, m_k) \qquad \text{statt} \qquad (m_1, \ldots, m_k) \in R.$$
Das soll verdeutlichen, dass R eine „Eigenschaft“ ist, die ein Tupel aus $M_1 \times \cdots \times M_k$ haben kann — oder eben nicht haben kann. Im Datums-Beispiel gilt: Gültig$(23, 6, 1912)$, aber es gilt *nicht*: Gültig$(30, 2, 1912)$.

2.3 Funktionen

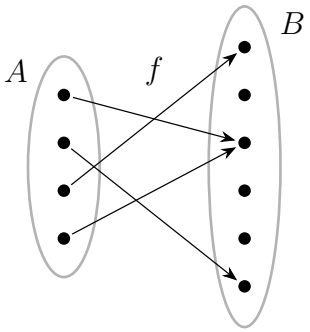
Totale Funktionen und partielle Funktionen

Folie 60

Definition 2.29. Seien A, B Mengen. Eine *Funktion* (oder *Abbildung*) von A nach B ist eine Relation f von A nach B (d.h. $f \subseteq A \times B$) mit der Eigenschaft, dass für jedes $a \in A$ *genau ein* $b \in B$ mit $(a, b) \in f$ existiert.

Anschaulich:

[1] Der 23. Juni 1912 ist der Geburtstag von *Alan M. Turing*, einem der einflussreichsten Pioniere der Informatik.



Folie 61

Notation 2.30.

(a) Wir schreiben $f : A \to B$, um auszudrücken, dass f eine Funktion von A nach B ist.

(b) Ist $f\colon A \to B$ und ist $a \in A$, so bezeichnet $f(a)$ das (eindeutig bestimmte) $b \in B$ mit $(a, b) \in f$. Insbesondere schreiben wir meistens $f(a) = b$ an Stelle von $(a, b) \in f$.

(c) Für $f\colon A \to B$ und $A' \subseteq A$ sei

$$f(A') \;:=\; \{\, f(a) \,:\, a \in A' \,\}.$$

(d) Die Menge aller Funktionen von A nach B bezeichnen wir mit $\mathrm{Abb}(A, B)$.

(e) In manchen Büchern wird $\mathrm{Abb}(A, B)$ auch mit B^A bezeichnet. Später, in Folgerung 2.39, werden wir sehen, dass für endliche Mengen A, B gilt:

$$|\mathrm{Abb}(A, B)| \;=\; |B|^{|A|}.$$

Folie 62

Definition 2.31.
Zwei Funktionen $f\colon A \to B$ und $g\colon A \to B$ sind *gleich* (kurz: $f = g$), falls f.a. $a \in A$ gilt: $f(a) = g(a)$.

Definition 2.32 (Definitionsbereich, Bildbereich, Bild)**.** Sei $f\colon A \to B$.

(a) Der *Definitionsbereich* von f ist die Menge $\mathrm{Def}(f) := A$.

(b) Der *Bildbereich* von f ist die Menge B.

(c) Das *Bild* von f (genauer: das Bild von A unter f) ist die Menge

$$\text{Bild}(f) \;:=\; f(A) \;=\; \{\, f(a) \,:\, a \in A \,\} \;\subseteq\; B.$$

Definition 2.33 (Restriktionen)**.**
Sei $f\colon A \to B$ eine Funktion und sei $A' \subseteq A$. Die *Restriktion* (oder *Einschränkung*) von f auf A' ist die Funktion

$$f|_{A'} \;:\; A' \to B,$$

die folgendermaßen definiert ist: f.a. $a \in A'$ ist $f|_{A'}(a) := f(a)$.

Folie 63

Definition 2.34.
Eine *partielle Funktion* von einer Menge A in eine Menge B ist eine Funktion f mit $\text{Def}(f) \subseteq A$ und $\text{Bild}(f) \subseteq B$.

Bemerkung 2.35.

(a) Im Gegensatz zu partiellen Funktionen nennt man Funktionen, wie wir sie in Definition 2.29 definiert haben, auch *totale Funktionen*.

Sprechen wir von „Funktionen“, ohne sie explizit als „partiell“ zu bezeichnen, so meinen wir in dieser Vorlesung immer „totale“ Funktionen.

(b) Jede partielle Funktion von einer Menge A in eine Menge B lässt sich auch als totale Funktion von A nach $B \,\dot\cup\, \{\perp\}$ auffassen, wobei $\perp$ ein spezielles Zeichen ist, das für „undefiniert“ steht, und das nicht zur Menge B gehört.

Eigenschaften von Funktionen

Folie 64

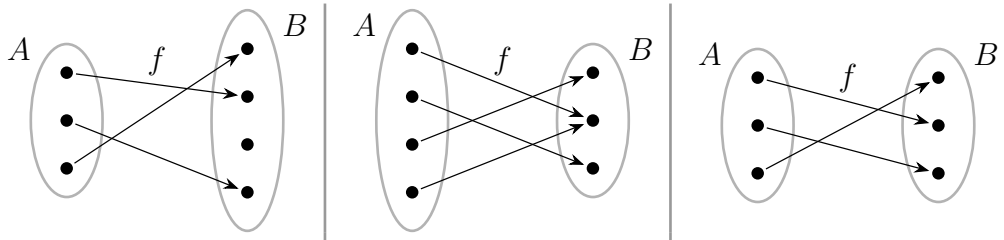
Definition 2.36. Sei $f\colon A \to B$.

(a) f heißt *injektiv*, falls es für jedes $b \in B$ höchstens ein $a \in A$ mit $f(a) = b$ gibt.

(b) f heißt *surjektiv*, falls es für jedes $b \in B$ mindestens ein $a \in A$ mit $f(a) = b$ gibt.

(c) f heißt *bijektiv*, falls es für jedes $b \in B$ genau ein $a \in A$ mit $f(a) = b$ gibt.

Anschaulich:



injektiv, nicht surjektiv, nicht bijektiv,

nicht injektiv, surjektiv, nicht bijektiv,

injektiv, surjektiv bijektiv

Beobachtung 2.37.

(a) Für jede Funktion $f\colon A \to B$ gilt:

$$f \text{ ist bijektiv} \iff f \text{ ist injektiv und surjektiv.}$$

(b) Seien A und B endliche Mengen. Dann gilt:

$$|A| = |B| \iff \text{es gibt eine bijektive Funktion von } A \text{ nach } B.$$

Folie 65

Satz 2.38.

(a) Für jede Menge M gibt es eine bijektive Funktion von $\mathcal{P}(M)$ nach $\mathrm{Abb}(M, \{0,1\})$.

(b) Sei B eine Menge, sei A eine endliche Menge und sei $k := |A|$. Dann gibt es eine bijektive Funktion von $\mathrm{Abb}(A, B)$ *nach B^k.*

Beweis. (a) Repräsentiere jedes $Z \in \mathcal{P}(M)$ (d.h. $Z \subseteq M$) durch die so genannte *charakteristische Funktion* $\chi_Z\colon M \to \{0,1\}$ mit

$$\chi_Z(m) \;:=\; \begin{cases} 1, & \text{falls } m \in Z \\ 0, & \text{sonst.} \end{cases} \qquad (*)$$

Sei nun $f\colon \mathcal{P}(M) \to \mathrm{Abb}(M, \{0,1\})$ definiert durch

$$f(Z) \;:=\; \chi_Z, \quad \text{für jedes } Z \in \mathcal{P}(M). \qquad (**)$$

Behauptung. f ist bijektiv.

Wir zeigen dies in 2 Schritten (und nutzen Beobachtung 2.37(a)).

Schritt 1: f ist injektiv:

Seien $Z, Z' \in \mathcal{P}(M)$ mit $f(Z) = f(Z')$.

Ziel: Zeige, dass $Z = Z'$.

Wegen $f(Z) = f(Z')$ gilt gemäß $(**)$, dass $\chi_Z = \chi_{Z'}$. D.h. f.a. $m \in M$ gilt $\chi_Z(m) = \chi_{Z'}(m)$. Gemäß $(*)$ gilt daher f.a. $m \in M$, dass

$$m \in Z \iff m \in Z'.$$

Somit ist $Z = Z'$.

Schritt 2: f ist surjektiv:

Sei $h \in \text{Abb}(M, \{0,1\})$, d.h. $h\colon M \to \{0,1\}$.

Ziel: Finde ein $Z \in \mathcal{P}(M)$ mit $f(Z) = h$.

Wir wählen

$$Z \;:=\; \{m \in M \,:\, h(m) = 1\}.$$

Dann ist klar: $Z \in \mathcal{P}(M)$. Gemäß $(*)$ gilt $\chi_Z = h$. Gemäß $(**)$ ist daher $f(Z) = h$.

(b) *Idee:* Sei $a_1, \ldots, a_k$ eine Liste aller Elemente in A. Repräsentiere jede Funktion $h \in \text{Abb}(A, B)$ durch das k-Tupel $t_h := \big(h(a_1), \ldots, h(a_k)\big)$.

Rest: Übungsaufgabe.

□

Folie 66

Folgerung 2.39. *Seien A, B, M endliche Mengen. Dann gilt:*

(a) $|\text{Abb}(A, B)| = |B|^{|A|}$.

(b) $|\mathcal{P}(M)| = 2^{|M|}$.

Beweis. (a) Gemäß Satz 2.38(b) und Beobachtung 2.37(b) gilt für $k := |A|$, dass

$$|\text{Abb}(A, B)| \;=\; \big|B^k\big|.$$

Laut Satz 2.21(c) ist $\big|B^k\big| = |B|^k$. Somit $|\text{Abb}(A, B)| = |B|^k = |B|^{|A|}$.

(b) Gemäß Satz 2.38(a) und Beobachtung 2.37(b) ist

$$|\mathcal{P}(M)| \;=\; |\mathrm{Abb}(M, \{0,1\})|.$$

Gemäß (a) ist

$$|\mathrm{Abb}(M, \{0,1\})| \;=\; |\{0,1\}|^{|M|} \;=\; 2^{|M|}.$$

□

Spezielle Funktionen

Folie 67

Definition 2.40. Die *Identitätsfunktion* auf einer Menge M ist die Funktion

$$\mathrm{id}_M \colon M \to M$$

mit $\mathrm{id}_M(m) := m$, f.a. $m \in M$.

Definition 2.41. Eine *Permutation* einer Menge M ist eine *bijektive* Funktion $f : M \to M$.

Definition 2.42. Eine *Multimenge* (engl.: *bag*) über einer Menge M ist eine Funktion $f \colon M \to \mathbb{N}$.

Mit solchen Multimengen kann man „Mengen“ beschreiben, in denen einzelne Elemente mehrfach vorkommen können: Für jedes $m \in M$ gibt $f(m)$ an, wie oft m in der Multimenge vorkommt.

Folie 68

Beispiel 2.43. Ein Geldbeutel mit

- 3 1-Cent-Münzen
- 2 10-Cent-Münzen
- 4 20-Cent-Münzen
- 1 50-Cent-Münzen
- 3 1-Euro-Münzen
- 2 2-Euro-Münzen

kann repräsentiert werden durch die Multimenge

$$\text{Geldbeutelinhalt} : \text{MünzenArten} \to \mathbb{N},$$

wobei

$$\text{MünzenArten} := \{1\text{c}, 2\text{c}, 5\text{c}, 10\text{c}, 20\text{c}, 50\text{c}, 1€, 2€\}$$

und

$$\begin{array}{lcl} \text{Geldbeutelinhalt}(1\text{c}) & := & 3 \\ \text{Geldbeutelinhalt}(2\text{c}) & := & 0 \\ \text{Geldbeutelinhalt}(5\text{c}) & := & 0 \\ \text{Geldbeutelinhalt}(10\text{c}) & := & 2 \\ \text{Geldbeutelinhalt}(20\text{c}) & := & 4 \\ \text{Geldbeutelinhalt}(50\text{c}) & := & 1 \\ \text{Geldbeutelinhalt}(1€) & := & 3 \\ \text{Geldbeutelinhalt}(2€) & := & 2. \end{array}$$

Bequemere Schreibweise (die konsistent ist mit Definition 2.29):

$$\begin{array}{lcl} \text{Geldbeutelinhalt} & := & \{\ (1\text{c}, 3),\ (2\text{c}, 0),\ (5\text{c}, 0),\ (10\text{c}, 2), \\ & & \quad (20\text{c}, 4),\ (50\text{c}, 1),\ (1€, 3),\ (2€, 2)\ \}\ . \end{array}$$

2.4 Beweise verstehen und selbst formulieren

Folie 69

Ziel dieses Abschnitts ist, einen kurzen Überblick über grundlegende Beweistechniken zu geben, insbesondere:

- direkter Beweis
- Beweis durch Kontraposition
- Beweis durch Widerspruch (indirekter Beweis)
- vollständige Induktion.

Nebenbei werden wir einige interessante mathematische Aussagen beweisen, die es sich zu merken lohnt.

Folie 70

Was sind *Sätze* und *Beweise*?

Ein *Satz* (bzw. *Theorem*) ist eine formale Aussage, die man sich merken sollte. Sie besteht aus Voraussetzungen und einer Behauptung. Voraussetzungen und Behauptung sind Aussagen, so dass Folgendes gilt: Wenn alle Voraussetzungen erfüllt sind, dann muss auch die Behauptung wahr sein.

Der *Beweis* eines Satzes muss nachweisen, dass die Behauptung des Satzes wahr ist und kann dabei verwenden:

- die Voraussetzungen des Satzes,
- Definitionen und bereits bekannte Tatsachen und Sätze,
- im Beweis selbst oder anderswo bereits als wahr bewiesene Aussagen,
- logische Schlussregeln.

Folie 71

Typische Fehler, die man beim Versuch, Beweise zu formulieren, *vermeiden* sollte, sind:

- unzulässiges Argumentieren mit Beispielen,
- Verwendung gleicher Symbole zur Bezeichnung verschiedener Dinge,
- Hantieren mit nicht exakt oder gar widersprüchlich definierten Begriffsbildungen,
- unzulässige Gedankensprünge beim Schlussfolgern,
- Ausnutzung von bis dahin noch unbewiesenen Behauptungen zur Begründung von einzelnen Beweisschritten.

Folie 72

Die Begriffe *Definition*, *Lemma*, *Korollar*, *Folgerung* und *Proposition*

Eine *Definition* führt einen neuen Begriff ein und legt dessen Bedeutung fest.

Ein *Lemma* (Plural: Lemmas oder Lemmata) ist so etwas ähnliches wie ein Satz. Es bezeichnet meistens einen „technischen Hilfssatz“, dessen Aussage

man sich nicht unbedingt dauerhaft merken muss, die aber nützlich ist, um ein Theorem zu beweisen.

Ein *Korollar* (bzw. eine *Folgerung*) ist eine formale Aussage (ähnlich wie ein Satz), die man sich merken sollte, und deren Beweis relativ leicht aus einem bereits vorher bewiesenen Sachverhalt folgt.

Eine *Proposition* ist eine formale Aussage (ähnlich wie ein Satz oder ein Lemma). Der Begriff wird auf unterschiedliche Art verwendet — manchmal, um eine Aussage zu bezeichnen, die man sich merken sollte und die ganz leicht zu beweisen ist; und manchmal um einen „technischen Hilfssatz“ zu bezeichnen, der schwer zu beweisen ist, den man sich aber nicht unbedingt merken muss.

Beweistechnik „direkter Beweis“

Folie 73

Bei einem *direkten Beweis* wird die Behauptung eines Satzes „direkt“, d.h. ohne „Umwege“, bewiesen.

Beispiele für direkte Beweise haben wir bereits kennengelernt, z.B. den Beweis von Satz 2.6, den Beweis von Satz 2.21, den Beweis von Satz 2.38, den Beweis von Folgerung 2.39.

Es folgt ein weiteres Beispiel für einen direkten Beweis.

Folie 74

Gaußsche Summenformel

Satz 2.44. *Für alle $n \in \mathbb{N}$ gilt:* $\displaystyle\sum_{i=0}^{n} i \;=\; \frac{n \cdot (n+1)}{2}$.

Beweis. Sei $n \in \mathbb{N}$ beliebig. Es gilt:

$$\begin{aligned} 2 \cdot \sum_{i=0}^{n} i \;&=\; \sum_{i=0}^{n} i \;+\; \sum_{j=0}^{n} j \;=\; \sum_{i=0}^{n} i \;+\; \sum_{i=0}^{n} (n-i) \\ &=\; \sum_{i=0}^{n} \big(i + (n-i)\big) \;=\; \sum_{i=0}^{n} n \;=\; n \cdot (n+1)\,. \end{aligned}$$

Es gilt also:

$$2 \cdot \sum_{i=0}^{n} \;=\; n \cdot (n+1)\;.$$

Somit gilt:

$$\sum_{i=0}^{n} \quad = \quad \frac{n \cdot (n+1)}{2} \ .$$

□

Beweistechnik „Beweis durch Kontraposition“

Folie 75

Man beachte, dass für beliebige Aussagen A und B das Folgende gilt:

die folgende Aussage ist wahr:
„Falls Aussage A gilt, so gilt auch Aussage B“

$\iff$ Aussage B gilt oder Aussage A gilt nicht

$\iff$ die folgende Aussage ist wahr:
„Falls Aussage B *nicht* gilt, so gilt auch Aussage A *nicht*.“

Beim *Beweis durch Kontraposition* wird ein Satz der Form

„Falls Aussage A gilt, so gilt auch Aussage B“

dadurch bewiesen, dass man zeigt:

„Falls Aussage B *nicht* gilt, so kann auch Aussage A *nicht* gelten.“

Folie 76

Als Beispiel für einen Beweis durch Kontraposition betrachten wir den folgenden Satz.

Definition 2.45. Eine *gerade* Zahl ist eine Zahl z, für die gilt: es gibt ein $y \in \mathbb{Z}$ so dass $z = 2 \cdot y$ ist. Eine *ungerade* Zahl ist eine Zahl $z \in \mathbb{Z}$, die nicht gerade ist.

Satz 2.46.
Für jedes $n \in \mathbb{N}$ gilt: Falls n^2 eine ungerade Zahl ist, so ist auch n eine ungerade Zahl.

Beweis. Durch Kontraposition. Sei $n \in \mathbb{N}$ beliebig.

Wir zeigen: Falls n *keine* ungerade Zahl ist, so ist auch n^2 *keine* ungerade Zahl.

$n \in \mathbb{N}$ war beliebig gewählt. Falls n ungerade ist, so ist nichts weiter zu beweisen. Wir betrachten daher nur den Fall, dass n *keine* ungerade Zahl ist (d.h. n ist gerade). Wir müssen zeigen, dass dann auch n^2 *keine* ungerade Zahl ist (d.h. n^2 ist eine gerade Zahl).

Es gilt:

$$\begin{aligned} n \text{ ist gerade} &\implies \text{es ex. } y \in \mathbb{Z} \text{ s.d. } n = 2 \cdot y \quad \text{(gemäß Def. 2.45)} \\ &\implies \text{es ex. } y \in \mathbb{Z} \text{ s.d. } n^2 = n \cdot (2 \cdot y) \\ &\implies \text{es ex. } y \in \mathbb{Z} \text{ s.d. } n^2 = 2 \cdot (n \cdot y) \\ &\implies \text{es ex. } y' \in \mathbb{Z} \text{ s.d. } n^2 = 2 \cdot y' \\ &\implies n^2 \text{ ist gerade} \quad \text{(gemäß Def. 2.45).} \end{aligned}$$

Somit ist n^2 gerade, d.h. n^2 ist keine ungerade Zahl. □

Beweistechnik Beweis durch Widerspruch *(indirekter Beweis)*

Folie 77

Beim *Beweis durch Widerspruch* wird ein Satz der Form

„Falls die Voraussetzungen A erfüllt sind, so gilt Aussage B“

dadurch bewiesen, dass man

- annimmt, dass die Voraussetzungen A erfüllt sind, aber die Aussage B *nicht* gilt und
- daraus einen Widerspruch herleitet.

Als Beispiel für einen Beweis durch Widerspruch betrachten wir folgenden Satz:

Satz 2.47. *Für alle geraden natürlichen Zahlen a und b gilt: $a \cdot b$ ist gerade.*

Beweis. Durch Widerspruch.
Angenommen, a und b sind gerade natürlichen Zahlen, so dass $a \cdot b$ *nicht* gerade ist.
Da a und b gerade sind, gibt es $k, \ell \in \mathbb{Z}$ s.d. $a = 2 \cdot k$ und $b = 2 \cdot \ell$.
Dann ist $a \cdot b = (2 \cdot k) \cdot (2 \cdot \ell)$. Insbesondere gibt es also ein $m \in \mathbb{Z}$, s.d. $a \cdot b = 2 \cdot m$ (nämlich $m = 2 \cdot k \cdot \ell$).
Gemäß Definition 2.45 ist also $a \cdot b$ gerade. Dies ist ein Widerspruch zur Annahme, dass $a \cdot b$ *nicht* gerade ist. □

Ein weiteres, etwas anspruchsvolleres Beispiel für einen Beweis durch Widerspruch ist der Beweis des folgenden Satzes, der „anschaulich“ besagt, dass die Potenzmenge von $\mathbb{N}$ *viel* größer ist als die Menge $\mathbb{N}$ selbst.

Satz 2.48 („$\mathcal{P}(\mathbb{N})$ ist nicht abzählbar“)**.**
Es gibt keine surjektive Funktion von $\mathbb{N}$ *nach* $\mathcal{P}(\mathbb{N})$.

Beweis. Durch Widerspruch. Angenommen, $f\colon \mathbb{N} \to \mathcal{P}(\mathbb{N})$ ist surjektiv. Sei

$$X \;:=\; \{\, n \in \mathbb{N} \,:\, n \notin f(n) \,\}. \qquad (*)$$

Klar: $X \in \mathcal{P}(\mathbb{N})$.

Da f surjektiv ist, muss es ein $m \in \mathbb{N}$ geben mit $f(m) = X$.
Klar: Entweder gilt $m \in X$ oder es gilt $m \notin X$.

Fall 1: $m \notin X$*:*
Wegen $f(m) = X$ gilt also $m \notin f(m)$.
Gemäß (*) für $n := m$ folgt, dass $m \in X$. $\lightning$ (Widerspruch zu „Fall 1: $m \notin X$“).

Fall 2: $m \in X$*:*
Wegen $f(m) = X$ gilt also: $m \in f(m)$.
Gemäß (*) für $n := m$ folgt, dass $m \notin X$. $\lightning$ (Widerspruch zu „Fall 2: $m \in X$“).

Somit führen beide Fälle zu einem Widerspruch. Daher muss unsere Annahme, dass es eine surjektive Funktion f von $\mathbb{N}$ nach $\mathcal{P}(\mathbb{N})$ gibt, falsch gewesen sein. □

Cantors zweites Diagonalargument

Bemerkung 2.49.
Die in diesem Beweis verwendete Technik ist unter dem Namen *Diagonalisierung* (oder *Cantors zweites Diagonalargument*) bekannt.

Die Grundidee des obigen Beweises lässt sich nämlich folgendermaßen veranschaulichen: Eine Funktion $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ können wir durch folgende

Tabelle repräsentieren

	0	**1**	**2**	**3**	**4**	**5**	$\cdots$
0	$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$\cdots$
1	$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$\cdots$
2	$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$\cdots$
3	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$	$\cdots$
4	$a_{4,0}$	$a_{4,1}$	$a_{4,2}$	$a_{4,3}$	$a_{4,4}$	$a_{4,5}$	$\cdots$
5	$a_{5,0}$	$a_{5,1}$	$a_{5,2}$	$a_{5,3}$	$a_{5,4}$	$a_{5,5}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

wobei der Eintrag $a_{i,j}$ in Zeile i und Spalte j folgendermaßen gewählt ist:

$$a_{i,j} \;:=\; \begin{cases} 1 & \text{falls } j \in f(i) \\ 0 & \text{falls } j \notin f(i). \end{cases}$$

Folie 80

Somit repräsentiert jede Zeile i dieser Tabelle die Menge $f(i)$, und es gilt

$$f(i) \;=\; \{\, j \in \mathbb{N} \,:\, a_{i,j} = 1 \,\}.$$

Wir wählen nun die Folge

$$b_0 \;\; b_1 \;\; b_2 \;\; b_3 \;\; b_4 \;\; b_5 \;\; \cdots$$

so, dass sich, für jedes $j \in \mathbb{N}$, der Wert b_j von dem Eintrag $a_{j,j}$ in der Diagonalen der Tabelle unterscheidet. D.h., wir wählen

$$b_j \;:=\; \begin{cases} 0 & \text{falls } a_{j,j} = 1 \\ 1 & \text{falls } a_{j,j} = 0, \end{cases}$$

für alle $j \in \mathbb{N}$.
Anhand dieser Wahl von $b_0, b_1, b_2, \ldots$ wissen wir, dass diese Folge in keiner Zeile der Tabelle stehen kann, denn für jede Zeile i unterscheidet sich der in Spalte i stehende Wert $a_{i,i}$ vom Wert b_i. Somit gilt für die Menge

$$X \;:=\; \{\, j \in \mathbb{N} \,:\, b_j = 1 \,\},$$

dass X nicht im Bild der Funktion f liegen kann, und dass f daher nicht surjektiv sein kann.

Folie 81

Man kann sich leicht davon überzeugen, dass die hier gewählte Menge X mit der im Beweis von Satz 2.48 gewählten Menge X übereinstimmt, denn

$$\begin{aligned} X &= \{ j \in \mathbb{N} : b_j = 1 \} &&= \{ j \in \mathbb{N} : a_{j,j} = 0 \} \\ &= \{ j \in \mathbb{N} : j \notin f(j) \} &&= \{ n \in \mathbb{N} : n \notin f(n) \}. \end{aligned}$$

Folie 82

Ein weiteres, sehr ähnliches Beispiel für einen Beweis durch Widerspruch haben wir bereits im Zusammenhang mit der Russellschen Antinomie kennengelernt:

Satz 2.50 („Es gibt keine Menge aller Mengen“)**.**
Es gibt keine Menge U, so dass für jede Menge M gilt: $M \in U$.

Folie 83

Beweis. Durch Widerspruch. Angenommen, U ist eine Menge, so dass für jede Menge M gilt: $M \in U$. Dann ist auch

$$X := \{M \in U : M \text{ ist eine Menge und } M \notin M\} \qquad (*)$$

eine Menge. Insbesondere gilt entweder $X \in X$ oder $X \notin X$.

Fall 1: $X \notin X$:
Wir wissen: X ist eine Menge, also insbesondere $X \in U$.
Da wir in Fall 1 sind, gilt außerdem: $X \notin X$.
Gemäß (*) (für $M := X$) muss dann aber gelten: $X \in X$. $\lightning$ (Widerspruch zu „Fall 1: $X \notin X$“).

Fall 2: $X \in X$:
Wegen $X \in X$ gilt gemäß (*) für $M := X$, dass $X \in U$ ist, dass X eine Menge ist, und dass $X \notin X$ ist. $\lightning$ (Widerspruch zu „Fall 2: $X \in X$“).

Somit führen beide Fälle zu einem Widerspruch. Daher kann es keine Menge U geben, so dass für jede Menge M gilt: $M \in U$. □

Folie 84

Bemerkung 2.51. Jede Aussage, die durch einen *Beweis durch Kontraposition* bewiesen werden kann, kann auch durch einen *Beweis durch Widerspruch* nachgewiesen werden.
Um zu zeigen, dass die Aussage

„Falls Aussage A gilt, so gilt auch Aussage B“

wahr ist, kann man in einem Beweis durch Widerspruch folgendermaßen vorgehen: Man nimmt an, dass Aussage A gilt und Aussage B nicht gilt und leitet aus dieser Annahme dann einen Widerspruch her.

Übungsaufgabe: Beweisen Sie Satz 2.46 durch einen „Beweis durch Widerspruch“.

Beweistechnik „Beweis durch vollständige Induktion“

Folie 85

Das Induktionsprinzip

Um die Grundidee der vollständigen Induktion zu erklären, sei $A(n)$ eine Aussage über die natürliche Zahl n. Das Ziel ist, zu zeigen, dass die Aussage $A(n)$ für jedes $n \in \mathbb{N}$ wahr ist.

Eine Möglichkeit, dies zu zeigen ist, sich das so genannte *Induktionsprinzip* zu Nutze zu machen: Man zeigt, dass eine Aussage $A(n)$ für alle $n \in \mathbb{N}$ wahr ist, indem man folgendermaßen vorgeht.

(1) Zuerst zeigt man, dass die Aussage $A(n)$ für die Zahl $n = 0$ gilt. Diesen Schritt nennt man *Induktionsanfang* bzw. Induktionsbasis.

(2) Danach zeigt man, dass für jede beliebige natürliche Zahl $n \in \mathbb{N}$ gilt: Falls die Aussage $A(n)$ wahr ist, so ist auch die Aussage $A(n{+}1)$ wahr. Diesen Schritt nennt man *Induktionsschritt*.

Folie 86

Beachte.
Wenn man die Schritte (1) und (2) bewiesen hat, so weiß man, dass die folgenden Aussagen wahr sind:

(i) $A(0)$ ist wahr gemäß Schritt (1).

(ii) $A(1)$ ist wahr gemäß (i) und Schritt (2) für $n = 0$,

(iii) $A(2)$ ist wahr gemäß (ii) und Schritt (2) für $n = 1$,

(iv) $A(3)$ ist wahr gemäß (iii) und Schritt (2) für $n = 2$,

(v) $A(4)$ ist wahr gemäß (iv) und Schritt (2) für $n = 3$,

(vi) $A(5)$ ist wahr gemäß (v) und Schritt (2) für $n = 4$,

(vii) usw.

Insgesamt hat man damit gezeigt, dass *für alle* $n \in \mathbb{N}$ die Aussage $A(n)$ wahr ist.

Folie 87

Als Beispiel für einen Beweis durch vollständige Induktion betrachten wir den folgenden Satz:

Satz 2.52. *F.a.* $n \in \mathbb{N}$ *gilt:*

$$\sum_{i=0}^{n} 2^i \quad = \quad 2^{n+1} - 1\,.$$

Beweis. Per Induktion nach n.
Die „Aussage $A(n)$“, deren Gültigkeit hier f.a. $n \in \mathbb{N}$ bewiesen werden soll, besagt:

$$\sum_{i=0}^{n} 2^i \quad = \quad 2^{n+1} - 1.$$

Induktionsanfang: $n = 0$

Behauptung: $\sum_{i=0}^{0} 2^i \;=\; 2^{0+1} - 1.$

Beweis:

Es gilt: $\sum_{i=0}^{0} 2^i \;=\; 2^0 \;=\; 1.$

Außerdem gilt: $2^{0+1} - 1 \;=\; 2^1 - 1 \;=\; 2 - 1 \;=\; 1.$

Somit: $\sum_{i=0}^{0} 2^i \;=\; 1 \;=\; 2^{0+1} - 1.$

Induktionsschritt: $n \to n + 1$

Sei $n \in \mathbb{N}$ beliebig.

Induktionsannahme: $\sum_{i=0}^{n} 2^i \;=\; 2^{n+1} - 1$

(D.h. wir gehen davon aus, dass die Aussage $A(n)$ wahr ist.)

Behauptung: $\sum_{i=0}^{n+1} 2^i \;=\; 2^{(n+1)+1} - 1$

(D.h. wir müssen zeigen, dass dann auch die Aussage $A(n{+}1)$ wahr ist.)

Beweis:

$$\begin{aligned}\sum_{i=0}^{n+1} 2^i &\overset{\text{Not.2.20}}{=} \left(\sum_{i=0}^{n} 2^i\right) + 2^{n+1} \\ &\overset{\text{Ind.ann.}}{=} (2^{n+1} - 1) + 2^{n+1} \\ &= 2 \cdot 2^{n+1} - 1 \\ &= 2^{(n+1)+1} - 1.\end{aligned}$$

□

Folie 88

Zwei nützliche Varianten des Induktionsprinzips

Um zu zeigen, dass eine Aussage $A(n)$ für alle $n \in \mathbb{N}$ mit $n \geqslant n_0$ wahr ist (wobei n_0 eine geeignete natürliche Zahl ist), kann man nach einem der beiden folgenden Schemata vorgehen:

Variante 1:

Induktionsanfang: $n = n_0$
Behauptung: Die Aussage $A(n_0)$ ist wahr.
Beweis: ...

Induktionsschritt: $n \to n{+}1$
Sei $n \in \mathbb{N}$ mit $n \geqslant n_0$ beliebig.
Induktionsannahme: Die Aussage $A(n)$ ist wahr.
Behauptung: Die Aussage $A(n{+}1)$ ist wahr.
Beweis: ...

Folie 89

Variante 2:

Induktionsanfang: $n = n_0$
Behauptung: Die Aussage $A(n_0)$ ist wahr.
Beweis: ...

Induktionsschritt: $n \to n{+}1$
Sei $n \in \mathbb{N}$ mit $n \geqslant n_0$ beliebig.
Induktionsannahme: Für jede natürliche Zahl i mit $n_0 \leqslant i \leqslant n$ ist die Aussage $A(i)$ wahr.
Behauptung: Die Aussage $A(n{+}1)$ ist wahr.
Beweis: ...

Beispiel 2.53.
Wir nutzen Variante 1, um die folgende Frage zu beantworten: Welche der Funktionen $f\colon \mathbb{N} \to \mathbb{Z}$ und $g\colon \mathbb{N} \to \mathbb{Z}$ mit $f(n) := n^2 - 7$ und $g(n) := 4 \cdot n$ (f.a. $n \in \mathbb{N}$) liefert größere Funktionswerte?

Um eine Vermutung darüber zu bekommen, welche der beiden Funktionen die größeren Werte liefert, stellen wir zunächst eine Tabelle auf, die die Funktionswerte für $n = 0$, $n = 1$, $n = 2$, etc. enthält:

n	0	1	2	3	4	5	6	7	8	9
$f(n)$	-7	-6	-3	2	9	18	29	42	57	74
$g(n)$	0	4	8	12	16	20	24	28	32	36

Anhand dieser Tabelle drängt sich die Vermutung auf, dass f.a. $n \in \mathbb{N}$ mit $n \geqslant 6$ gilt: $f(n) > g(n)$. Die Korrektheit dieser Vermutung weisen wir im Folgenden per Induktion nach n nach.

INDUKTIONSANFANG: $n = 6$
Behauptung: $f(6) > g(6)$
Beweis:
Es gilt: $f(6) = 6^2 - 7 = 29$.
Außerdem gilt: $g(6) = 4 \cdot 6 = 24$.
Also: $f(6) = 29 > 24 = g(6)$.

INDUKTIONSSCHRITT: $n \to n{+}1$
Sei $n \in \mathbb{N}$ mit $n \geqslant 6$ beliebig.
Induktionsannahme: $f(n) > g(n)$, d.h. $n^2 - 7 > 4 \cdot n$.
Behauptung: $f(n+1) > g(n+1)$, d.h. $(n+1)^2 - 7 > 4 \cdot (n+1)$.
Beweis:

$$\begin{aligned}
(n+1)^2 - 7 &= n^2 + 2n + 1 - 7 \\
&= (n^2 - 7) + 2n + 1 \\
&\overset{\text{Ind.ann}}{>} 4n + 2n + 1 \\
&\overset{n \geqslant 6,\ \text{also } 2n+1 \geqslant 13 > 4}{\geqslant} 4n + 4 \\
&= 4(n{+}1).
\end{aligned}$$

Insgesamt haben wir damit bewiesen, dass f.a. $n \in \mathbb{N}$ mit $n \geqslant 6$ gilt: $f(n) > g(n)$.

□Ende Beispiel 2.53

Auf ähnliche Weise kann man per Induktion auch Folgendes beweisen:

Satz 2.54.

(a) *F.a.* $n \in \mathbb{N}$ *mit* $n \geqslant 1$ *gilt:* $\sum_{i=1}^{n}(2i-1) = n^2$

(d.h. die Summe der ersten n *ungeraden Zahlen ergibt gerade die Zahl* n^2*).*

(b) *F.a.* $n \in \mathbb{N}$ *mit* $n \geqslant 1$ *gilt:* $\sum_{i=1}^{n} i = \frac{n\cdot(n+1)}{2}$.

(c) *F.a.* $n \in \mathbb{N}$ *mit* $n \geqslant 1$ *gilt:* $\sum_{i=1}^{n} i^2 = \frac{n\cdot(n+1)\cdot(2n+1)}{6}$.

(d) *F.a.* $n \in \mathbb{N}$ *gilt:* $2^n > n$.

Beweis. Übungsaufgabe. □

Das folgende Beispiel zeigt, dass man beim Führen von Induktionsbeweisen sehr sorgfältig sein muss:

Beispiel 2.55.
Der folgende Satz ist offensichtlich nicht wahr — aber wo steckt der Fehler im Beweis?

„Satz“: *F.a.* $n \in \mathbb{N}$ *mit* $n \geqslant 1$ *gilt: Ist* M *eine Menge von Menschen mit* $|M| = n$*, so haben alle Menschen in* M *die gleiche Größe.*

„Beweis“: Per Induktion nach n.

Induktionsanfang: $n = 1$

Behauptung: Ist M eine Menge von Menschen mit $|M| = 1$, so haben alle Menschen in M die gleiche Größe.

Beweis: Sei M eine Menge von Menschen mit $|M| = 1$. D.h. M besteht aus genau einem Menschen. Daher haben offensichtlich alle Menschen in M die gleiche Größe.

Induktionsschritt: $n \to n+1$

Sei $n \in \mathbb{N}$ mit $n \geqslant 1$ beliebig.

Induktionsannahme: Ist M' eine Menge von Menschen mit $|M'| = n$, so haben alle Menschen in M' die gleiche Größe.

Behauptung: Ist M eine Menge von Menschen mit $|M| = n{+}1$, so haben alle Menschen in M die gleiche Größe.

Beweis: Sei M eine Menge von Menschen mit $|M| = n{+}1$. Sei $a_1, a_2, \ldots, a_n, a_{n+1}$ eine Liste aller Menschen in M, d.h. $M = \{a_1, a_2, \ldots, a_n, a_{n+1}\}$. Sei

$$M' \;:=\; \{a_1, a_2, \ldots, a_n\} \quad \text{und} \quad M'' \;:=\; \{a_2, \ldots, a_n, a_{n+1}\}.$$

Offensichtlich sind M' und M'' Mengen von Menschen mit $|M'| = n$ und $|M''| = n$. Gemäß der Induktionsannahme gilt daher:

(1) Alle Menschen in M' haben die gleiche Größe, und

(2) alle Menschen in M'' haben die gleiche Größe.

Sei g' die Größe, die gemäß (1) jeder Mensch in M' hat, und sei g'' die Größe, die gemäß (2) jeder Mensch in M'' hat. Laut Definition von M' und M'' gilt: $a_2 \in M'$ und $a_2 \in M''$. Da jeder einzelne Mensch (und daher insbes. der Mensch a_2) nur *eine* Größe haben kann, gilt: $g' = g''$. Wegen $M = M' \cup M''$ gilt daher, dass alle Menschen in M die gleiche Größe haben, nämlich die Größe $g := g' = g''$. □

Frage. Wo steckt der Fehler im Beweis? □Ende Beispiel 2.55

2.5 Rekursive Definition von Funktionen und Mengen

Folie 93

Rekursive Definitionen von Funktionen

Das Induktionsprinzip lässt sich auch zur „induktiven“ (bzw. „rekursiven“) Definition von Funktionen $f\colon \mathbb{N} \to M$ (wobei M eine beliebige Menge ist) nutzen, indem man folgendermaßen vorgeht:

(1) Definiere $f(0)$.
Diesen Schritt bezeichnet man als *Rekursionsanfang*.

(2) Definiere, f.a. $n \in \mathbb{N}$, $f(n{+}1)$ unter Verwendung des Werts $f(n)$ (bzw. unter Verwendung der Werte $f(n), f(n{-}1), \ldots, f(1), f(0)$).
Diesen Schritt bezeichnet man als *Rekursionsschritt*.

Auch hier sind wieder eine Reihe von Varianten möglich.

Beispiel 2.56.

(a) *Frage:* Wie viele Möglichkeiten gibt es, n Studierende so an n PCs zu verteilen, dass an jedem PC genau ein Studierender sitzt?

Antwort: $\text{fak}(n)$, wobei

- $\text{fak}(1) \;=\; 1$ und
- $\text{fak}(n{+}1) \;=\; (n{+}1) \cdot \text{fak}(n)$ (für alle $n \in \mathbb{N}_{\geqslant 1}$).

Insbesondere ist fak eine Funktion von $\mathbb{N}_{\geqslant 1}$ nach $\mathbb{N}_{\geqslant 1}$, d.h. $\text{fak}\colon \mathbb{N}_{\geqslant 1} \to \mathbb{N}_{\geqslant 1}$.

Beispielsweise ist

$$\text{fak}(4) \;=\; 4 \cdot \text{fak}(3) \;=\; 4 \cdot 3 \cdot \text{fak}(2) \;=\; 4 \cdot 3 \cdot 2 \cdot \text{fak}(1) \;=\; 4 \cdot 3 \cdot 2 \cdot 1 \;=\; 24.$$

Allgemein gilt f.a. $n \in \mathbb{N}_{\geqslant 1}$:

$$\text{fak}(n) \;=\; n \cdot (n{-}1) \cdot (n{-}2) \cdot \cdots \cdot 2 \cdot 1 \;\overset{\text{Not.2.20}}{=}\; \prod_{i=1}^{n} i.$$

Notation.
Die Funktion fak wird *Fakultätsfunktion* genannt. Meistens schreibt man $n!$ um die Zahl $\text{fak}(n)$ zu bezeichnen.

(b) *Fragestellung:* Ein Bauer züchtet Kaninchen. Jedes weibliche Kaninchen bringt im Alter von zwei Monaten ein weibliches Kaninchen zur Welt und danach jeden Monat ein weiteres.
Wie viele weibliche Kaninchen hat der Bauer zu Beginn des n-ten Monats, wenn er mit einem neu geborenen weiblichen Kaninchen startet?

Antwort: $\text{fib}(n)$, wobei die Funktion $\text{fib}\colon \mathbb{N}_{\geqslant 1} \to \mathbb{N}_{\geqslant 1}$ rekursiv wie folgt definiert ist:

- $\text{fib}(1) \;:=\; 1$,
- $\text{fib}(2) \;:=\; 1$ und
- $\text{fib}(n{+}1) \;:=\; \text{fib}(n) + \text{fib}(n{-}1)$ (f.a. $n \in \mathbb{N}$ mit $n \geqslant 2$).

Somit gilt:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\text{fib}(n)$	1	1	2	3	5	8	13	21	34	55	89	144

Die Funktion fib wird auch *Fibonacci-Folge* genannt; sie ist benannt nach italienischen Mathematiker Leonardo Fibonacci (13. Jh.). Die Zahl $\text{fib}(n)$ heißt auch *n-te Fibonacci-Zahl*.

Folie 96

Um Aussagen über rekursiv definierte Funktionen zu beweisen, kann man wieder das Induktionsprinzip nutzen. Der folgende Satz gibt dazu ein Beispiel.

Satz 2.57. *Sei* $\text{fib}\colon \mathbb{N}_{\geqslant 1} \to \mathbb{N}_{\geqslant 1}$ *die Fibonacci-Folge. Dann gilt f.a.* $n \in \mathbb{N}_{\geqslant 1}$*:* $\text{fib}(n) \leqslant 2^n$.

Beweis. Per Induktion nach n.

Induktionsanfang: Betrachte $n = 1$ und $n = 2$.

Behauptung: $\text{fib}(1) \leqslant 2^1$ und $\text{fib}(2) \leqslant 2^2$.

Beweis: Es gilt: $\text{fib}(1) \overset{\text{Def.}}{=} 1 \leqslant 2 = 2^1$ und $\text{fib}(2) \overset{\text{Def.}}{=} 1 \leqslant 4 = 2^2$.

Induktionsschritt: $n \to n{+}1$

Sei $n \in \mathbb{N}$ mit $n \geqslant 2$ beliebig.

Induktionsannahme: F.a. $i \in \mathbb{N}_{\geqslant 1}$ mit $i \leqslant n$ gilt: $\text{fib}(i) \leqslant 2^i$.

Behauptung: $\text{fib}(n{+}1) \leqslant 2^{n+1}$.

Beweis:

$$\text{fib}(n{+}1) \overset{\text{Def.}}{=} \text{fib}(n) + \text{fib}(n{-}1) \overset{\text{Ind.ann.}}{\leqslant} 2^n + 2^{n-1} \leqslant 2 \cdot 2^n = 2^{n+1}. \qquad \square$$

Folie 97

Vergleich der Laufzeit zweier Algorithmen

Bemerkung 2.58. Ein möglicher Algorithmus, um für eine Zahl $n \in \mathbb{N}_{\geqslant 1}$ den Wert $\text{fib}(n)$ der Fibonacci-Folge zu berechnen, ist:

Algo 1 (bei Eingabe einer Zahl $n \in \mathbb{N}_{\geqslant 1}$):

1. Falls $n = 1$ oder $n = 2$, dann gib 1 als Ergebnis zurück.

2. Falls $n \geqslant 3$, dann:
3. Sei x_1 die Ausgabe von *Algo 1* bei Eingabe der Zahl $n-1$.
4. Sei x_2 die Ausgabe von *Algo 1* bei Eingabe der Zahl $n-2$.
5. Gib den Wert $(x_1 + x_2)$ als Ergebnis zurück.

Der Algorithmus benötigt bei Eingabe einer Zahl n höchstens $g_1(n)$ Schritte, wobei

$$\begin{aligned} g_1(1) &= 2 \quad \text{und} \quad g_1(2) = 3 \quad \text{und} \\ g_1(n) &= 3 + g_1(n-1) + g_1(n-2) + 2 \\ &= 5 + g_1(n-1) + g_1(n-2) \quad \text{für alle } n \in \mathbb{N} \text{ mit } n \geqslant 3 \end{aligned}$$

(wir zählen hier jede Addition, jeden Vergleich, und jedes Zurückgeben eines Ergebnisses als einen Schritt).

Folie 98

Ein anderer Algorithmus, der für eine Zahl $n \in \mathbb{N}_{\geqslant 1}$ den Wert $\text{fib}(n)$ berechnet, ist:

Algo 2 (bei Eingabe einer Zahl $n \in \mathbb{N}_{\geqslant 1}$):

1. Falls $n = 1$ oder $n = 2$, dann gib 1 als Ergebnis zurück.
2. Seien $a_0 := 0$, $a_1 := 1$ und $a_2 := 1$.
3. Wiederhole für alle i von 3 bis n:
4. Ersetze a_0 durch a_1 und a_1 durch a_2.
5. Ersetze a_2 durch $a_0 + a_1$.
6. Gib den Wert a_2 als Ergebnis zurück.

Dieser Algorithmus benötigt bei Eingabe $n \in \mathbb{N}_{\geqslant 1}$ höchstens $g_2(n)$ Schritte, wobei

$$g_2(1) := 2, \quad g_2(2) := 3, \quad \text{und} \quad g_2(n) := 6 + 6 \cdot (n-2) \quad \text{f.a. } n \geqslant 3$$

(ähnlich wie oben zählen wir jeden Vergleich, jedes Zurückgeben eines Werts und jedes Setzen eines Werts als einen Schritt. Für jeden Schleifendurchlauf berechnen wir zusätzlich 2 Schritte, um i um eins zu erhöhen und zu testen, ob das Ergebnis kleiner oder gleich n ist).

Folie 99

Frage: Welcher der beiden Algorithmen läuft im Allgemeinen schneller? D.h. welche der beiden Funktionen g_1 und g_2 liefert kleinere Funktionswerte?

Mit den in diesem Kapitel bereitgestellten Werkzeugen können wir eine Antwort auf diese Frage finden, und wir können sogar beweisen, dass die Antwort korrekt ist. Hierzu können wir ähnlich vorgehen wie in Beispiel 2.53.

Folie 100

Bemerkung 2.59. Es gibt auch eine „geschlossene Formel“, mit der man die n-te Fibonacci-Zahl, d.h. die Zahl $\text{fib}(n)$, direkt ausrechnen kann, ohne dafür sämtliche Werte $\text{fib}(1)$, $\text{fib}(2)$, …, $\text{fib}(n-1)$ ausrechnen zu müssen: F.a. $n \in \mathbb{N}_{\geqslant 1}$ gilt:

$$\text{fib}(n) \quad = \quad \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Beweis. Übungsaufgabe (per Induktion nach n; Details finden sich in [MM00]). □

Folie 101

Rekursive Definitionen von Mengen

Oft ist es nützlich, auch *Mengen* rekursiv (bzw. induktiv) zu definieren. Eine rekursive Definition einer Menge M besteht aus:

(a) *Basisregeln* der Form „$m \in M$“.

(D.h. die Basisregeln listen explizit bestimmte Elemente auf, die zur Menge M gehören.)

(b) *Rekursiven Regeln* der Form:

„Wenn $m_1, \ldots, m_k \in M$, dann $m \in M$“,

wobei m von $m_1, \ldots, m_k$ abhängt.

Die dadurch definierte Menge M ist dann die Menge aller Elemente, deren Zugehörigkeit zu M durch endlich-maliges Anwenden der Regeln gezeigt werden kann.

Beispiel 2.60 (Die Menge PAL)**.**
Betrachte das Alphabet $A := \{a, b\}$.
Die Menge PAL $\subseteq A^*$ sei wie folgt rekursiv definiert:

Basisregeln:

(B1): $\varepsilon \in$ PAL

(B2): $a \in$ PAL

(B3): $b \in$ PAL

Rekursive Regeln:

(R1): Ist $w \in$ PAL, so ist auch $awa \in$ PAL.

(R2): Ist $w \in$ PAL, so ist auch $bwb \in$ PAL.

Beispiele für Worte, die zur Menge PAL gehören:

$$\underbrace{\varepsilon,\ a,\ b}_{\text{durch Basisregeln}} \qquad \underbrace{aa,\ bb}_{\text{durch rek. Regeln mit } w := \varepsilon}$$

$$\underbrace{aaa,\ bab}_{\text{durch rek. Regeln mit } w := a} \qquad \underbrace{aba,\ bbb}_{\text{durch rek. Regeln mit } w := b}$$

Es gilt beispielsweise auch: $aababaa \in$ PAL.

Beweis.

- $a \in$ PAL (gemäß Basisregel (B2)).
- Regel (R2) mit $w := a$ liefert: $bab \in$ PAL.
- Regel (R1) mit $w := bab$ liefert: $ababa \in$ PAL.
- Regel (R1) mit $w := ababa$ liefert: $aababaa \in$ PAL.

□

Aber beispielsweise gilt

$$aab \notin \text{PAL},$$

denn aus den Basisregeln und den rekursiven Regeln folgt, dass für jedes Wort $w \in$ PAL der erste und der letzte Buchstabe von w identisch sind. □Ende Beispiel 2.60

Folie 103

Induktionsprinzip für rekursiv definierte Mengen:

Sei M eine rekursiv definierte Menge. Dass eine Aussage $A(m)$ für alle $m \in M$ wahr ist, kann man folgendermaßen zeigen:

(1) Zuerst betrachtet man nacheinander jede Basisregel der Form „$m \in M$“ und zeigt, dass die Aussage $A(m)$ wahr ist.
Dieser Schritt heißt *Induktionsanfang*.

(2) Danach betrachtet man nacheinander jede rekursive Regel der Form „Wenn $m_1, \ldots, m_k \in M$, dann $m \in M$“ und zeigt Folgendes: Wenn die Aussagen $A(m_1), \ldots, A(m_k)$ wahr sind, dann ist auch die Aussage $A(m)$ wahr.
Dieser Schritt heißt *Induktionsschritt*.

Beachte. Man kann leicht sehen, dass Folgendes gilt: Wenn man die Schritte (1) und (2) bewiesen hat, so weiß man, dass die Aussage $A(m)$ für alle $m \in M$ wahr ist.

Folie 104

Im Folgenden betrachten wir ein Beispiel dafür, wie das Induktionsprinzip dazu genutzt werden kann, Eigenschaften von rekursiv definierten Mengen nachzuweisen.

Beispiel 2.61 (Palindrome)**.**
Sei $A := \{a, b\}$. Für jedes Wort $w \in A^*$ sei w^R das Wort, das durch „Rückwärtslesen“ von w entsteht, d.h.:

- Ist $w = \varepsilon$, so ist $w^R = \varepsilon$.
- Ist $w = w_1 \cdots w_k$ mit $k \in \mathbb{N}_{\geqslant 1}$ und $w_1, \ldots, w_k \in A$, so ist $w^R := w_k \cdots w_1$.

Beispiel: $aaab^R = baaa$.

Definition: Ein Wort $w \in A^*$ heißt *Palindrom*, wenn gilt: $w = w^R$.

Sei PAL die in Beispiel 2.60 rekursiv definierte Teilmenge von A^*.

Behauptung 1: Für jedes Wort $w \in$ PAL gilt: $w = w^R$.

Beweis: Per Induktion über den Aufbau von PAL.

INDUKTIONSANFANG: Betrachte diejenigen Worte, die aufgrund von Basisregeln zur Menge PAL gehören.
Behauptung: $\varepsilon = \varepsilon^R$, $a = a^R$ und $b = b^R$.
Beweis: Gemäß der Definition von w^R gilt offensichtlich, dass $\varepsilon = \varepsilon^R$, $a = a^R$ und $b = b^R$.

INDUKTIONSSCHRITT: Betrachte die rekursiven Regeln.

- (R1): Sei $w \in \text{PAL}$ und sei $v := awa$. Gemäß (R1) ist $v \in \text{PAL}$.

  Induktionsannahme: $w = w^R$.

  Behauptung: $v = v^R$.

  Beweis: $v^R \overset{\text{Def. } v}{=} (awa)^R \overset{\text{Def. } (\cdot)^R}{=} aw^Ra \overset{\text{Ind.ann.: } w = w^R}{=} awa \overset{\text{Def. } v}{=} v$.

- (R2): Sei $w \in \text{PAL}$ und sei $v := bwb$. Gemäß (R2) ist $v \in \text{PAL}$.

  Induktionsannahme: $w = w^R$.

  Behauptung: $v = v^R$.

  Beweis: $v^R \overset{\text{Def. } v}{=} (bwb)^R \overset{\text{Def. } (\cdot)^R}{=} bw^Rb \overset{\text{Ind.ann.: } w = w^R}{=} bwb \overset{\text{Def. } v}{=} v$.

$\square_{\text{Beh. 1}}$

Behauptung 2: Für jedes $w \in A^*$ mit $w = w^R$ gilt: $w \in \text{PAL}$.

Beweisansatz: Zeige folgende Aussage per Induktion nach n:

> Für alle $n \in \mathbb{N}$ gilt: Ist $w \in A^*$ mit $w = w^R$ und $|w| \leqslant n$, so gilt $w \in \text{PAL}$.

Im Induktionsanfang werden $n = 0$ und $n = 1$ betrachtet; im Induktionsschritt $n \to n+1$ werden alle $n \geqslant 1$ betrachtet.
Details: Übungsaufgabe. $\square_{\text{Beh. 2}}$

Aus Behauptung 1 und Behauptung 2 folgt, dass $\text{PAL} = \{w \in A^* : w = w^R\}$.

$\square_{\text{Ende Beispiel 2.61}}$

2.6 Größenvergleich von Mengen

Folie 105

Definition 2.62. Seien A und B beliebige Mengen.

(a) A heißt *höchstens so mächtig wie* B, wenn es eine injektive Abbildung von A nach B gibt.

(b) A und B heißen *gleichmächtig*, wenn es eine bijektive Abbildung von A nach B gibt.

(c) B heißt *echt mächtiger* als A, wenn gilt: A ist höchstens so mächtig wie B, und A und B sind nicht gleichmächtig.

Beispiel 2.63 ($\mathcal{P}(\mathbb{N})$ ist echt mächtiger als $\mathbb{N}$)**.**
$\mathbb{N}$ ist höchstens so mächtig wie $\mathcal{P}(\mathbb{N})$. Dies wird belegt durch die injektive Abbildung $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ mit $f(n) := \{n\}$ f.a. $n \in \mathbb{N}$.
$\mathbb{N}$ und $\mathcal{P}(\mathbb{N})$ sind nicht gleichmächtig. Dies folgt direkt aus Satz 2.48.
Somit ist $\mathcal{P}(\mathbb{N})$ echt mächtiger als $\mathbb{N}$.

Folie 106

Satz 2.64. *Für jede Menge M gilt:*

(a) $\mathcal{P}(M)$ ist echt mächtiger als M.

(b) $\mathcal{P}(M)$ und $\mathrm{Abb}(M, \{0,1\})$ sind gleichmächtig.

Beweis.
(a): Übungsaufgabe.
(b): Dies folgt direkt aus Satz 2.38(a). □

Folie 107

Bemerkung 2.65. In einem späteren Kapitel (Kapitel 3, Satz 3.73) werden wir beweisen, dass Folgendes für alle Mengen A und B gilt:

> Wenn es eine injektive Funktion von A nach B und eine injektive Funktion von B nach A gibt, dann gibt es auch eine bijektive Funktion von A nach B.

Daraus folgt dann:

> Zwei Mengen A und B sind genau dann gleichmächtig, wenn gilt: A ist höchstens so mächtig wie B und B ist höchstens so mächtig wie A.

Definition 2.66.

(a) Eine Menge A heißt *abzählbar*, wenn es eine injektive Abbildung $f : A \to \mathbb{N}$ gibt (d.h. wenn A höchstens so mächtig ist wie $\mathbb{N}$).

(D.h. die Elemente in A können mit natürlichen Zahlen so „durchnummeriert" werden, dass jedes Element in A eine andere „Nummer" bekommt.)

(b) Eine Menge heißt *abzählbar unendlich*, wenn sie abzählbar und unendlich ist.

(c) Eine Menge heißt *überabzählbar*, wenn sie nicht abzählbar ist.

Bemerkung. In vielen Teilen der Fachliteratur werden die Begriffe „abzählbar" und „abzählbar unendlich" genau so verwendet, wie wir sie hier definiert haben. Aber in manchen Teilen der Literatur wird der Begriff „abzählbar" verwendet um das zu bezeichnen, das wir hier „abzählbar unendlich" nennen; das, was wir hier „abzählbar" nennen, wird dort dann „höchstens abzählbar" genannt.

Satz 2.67. *$\mathcal{P}(\mathbb{N})$ ist überabzählbar.*

Beweis. Durch Widerspruch.
Angenommen, $\mathcal{P}(\mathbb{N})$ wäre abzählbar. Dann gibt es eine injektive Funktion $g : \mathcal{P}(\mathbb{N}) \to \mathbb{N}$. Sei dann die Funktion $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ für alle $n \in \mathbb{N}$ wie folgt definiert: Falls es ein $X \in \mathcal{P}(\mathbb{N})$ mit $g(X) = n$ gibt, so setze $f(n) := X$ (dies ist wohldefiniert, da g injektiv ist — daher gibt es kein weiteres $X' \in \mathcal{P}(\mathbb{N})$ mit $X' \neq X$, für das $g(X') = n$ gilt). Ansonsten setze $f(n) := \emptyset$.

Behauptung: Die Funktion f ist surjektiv.
Beweis: Für jedes beliebige $X \in \mathcal{P}(\mathbb{N})$ gilt: $f(n) = X$ für $n := g(X)$.

$\square_{\text{Beh.}}$

Aber diese Behauptung widerspricht Satz 2.48. $\square$

Beispiel 2.68. Jede der folgenden Mengen ist abzählbar:
$\mathbb{N}$, jedes $M \subseteq \mathbb{N}$, $\mathbb{Z}$.

Beweis. Die Abzählbarkeit der Menge $\mathbb{N}$ wird durch die Identitätsfunktion $\mathrm{id}_{\mathbb{N}}$ belegt; diese Funktion ist injektiv.

Sei $M \subseteq \mathbb{N}$. Die Abzählbarkeit der Menge M wird durch die Funktion $f : M \to \mathbb{N}$ mit $f(x) := x$ f.a. $x \in M$ belegt; diese Funktion ist injektiv.

Die Abzählbarkeit der Menge $\mathbb{Z}$ wird durch die Funktion $g : \mathbb{Z} \to \mathbb{N}$ belegt, die f.a. $z \in \mathbb{Z}$ wie folgt definiert ist:

$$g(z) \;:=\; \begin{cases} 2z & \text{falls } z \geqslant 0 \\ 2|z| - 1 & \text{falls } z < 0. \end{cases}$$

Hierbei bezeichnet $|z|$ den *Betrag* der Zahl z; dieser ist definiert als

$$|z| \;:=\; \begin{cases} z & \text{falls } z \geqslant 0 \\ (-1) \cdot z & \text{falls } z < 0. \end{cases}$$

Beispielsweise ist $|42| = |-42| = 42$.
Offensichtlicherweise bildet diese Funktion g die nicht-negativen ganzen Zahlen auf die geraden natürlichen Zahlen ab; und sie bildet die negativen ganzen Zahlen auf die ungeraden natürlichen Zahlen ab. Man sieht leicht, dass die Funktion g injektiv ist. □

Folie 110

Satz 2.69 („pairing function“)**.** *Die Abbildung* $\pi : \mathbb{N}^2 \to \mathbb{N}$ *mit*[2]

$$\pi(x, y) \;:=\; y + \sum_{i=0}^{x+y} i \;, \qquad \text{f.a. } (x, y) \in \mathbb{N}^2$$

ist bijektiv.

Beachte: Gemäß der Gaußschen Summenformel ist

$$\pi(x, y) \;=\; y \;+\; \tfrac{1}{2}(x+y)(x+y+1) \;.$$

[2]Statt $\pi(x, y)$ müssten wir, um formal korrekt zu sein, eigentlich $\pi((x, y))$ schreiben. Der besseren Lesbarkeit halber nutzt man i.d.R. aber meistens die „Kurzschreibweise“, bei der man die äußeren Klammern eines Tupels, auf das die Funktion angewendet wird, weglässt.

Beweis. Wir zeigen zunächst, dass π *surjektiv* ist:
Betrachte ein beliebiges $n \in \mathbb{N}$. Unser Ziel ist, $(x, y) \in \mathbb{N}^2$ zu finden, so dass gilt: $\pi(x, y) = n$.
Dazu wählen wir die größte Zahl $d \in \mathbb{N}$, für die gilt: $\sum_{i=0}^{d} i \leqslant n$. Es gilt:

$$\sum_{i=0}^{d} i \quad \leqslant \quad n \quad < \quad \sum_{i=0}^{d} i \;+\; d{+}1\,.$$

Wähle

$$y \;:=\; n \;-\; \sum_{i=0}^{d} i \qquad \text{und} \qquad x \;:=\; d - y\,.$$

Klar: $y \in \{j \in \mathbb{N} : 0 \leqslant j \leqslant d\}$ und $x \in \{j \in \mathbb{N} : 0 \leqslant j \leqslant d\}$. Insbesondere ist also $(x, y) \in \mathbb{N}^2$. Außerdem gilt: $x + y = d$ und

$$\pi(x,y) \;=\; y \;+\; \sum_{i=0}^{x+y} i \;=\; n \;-\; \sum_{i=0}^{d} i \;+\; \sum_{i=0}^{d} i \;=\; n\,.$$

Somit ist π also surjektiv.

Wir zeigen nun noch, dass π *injektiv* ist:
Seien $(x, y) \in \mathbb{N}^2$ und $(x', y') \in \mathbb{N}^2$ mit $\pi(x, y) = \pi(x', y')$. Unser Ziel ist zu zeigen, dass $(x, y) = (x', y')$.
Fall 1: $x{+}y = x'{+}y'$. Gemäß Voraussetzung gilt dann:

$$0 \;=\; \pi(x',y') - \pi(x,y) \;=\; y' - y \;+\; \sum_{i=0}^{x'+y'} i \;-\sum_{i=0}^{x+y} i \;=\; y' - y.$$

Also ist $y = y'$. Und wegen $x + y = x' + y'$ folgt dann auch, dass $x = x'$ ist. Somit ist $(x, y) = (x', y')$.
Fall 2: $x{+}y < x'{+}y'$. Sei $I := \{i \in \mathbb{N} : x{+}y < i \leqslant x'{+}y'\}$. Insbesondere ist $x{+}y{+}1 \in I$. Gemäß Voraussetzung gilt:

$$\begin{aligned} 0 \;=\; \pi(x',y') - \pi(x,y) \;&=\; y' - y \;+\; \sum_{i=0}^{x'+y'} i \;-\sum_{i=0}^{x+y} i \\ &=\; y' - y \;+\; \sum_{i \in I} i \\ &\geqslant\; y' - y \;+\; x{+}y{+}1 \\ &=\; y' + x + 1 \end{aligned}$$

Da $y' \in \mathbb{N}$ und $x \in \mathbb{N}$, ist $y'+x+1 \geqslant 1$. Insgesamt ergibt dies, dass $0 \geqslant 1$ ist. Dies ist ein Widerspruch. Somit kann Fall 2 nicht eintreten.

Fall 3: $x+y > x'+y'$. Analog zu Fall 2 (wobei die Rollen von (x, y) und (x', y') vertauscht werden).

Insgesamt haben wir somit gezeigt, dass π injektiv ist. □

Cantors erstes Diagonalargument

Bemerkung 2.70. Die bijektive Funktion $\pi : \mathbb{N}^2 \to \mathbb{N}$ aus Satz 2.69 wird auch *pairing function* genannt. Die Grundidee der Wahl dieser Funktion ist unter dem Namen *Cantors erstes Diagonalargument* bekannt und lässt sich folgendermaßen veranschaulichen (siehe Abbildung 2.1):

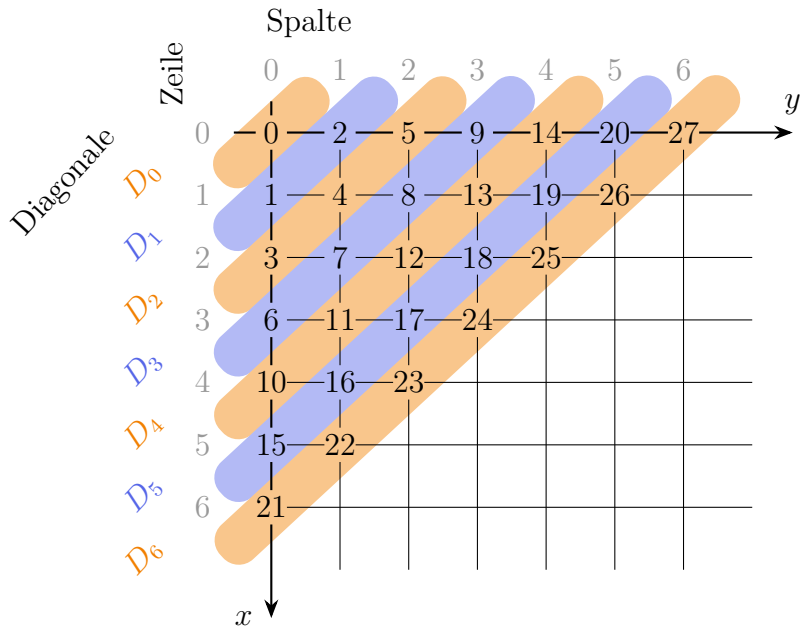


Abbildung 2.1: Veranschaulichung der Funktion π. Der Wert $\pi(x, y)$ ist in Zeile x und Spalte y eingetragen (schwarze Zahlen). Die „i-te Diagonale“ D_i besteht aus allen Punkten (x, y), für die gilt: $x+y = i$.

Die Menge $\mathbb{N}^2$ wird eingeteilt in „Diagonalen“: Für jede Zahl $i \in \mathbb{N}$ ist die *i-te Diagonale* definiert als die Menge

$$D_i \;:=\; \{\, (x, y) \in \mathbb{N}^2 \;:\; x+y = i \,\}$$

Insbes. ist $D_0 = \{(0,0)\}$, $D_1 = \{(1,0),(0,1)\}$, $D_2 = \{(2,0),(1,1),(0,2)\}$. Um die Menge $\mathbb{N}^2$ „abzuzählen“, nummerieren wir die Elemente in $\mathbb{N}^2$ wie folgt durch: Zunächst betrachten wir D_0 und geben dem einzigen Element darin die Nummer 0. Dann betrachten wir D_1 und geben dem Tupel $(1,0)$ die Nummer 1 und dem Tupel $(0,1)$ die Nummer 2. Danach betrachten wir D_2 und geben den Tupeln $(2,0)$, $(1,1)$ und $(0,2)$ die Nummern 3, 4 und 5. Insgesamt betrachten wir nacheinander alle Diagonalen D_i (für $i = 0,1,2,3,\ldots$), betrachten die Elemente in D_i in der Reihenfolge gemäß aufsteigendem y-Wert und verteilen fortlaufende Nummern. Die Funktion π aus Satz 2.69 ist so gewählt, dass die Nummer, die das Tupel $(x,y) \in \mathbb{N}^2$ bekommt, genau die Zahl $\pi(x,y)$ ist.

Folie 112

Lemma 2.71. *Seien Mengen A, B und B_i für alle $i \in \mathbb{N}$ gegeben. Es gilt:*

(a) Falls A und B abzählbar sind ist, so ist auch $A \times B$ abzählbar.

(b) Falls B abzählbar ist, so ist auch B^k abzählbar für jedes $k \in \mathbb{N}$.

(c) Falls für jedes $i \in \mathbb{N}$ die Menge B_i abzählbar ist, so ist auch die Menge $\bigcup_{i\in\mathbb{N}} B_i$ abzählbar.

Beweis. Wir nutzen die bijektive Funktion $\pi : \mathbb{N}^2 \to \mathbb{N}$ aus Satz 2.69.

(a)*:* Gemäß Voraussetzung sind A und B abzählbar, d.h. es gibt injektive Funktionen $f : A \to \mathbb{N}$ und $g : B \to \mathbb{N}$. Wir wollen zeigen, dass es eine injektive Funktion $h : A \times B \to \mathbb{N}$ gibt. Wir wählen h wie folgt: Für alle $(a,b) \in A \times B$ setzen wir

$$h(a,b) \quad := \quad \pi\big(f(a), g(b)\big) \; .$$

Klar: $h(a,b) \in \mathbb{N}$. Somit ist h eine Funktion von $A \times B$ nach $\mathbb{N}$.
Diese Funktion h ist injektiv, denn: Seien (a,b) und (a',b') Elemente in $A \times B$ mit $h(a,b) = h(a',b')$. Wir müssen zeigen, dass $(a,b) = (a',b')$ ist.
Wegen $h(a,b) = h(a',b')$ gilt: $\pi\big(f(a), g(b)\big) = \pi\big(f(a'), g(b')\big)$.
Da π injektiv ist gilt: $\big(f(a), g(b)\big) = \big(f(a'), g(b')\big)$.
Somit ist $f(a) = f(a')$ und $g(b) = g(b')$.
Da f und g injektiv sind gilt $a = a'$ und $b = b'$. Somit ist $(a,b) = (a',b')$.
Dies beendet den Beweis von (a).

(b)*:* Wir führen den Beweis per Induktion nach k. Im Induktionsschritt benutzen wir Aussage (a). Gemäß Voraussetzung ist B abzählbar, d.h. es gibt eine injektive Funktion $g : B \to \mathbb{N}$.

INDUKTIONSANFANG: Betrachte $k = 0$ und $k = 1$.
Behauptung: B^0 und B^1 sind abzählbar.
Beweis:
$B^0 = \{()\}$ ist abzählbar; dies wird belegt durch die injektive Funktion $f_0 : B^0 \to \mathbb{N}$ mit $f_0(()) := 0$.
$B^1 = \{(b) : b \in B\}$ ist abzählbar; dies wird belegt durch die injektive Funktion $f_1 : B^1 \to \mathbb{N}$ mit $f_1((b)) := g(b)$ für jedes $b \in B$.

INDUKTIONSSCHRITT: $k \to k+1$
Sei $k \in \mathbb{N}$ beliebig mit $k \geqslant 1$.
Induktionsannahme: B^k ist abzählbar.
Behauptung: B^{k+1} ist abzählbar.
Beweis: Gemäß Induktionsannahme ist B^k abzählbar. Gemäß Voraussetzung ist B abzählbar. Aussage (a) (für $A := B^k$) liefert, dass $B^k \times B$ abzählbar ist. Somit gibt es eine injektive Funktion $g : B^k \times B \to \mathbb{N}$. Wir wollen zeigen, dass es eine injektive Funktion $h : B^{k+1} \to \mathbb{N}$ gibt. Dazu wählen wir h wie folgt: Für alle $(b_1, \ldots, b_k, b_{k+1}) \in B^{k+1}$ setze[3]

$$h\big((b_1, \ldots, b_k, b_{k+1})\big) \quad := \quad g\big(((b_1, \ldots, b_k), b_{k+1})\big) \; .$$

Offensichtlicherweise ist h injektiv (da g injektiv ist).
Dies beendet den Beweis von (b).

(c)*:* Wir benutzen Aussage (b) und die Funktion π.
Gemäß Voraussetzung gilt für jedes $i \in \mathbb{N}$: Die Menge B_i ist abzählbar — d.h. es gibt eine injektive Funktion $f_i : B_i \to \mathbb{N}$. Sei

$$M \quad := \quad \bigcup_{i \in \mathbb{N}} B_i \; .$$

Wir wollen zeigen, dass es eine injektive Funktion $h : M \to \mathbb{N}$ gibt. Wir wählen h wie folgt: Für jedes $x \in M$ sei i_x die kleinste natürliche Zahl i, für die gilt: $x \in B_i$. Für jedes $x \in M$ setzen wir

$$h(x) \quad := \quad \pi\big(f_{i_x}(x), i_x\big) \; .$$

Klar: $h(x) \in \mathbb{N}$. Somit ist h eine Funktion von M nach $\mathbb{N}$.
Diese Funktion ist injektiv, denn: Seien x und y Elemente in M mit $h(x) = h(y)$. Wir müssen zeigen, dass $x = y$ ist.

[3] Dies ist die formal korrekte Schreibweise, die alle nötigen Klammern enthält. Gemäß der in der vorherigen Fußnote vereinbarten Kurzschreibweise können wir stattdessen auch schreiben: $h\big(b_1, \ldots, b_k, b_{k+1}\big) := g\big((b_1, \ldots, b_k), b_{k+1}\big)$

Wegen $h(x) = h(y)$ ist $\pi\big(f_{i_x}(x), i_x\big) = \pi\big(f_{i_y}(y), i_y\big)$.
Da π injektiv ist, gilt: $\big(f_{i_x}(x), i_x\big) = \big(f_{i_y}(y), i_y\big)$. Somit ist $i_x = i_y$ und $f_{i_x}(x) = f_{i_y}(y)$.
Sei $i := i_x$. Gemäß unserer Wahl von i_x und i_y und da $i = i_x = i_y$ ist, gilt: $x \in B_i$ und $y \in B_i$. Da f_i injektiv ist und $f_i(x) = f_i(y)$ gilt, erhalten wir, dass $x = y$ ist.
Dies beendet den Beweis von (c). □

Folie 113

Satz 2.72. *Für jede Menge A gilt:*
Falls A abzählbar ist, so ist auch A^* abzählbar.

Beweis. Dies folgt leicht aus Lemma 2.71:
Für jedes $i \in \mathbb{N}$ sei $B_i := A^i$. Es gilt:

$$A^* \quad = \quad \bigcup_{i \in \mathbb{N}} A^i \quad = \quad \bigcup_{i \in \mathbb{N}} B_i \ .$$

Lemma 2.71(b) liefert für jedes $i \in \mathbb{N}$, dass B_i abzählbar ist.
Lemma 2.71(c) liefert, dass $\bigcup_{i \in \mathbb{N}} B_i$ abzählbar ist.
Dies beendet den Beweis. □

Folie 114

Existenz nicht-berechenbarer Funktionen

Folgerung 2.73.
Es gibt Funktionen $f : \mathbb{N} \to \{0,1\}$, die nicht berechenbar sind.

Begründung:

Aus Satz 2.67 und Satz 2.64(b) folgt, dass die Menge $\mathrm{Abb}(\mathbb{N}, \{0,1\})$ überabzählbar ist. Somit gibt es überabzählbar viele verschiedene Funktionen $f : \mathbb{N} \to \{0,1\}$.

Eine Funktion $f : \mathbb{N} \to \{0,1\}$ nennen wir *berechenbar*, wenn es ein JAVA-Programm P gibt, so dass für jedes $n \in \mathbb{N}$ gilt: Bei Eingabe von n hält das Programm P nach endlich vielen Schritten an und gibt den Wert $f(n)$ aus — wir sagen dann: *Das Programm P berechnet die Funktion f.*

Jedes JAVA-Programm ist ein Text, dessen Buchstaben Elemente des ASCII-Alphabets sind. Somit ist jedes JAVA-Programm P ein Element in A^*, wobei A das ASCII-Alphabet ist.

Klar: A besteht aus nur endlich vielen verschiedenen Symbolen. Insbesondere ist A abzählbar. Gemäß Satz 2.72 ist A^* abzählbar. Somit gibt es nur abzählbar viele verschiedene JAVA-Programme.

Aber es gibt überabzählbar viele verschiedene Funktionen $f : \mathbb{N} \to \{0,1\}$. Daher muss es Funktionen $f : \mathbb{N} \to \{0,1\}$ geben, die nicht berechenbar sind.

Formaler Beweis:
Durch Widerspruch. Wir nehmen an, dass es für jedes $f : \mathbb{N} \to \{0,1\}$ ein JAVA-Programm P_f gibt, das die Funktion f berechnet.
Klar: $P_f \in A^*$, wobei A das ASCII-Alphabet ist.
Da A abzählbar ist, ist gemäß Satz 2.72 auch A^* abzählbar. D.h. es gibt eine injektive Funktion $g : A^* \to \mathbb{N}$. Wir definieren die Funktion

$$h \;:\; \text{Abb}(\mathbb{N}, \{0,1\}) \to \mathbb{N}$$

wie folgt: Für jedes $f \in \text{Abb}(\mathbb{N}, \{0,1\})$ setzen wir

$$h(f) \;:=\; g(P_f)\ .$$

Diese Funktion h ist injektiv, denn:
Seien $f_1, f_2 \in \text{Abb}(\mathbb{N}, \{0,1\})$ mit $h(f_1) = h(f_2)$. *Zu zeigen:* $f_1 = f_2$.
Wegen $h(f_1) = h(f_2)$ gilt: $g(P_{f_1}) = g(P_{f_2})$. Da g injektiv ist, gilt $P_{f_1} = P_{f_2}$.
Das heißt: f_1 und f_2 werden durch genau dasselbe JAVA-Programm berechnet. Somit gilt für alle Eingaben $n \in \mathbb{N}$, die dieses JAVA-Programm erhält, dass dessen Ausgabe der Wert $f_1(n) = f_2(n)$ ist. Daher ist $f_1 = f_2$.
Wir haben also gezeigt, dass die Funktion h injektiv ist.

Gemäß Satz 2.64(b) sind die Mengen $\mathcal{P}(\mathbb{N})$ und $\text{Abb}(\mathbb{N}, \{0,1\})$ gleichmächtig. D.h. es gibt eine bijektive Funktion $\beta : \mathcal{P}(\mathbb{N}) \to \text{Abb}(\mathbb{N}, \{0,1\})$. Da β und h injektiv sind, ist auch die wie folgt definierte Funktion $\gamma : \mathcal{P}(\mathbb{N}) \to \mathbb{N}$ injektiv: F.a. $M \in \mathcal{P}(\mathbb{N})$ setze

$$\gamma(M) \;:=\; h\big(\beta(M)\big)\ .$$

Somit ist also $\mathcal{P}(\mathbb{N})$ abzählbar. Dies ist ein Widerspruch zu Satz 2.67.

□Folg.2.73

Folie 115

Abzählbarkeit der rationalen Zahlen und Überabzählbarkeit der reellen Zahlen

Satz 2.74.

(a) $\mathbb{Q}$ *ist abzählbar.*

(b) $\mathbb{R}$ *ist überabzählbar.*

Beweis.
(a)*:* Gemäß Beispiel 2.68 ist $\mathbb{Z}$ abzählbar, d.h. es gibt eine injektive Funktion $f : \mathbb{Z} \to \mathbb{N}$.
Außerdem sei $\pi : \mathbb{N}^2 \to \mathbb{N}$ die bijektive Funktion aus Satz 2.69, d.h. f.a. $(x, y) \in \mathbb{N}^2$ ist $\pi(x, y) = y + \sum_{i=0}^{x+y} i$. Insbesondere gilt f.a. $(x, y) \in \mathbb{N}^2$:

$$\pi(x, y) = 0 \quad \iff \quad (x, y) = 0 \ . \tag{2.2}$$

Gesucht ist eine injektive Funktion $g : \mathbb{Q} \to \mathbb{N}$. Wir gehen wie folgt vor:
Jede rationale Zahl $\neq 0$ lässt sich eindeutig darstellen als „gekürzten Bruch“, bei dem der Zähler eine ganze Zahl $\neq 0$ und der Nenner eine natürliche Zahl $\neq 0$ ist.
Wir wählen

$$g(0) \ := \ 0 \ ;$$

und für jeden gekürzten Bruch $\frac{z}{y}$ mit $z \in \mathbb{Z} \setminus \{0\}$ und $y \in \mathbb{N}_{\geqslant 1}$ wählen wir

$$g\Big(\tfrac{z}{y}\Big) \ := \ \pi\big(f(z), y\big) \ .$$

Beachte: Wegen $y \geqslant 1$ und (2.2) ist

$$g\Big(\tfrac{z}{y}\Big) \ \neq \ 0 \ . \tag{2.3}$$

Klar: g ist eine Funktion von $\mathbb{Q}$ nach $\mathbb{N}$.
Wir zeigen nun, dass g injektiv ist. Seien dazu $q, q' \in \mathbb{Q}$ mit $g(q) = g(q')$. Unser Ziel ist zu zeigen, dass $q = q'$ ist.
Fall 1: $g(q) = 0$.
Gemäß (2.3) und unserer Wahl von g ist dann $q = q' = 0$; insbes. ist $q = q'$.
Fall 2: $g(q) \neq 0$.
Gemäß unserer Wahl von g gilt dann: $q \neq 0$ und $q' \neq 0$. Wir stellen q und q' als gekürzte Brüche $\frac{z}{y}$ und $\frac{z'}{y'}$ mit Zählern $z, z' \in \mathbb{Z} \setminus \{0\}$ und Nennern $y, y' \in \mathbb{N}_{\geqslant 1}$ dar. Gemäß unserer Wahl von g gilt:

$$\pi\big(f(z), y\big) \ = \ g\Big(\tfrac{z}{y}\Big) \ = \ g\Big(\tfrac{z'}{y'}\Big) \ = \ \pi\big(f(z'), y'\big) \ .$$

Da π injektiv ist gilt $\big(f(z), y\big) = \big(f(z'), y'\big)$. Also ist $f(z) = f(z')$ und $y = y'$. Da f injektiv ist gilt $z = z'$. Also ist $z = z'$ und $y = y'$. Somit gilt auch: $\frac{z}{y} = \frac{z'}{y'}$, also $q = q'$.

Insgesamt haben wir gezeigt, dass die Funktion $g : \mathbb{Q} \to \mathbb{N}$ injektiv ist.
Somit ist $\mathbb{Q}$ abzählbar.

(b)*:* Wir führen einen Beweis durch Widerspruch. Angenommen, $\mathbb{R}$ wäre abzählbar. Dann gibt es eine injektive Funktion $f : \mathbb{R} \to \mathbb{N}$.
Wir zeigen, dass es dann auch eine injektive Funktion $g : \mathcal{P}(\mathbb{N}) \to \mathbb{N}$ gibt; dies steht dann im Widerspruch zu Satz 2.67.
Zur Definition der Funktion g gehen wir wie folgt vor.
Für jedes $M \subseteq \mathbb{N}$ und jedes $i \in \mathbb{N}$ sei

$$a_{M,i} \quad := \quad \begin{cases} 1 & \text{falls } i \in M \\ 0 & \text{sonst.} \end{cases}$$

Wir repräsentieren $M \subseteq \mathbb{N}$ durch die reelle Zahl r_M mit $0 \leqslant r_M < 1$, deren i-te Nachkommastelle die Ziffer $a_{M,i-1}$ ist (f.a. $i \in \mathbb{N}_{\geqslant 1}$). D.h.:

$$r_M \quad = \quad 0\,,\; a_{M,0}\; a_{M,1}\; a_{M,2}\; a_{M,3} \cdots$$

Beispiele:

- $r_\emptyset \;=\; 0{,}000000\cdots \;=\; 0$
- $r_{\{0,1\}} \;=\; 0{,}1100000\cdots \;=\; 0{,}11$
- $r_{\{0,1,4\}} \;=\; 0{,}11001000000\cdots \;=\; 0{,}11001$
- $r_{\{i\in\mathbb{N}\,:\,i \text{ gerade}\}} \;=\; 0{,}10101010\cdots \;=\; 0{,}\overline{10}.$

Für jedes $M \subseteq \mathbb{N}$ setzen wir $g(M) := f(r_M)$.
Klar: g ist eine Funktion von $\mathcal{P}(\mathbb{N})$ nach $\mathbb{N}$.
Wir zeigen nun, dass g injektiv ist.
Seien dazu $M, M' \subseteq \mathbb{N}$ mit $g(M) = g(M')$. Unser Ziel ist zu zeigen, dass $M = M'$ ist.
Gemäß unserer Definition der Funktion g ist $f(r_M) = f(r_{M'})$.
Gemäß unserer Annahme ist f injektiv. Daher ist $r_M = r_{M'}$. Um den Beweis zu beenden, müssen wir hieraus noch folgern, dass $M = M'$ ist. Das hierfür nötige formale Argument liefern wir im nächsten Abschnitt nach (siehe Bemerkung 2.77). □

2.7 Darstellung von Zahlen

Folie 116

Vorsicht mit der Darstellung reeller Zahlen

Beobachtung 2.75. *Es gilt:* $0{,}\overline{9} = 1$.

Beweis. Sei

$$x := 0{,}\overline{9} = 0{,}999999999\cdots$$

Dann gilt: $10{\cdot}x = 9{,}\overline{9}$.
Und es gilt: $9{\cdot}x = 10{\cdot}x - x = 9{,}\overline{9} - 0{,}\overline{9} = 9$.
Teilen durch 9 liefert: $x = 1$. □

Im Folgenden schauen wir uns etwas genauer an, was hier passiert ist und wie wir korrekt mit der Darstellung reeller Zahlen umgehen können.

Folie 117

Ein Lemma, das man sich merken sollte

Lemma 2.76 (*Geometrische Summenformel*)**.**
Für alle $x \in \mathbb{R} \setminus \{1\}$ *und alle* $\ell \in \mathbb{N}$ *gilt:*

$$\sum_{i=0}^{\ell} x^i = \frac{x^{\ell+1} - 1}{x - 1} .$$

Beweis. Es gilt:

$$(x{-}1) \cdot \sum_{i=0}^{\ell} x^i = \sum_{i=1}^{\ell+1} x^i - \sum_{i=0}^{\ell} x^i \tag{2.4}$$

$$= x^{\ell+1} + \sum_{i=1}^{\ell} x^i - \sum_{i=1}^{\ell} x^i - x^0 \tag{2.5}$$

$$= x^{\ell+1} - 1 . \tag{2.6}$$

Gemäß Voraussetzung ist $x - 1 \neq 0$. Somit liefert Teilen durch $(x{-}1)$, dass

$$\sum_{i=0}^{\ell} x^i = \frac{x^{\ell+1} - 1}{x - 1} .$$

□

Bemerkung. Die in (2.4) bzw. (2.5) stehende Summe (sowie ähnliche Summen, bei denen sich die meisten Summanden gegenseitig wegheben), nennt man *Teleskopsumme*.

Folie 118

Details zur Darstellung reeller Zahlen

Bemerkung 2.77. Eine nicht-negative reelle Zahl stellen wir in der Form

$$n_0 \ , \ n_1 \ n_2 \ n_3 \ n_4 \cdots$$

dar, wobei gilt: $n_0 \in \mathbb{N}$ und $n_i \in \{0, 1, \ldots, 9\}$ für jedes $i \in \mathbb{N}_{\geqslant 1}$. Dies ist genau die Zahl r, die man durch Ausrechnen des folgenden Ausdrucks erhält:

$$n_0 \ + \ \sum_{i=1}^{\infty} n_i \cdot \left(\tfrac{1}{10}\right)^i \ .$$

Um einzusehen, dass die „unendliche Summe“ sinnvoll ist, kann man Lemma 2.76 für $x := \frac{1}{10}$ nutzen.

Daraus ergibt sich:

$$\sum_{i=0}^{\infty}\left(\tfrac{1}{10}\right)^i \ = \ \sum_{i=0}^{\infty} x^i \qquad = \lim_{\ell\to\infty} \sum_{i=0}^{\ell} x^i \ = \ \lim_{\ell\to\infty} \tfrac{x^{\ell+1}-1}{x-1}$$

$$= \lim_{\ell\to\infty} \frac{1-(\frac{1}{10})^{\ell+1}}{1-\frac{1}{10}} \ = \ \frac{1}{1-\frac{1}{10}} \qquad = \ \frac{1}{\frac{9}{10}} \qquad = \ \frac{10}{9} \ .$$

Somit ist

$$\sum_{i=1}^{\infty}\left(\tfrac{1}{10}\right)^i \ = \ \sum_{i=0}^{\infty} x^i \ - \ x^0 \ = \ \tfrac{10}{9} - 1 \ = \ \tfrac{1}{9} \ .$$

Daraus folgt:

$$\sum_{i=1}^{\infty} 9 \cdot \left(\tfrac{1}{10}\right)^i \ = \ 9 \cdot \sum_{i=1}^{\infty}\left(\tfrac{1}{10}\right)^i \ = \ 9 \cdot \tfrac{1}{9} \ = \ 1 \ ,$$

d.h.: $0{,}999999\cdots = 1$ (was wir ja auch bereits in Beobachtung 2.75 festgestellt haben).

Folie 119

Auf ähnliche Art kann man sich davon überzeugen (Details: Übungsaufgabe), dass für jede Wahl von $n_0, \tilde{n}_0 \in \mathbb{N}$ und alle $n_i, \tilde{n}_i \in \{0, 1, \ldots, 9\}$ (f.a. $i \in \mathbb{N}_{\geqslant 1}$) die beiden Ausdrücke

$$n_0 \, , \, n_1 \ n_2 \ n_3 \cdots \qquad \text{und} \qquad \tilde{n}_0 \, , \, \tilde{n}_1 \ \tilde{n}_2 \ \tilde{n}_3 \cdots$$

genau dann *dieselbe* reelle Zahl beschreiben, wenn gilt:

- $n_i = \tilde{n}_i$ für alle $i \in \mathbb{N}$, oder
- es gibt ein $j \in \mathbb{N}$ s.d. gilt:
  - f.a. $i < j$ ist $n_i = \tilde{n}_i$ und
    $\tilde{n}_j = n_j{+}1$ und
    f.a. $i > j$ ist $n_i = 9$ und $\tilde{n}_i = 0$, oder
  - f.a. $i < j$ ist $n_i = \tilde{n}_i$ und
    $n_j = \tilde{n}_j{+}1$ und
    f.a. $i > j$ ist $\tilde{n}_i = 9$ und $n_i = 0$.

Am Ende des Beweises von Satz 2.74(b) benutzen wir, dass für alle Mengen $M, M' \subseteq \mathbb{N}$ mit $M \neq M'$ gilt: die im Beweis von Satz 2.74(b) betrachteten Darstellungen der reellen Zahlen r_M und $r_{M'}$ beschreiben *verschiedene* Zahlen (dies sieht man anhand der obigen Charakterisierung und der Tatsache, dass keine der beiden Darstellungen die Ziffer 9 enthält).

Folie 120

Darstellung natürlicher Zahlen zur Basis n

Wir sind es gewohnt, Zahlen im *Dezimalsystem* darzustellen. Zum Beispiel steht

$$1024 \qquad \text{für die Zahl} \qquad 4{\cdot}10^0 + 2{\cdot}10^1 + 0{\cdot}10^2 + 1{\cdot}10^3 \ .$$

Das ist genau die Zahl 2^{10}, die sich im *Binärsystem* darstellen lässt als

$$10000000000 \quad — \quad \text{dies steht für die Zahl} \quad \sum_{i=0}^{9} 0{\cdot}2^i \ + \ 1{\cdot}2^{10}.$$

An Stelle der Basis 10 (im Dezimalsystem) und der Basis 2 (im Binärsystem) kann man allgemein auch jede beliebige natürliche Zahl $n \geqslant 2$ als Basis benutzen. Zahlen werden dann unter Verwendung der Ziffern $0, 1, \ldots, n{-}1$ dargestellt. Für $\ell \in \mathbb{N}$ und $a_i \in \{0, 1, \ldots, n{-}1\}$ (f.a. $i \leqslant \ell$) steht dann

$$a_\ell \cdots a_1 a_0 \qquad \text{für die Zahl} \qquad \sum_{i=0}^{\ell} a_i{\cdot}n^i.$$

Zumeist vermeidet man „führende Nullen“, d.h. man fordert, dass $a_\ell \neq 0$ ist.

Beispiel: Die zur Basis $n := 8$ (d.h. im *Oktalsystem*) geschriebene Darstellung

$$2000 \quad \text{steht für die Zahl} \quad 0{\cdot}8^0 + 0{\cdot}8^1 + 0{\cdot}8^2 + 2{\cdot}8^3 \ \ (\text{also } 2^{10}).$$

Eindeutigkeit der Darstellung natürlicher Zahlen zur Basis n

Der folgende Satz besagt, dass die Darstellung einer natürlichen Zahl zur Basis n eindeutig ist (d.h. jede natürliche Zahl hat genau *eine* Darstellung zur Basis n).

Satz 2.78. *Sei $n \in \mathbb{N}$ mit $n \geqslant 2$. Seien $\ell, m \in \mathbb{N}$ und seien $a_0, \ldots, a_\ell, b_0, \ldots, b_m \in \{0, 1, \ldots, n-1\}$ mit $a_\ell \neq 0$ und $b_m \neq 0$. Dann gilt:*

$$\sum_{i=0}^{\ell} a_i \cdot n^i \;=\; \sum_{j=0}^{m} b_j \cdot n^j \quad \Longleftrightarrow \quad \ell = m \;\; \text{und} \;\; a_i = b_i \;\; \text{f.a.} \;\; i \leqslant \ell.$$

Beweis. Die Richtung „$\Longleftarrow$“ ist offensichtlich.
Zum Beweis der Richtung „$\Longrightarrow$“ nutzen wir Lemma 2.76 (für $x := n$). Wir betrachten[4] o.B.d.A. den Fall, dass $\ell \geqslant m$ ist.[5] Gemäß Voraussetzung gilt $\sum_{i=0}^{\ell} a_i \cdot n^i = \sum_{j=0}^{m} b_j \cdot n^j$. Wir führen einen Beweis durch Widerspruch. Dazu nehmen wir an, dass $\ell \neq m$ ist oder dass es ein $i \leqslant \ell$ mit $a_i \neq b_i$ gibt.
Für alle $k \in \mathbb{N}$ mit $m < k \leqslant \ell$ setzen wir $b_k := 0$ und erhalten:

$$\sum_{i=0}^{\ell} b_i \cdot n^i \;=\; \sum_{j=0}^{m} b_j \cdot n^j \;=\; \sum_{i=0}^{\ell} a_i \cdot n^i \,. \tag{2.7}$$

Wir wählen nun die *größte* natürliche Zahl $k \leqslant \ell$, so dass $a_k \neq b_k$.[6]
Für jede natürliche Zahl $j \in G := \{i \in \mathbb{N} : k < i \leqslant \ell\}$ gilt dann $a_j = b_j$.

Falls $k = 0$ ist, so ist $a_i = b_i$ f.a. $i \in \{1, \ldots, \ell\}$, und daher

$$0 \;=\; \sum_{i=0}^{\ell} a_i \cdot n^i \;-\; \sum_{i=0}^{\ell} b_i \cdot n^i \;=\; a_0 - b_0 \,.$$

Dies ist ein Widerspruch zu $a_k \neq b_k$.
Somit gilt: $k \geqslant 1$.

Fall 1: $a_k > b_k$, d.h. $a_k \geqslant b_k + 1$.

[4] „*o.B.d.A.*“ steht für „ohne Beschränkung der Allgemeinheit“

[5] Diese Annahme ist tatsächlich „o.B.d.A.“, weil der Fall $\ell < m$ durch Vertauschen der Rollen von ℓ und m genauso behandelt werden kann.

[6] Falls $\ell > m$ ist, so ist $k = \ell$. Aber falls $\ell = m$ ist, so könnte k auch $\leqslant \ell$ sein.

Dann ist

$$\sum_{i=0}^{\ell} b_i{\cdot}n^i \quad = \quad \sum_{i\in G} a_i{\cdot}n^i \;+\; b_k{\cdot}n^k \;+\; \sum_{i=0}^{k-1} b_i{\cdot}n^i \;. \tag{2.8}$$

Es gilt:

$$\sum_{i=0}^{k-1} b_i{\cdot}n^i \;\leqslant\; \sum_{i=0}^{k-1} (n{-}1)\cdot n^i \quad = \quad (n{-}1)\cdot \sum_{i=0}^{k-1} n^i$$

$$\overset{\text{Lem.2.76}}{=} \quad (n{-}1)\cdot \tfrac{n^k-1}{n-1} \quad = \quad n^k - 1\;.$$

Gemeinsam mit (2.8) erhalten wir:

$$\begin{aligned}
\sum_{i=0}^{\ell} b_i{\cdot}n^i \quad &\leqslant \quad \sum_{i\in G} a_i{\cdot}n^i \;+\; b_k{\cdot}n^k \;+\; n^k - 1 \\
&< \quad \sum_{i\in G} a_i{\cdot}n^i \;+\; (b_k{+}1){\cdot}n^k \\
&\leqslant \quad \sum_{i\in G} a_i{\cdot}n^i \;+\; a_k{\cdot}n^k \\
&\leqslant \quad \sum_{i=0}^{\ell} a_i{\cdot}n^i
\end{aligned}$$

Somit ist also $\sum_{i=0}^{\ell} b_i{\cdot}n^i < \sum_{i=0}^{\ell} a_i{\cdot}n^i$. Dies ist ein Widerspruch zu (2.7).

Fall 2: $a_k \not> b_k$. Wegen $a_k \neq b_k$ gilt dann: $b_k > a_k$, d.h. $b_k \geqslant a_k{+}1$.
Dieser Fall kann analog zu Fall 1 behandelt werden, indem man die Rollen von $\sum_{i=0}^{\ell} a_i{\cdot}n^i$ und $\sum_{i=0}^{\ell} b_i{\cdot}n^i$ vertauscht (Details: Übungsaufgabe). □

Folie 122

„Plus 1"-Rechnen bei Darstellungen von Zahlen zur Basis n

Beispiel:
Wenn wir die im Dezimalsystem dargestellte Zahl 12999 um 1 erhöhen, erhalten wir die Zahl 13000.

Allgemein funktioniert „+1"-Rechnen im Dezimalsystem wie folgt:
Suche von rechts nach links die erste Ziffer $\neq 9$; erhöhe diese um 1 und ersetze bei jeder Ziffer rechts davon die 9 durch eine 0.
Spezialfall: Wenn *jede* Ziffer der Zahl eine 9 ist, dann hänge ganz links eine neue Ziffer 0 an und gehe wie oben beschrieben vor.

Das gleiche Vorgehen funktioniert auch bei der Darstellung von Zahlen zur Basis n für jedes beliebige $n \in \mathbb{N}$ mit $n \geqslant 2$. Hierbei spielt dann die Ziffer $n-1$ die Rolle der Ziffer 9 im Dezimalsystem.

„+1"-Rechnen bei Darstellung einer Zahl zur Basis n:
Suche von rechts nach links die erste Ziffer $\neq n-1$; erhöhe diese um 1 und ersetze bei jeder Ziffer rechts davon die $n-1$ durch eine 0.
Spezialfall: Wenn *jede* Ziffer der Zahl eine $n-1$ ist, dann hänge ganz links eine neue Ziffer 0 an und gehe wie oben beschrieben vor.

Folie 123

Beispiel 2.79. Im *Binärsystem* werden Zahlen dargestellt zur Basis $n := 2$.

Dezimalzahl	Binärzahl
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001
10	1010

Antwort auf die Frage aus Beispiel 2.55:

Der „Induktionsschritt $n \to n+1$" ist für den Wert $n = 1$ nicht schlüssig, denn in diesem Fall gilt $n+1 = 2$ und

- $M = \{a_1, a_2\}$,
- $M' = \{a_1\}$,
- $M'' = \{a_2\}$.

Insbesondere gilt also zwar, dass $a_2 \in M''$, aber es gilt nicht, dass $a_2 \in M'$.

2.8 Literaturhinweise

Als vertiefende Lektüre seien die Kapitel 3, 6 und 7 in [MM00] empfohlen. Wertvolle Tipps und Tricks zur Formulierung mathematischer Gedanken und Beweise finden sich in [Beu02] und [Wol17]. Einen Crashkurs in die diskrete Mathematik für Informatiker*innen gibt das Buch [Juk08]. Eine umfassende Einführung in die Mengenlehre gibt das Lehrbuch [Ebb03].

Quellennachweis: Abschnitte 2.1–2.5 sind dem Vorlesungsskript [Sch13] entnommen. Teile der Abschnitte 2.1–2.3 sowie 2.5 orientieren sich an [Gro07]. Teile von Abschnitt 2.4 orientieren sich an [MM00].

2.9 Übungsaufgaben

Aufgabe 2.1. Abgeordnete des Deutschen Bundestages bilden Ausschüsse, die sich mit einem bestimmten Thema befassen. Sei A die Menge der Abgeordneten, die im Ausschuss Arbeit/Soziales sind und F die Menge der Abgeordneten, die sich im Ausschuss Finanzen befinden. Außerdem sei S die Menge der Abgeordneten, die im Sport-Ausschuss sind. Es sind folgende Informationen über die Anzahl der Abgeordneten in den verschiedenen Ausschüssen bekannt:

$$|A| = 17, \qquad |A \cap F| = 8, \qquad |A \cap F \cap S| = 5.$$
$$|F| = 18, \qquad |A \cap S| = 7,$$
$$|S| = 15, \qquad |F \cap S| = 9,$$

(a) Wie viele Abgeordnete sind in mindestens einem der Ausschüsse Mitglied?
D.h. berechnen Sie $|A \cup F \cup S|$.

(b) Wie viele der Abgeordneten sind in genau zwei Ausschüssen?
D.h. berechnen Sie $|((A \cap F) \cup (A \cap S) \cup (F \cap S)) \setminus (A \cap F \cap S)|$.

(c) Es soll ein Unterausschuss gebildet werden, dem alle Abgeordneten des Sport-Ausschusses angehören und zusätzlich alle Abgeordneten, die im Arbeit/Soziales- aber nicht im Finanz-Ausschuss sitzen. Wie viele Mitglieder hat dieser Unterausschuss?
D.h. berechnen Sie $|S \cup (A \setminus F)|$.

Hinweis: Überlegen Sie sich zunächst anhand von Venn-Diagrammen, wie man die Kardinalitäten der Mengen berechnen kann.

Aufgabe 2.2. Schreiben Sie jede der folgenden Mengen in extensionaler Form auf und geben Sie ihre Kardinalität an.

(a) Für ein festes Universum $U := \{1, 2, \ldots, 10\}$ sowie $M := \{1, 3, 5\}$, $N := \{2, 3, 5, 7\}$ und $P := \{1, 4, 9\}$.

(i) $M \setminus (N \cup P)$

(ii) $(M \setminus N) \cup (M \setminus P)$

(iii) $(M \cup N) \cap \overline{P}$

(iv) $(M \cap \overline{P}) \cup (N \cap \overline{P})$

(v) $\{Q : Q \subseteq N, |Q| = 3\}$

(b) Für $M := \{2, 5, 8\}$ und $N := \{3, 5, 7, 11\}$.

(i) $M \cup N$

(ii) $M \setminus N$

(iii) $\{P \in \mathcal{P}(M) : |P| = 2\}$

(iv) $\mathcal{P}(\{\emptyset\})$

(v) $M \times \{a, b\}$

(vi) $\{M\} \times \{a, b\}$

(vii) $N^2 \setminus \{(x, x) : x \in N\}$

Aufgabe 2.3. Geben Sie die folgenden Mengen in intensionaler Form an.

(a) Die Menge A aller ganzen Zahlen, die Lösung der Ungleichung $3x + 2 < 1$ sind.

(b) Die Menge B aller Tupel (x, y) reeller Zahlen, sodass der Betrag der Differenz zwischen x und y höchstens 5 ist.

(c) Die Menge C aller natürlichen Zahlen, die das Produkt zweier ungerader Zahlen $\geqslant 3$ sind.

Aufgabe 2.4. Geben Sie an, welche der folgenden Aussagen richtig und welche falsch sind.

(a) $\emptyset \in \{1, 2, \emptyset\}$

(b) $\emptyset \subseteq \{1, 2, \emptyset\}$

(c) $\{\emptyset\} \subseteq \{1, \{2, \emptyset\}\}$

(d) $\emptyset \subseteq \emptyset$

(e) $\{3, 2, 1\} \subsetneqq \{1, 3, \{1, 2\}\}$

(f) $\{\emptyset, \{2, 3\}\} \subseteq \mathcal{P}(\{1, 2, 3\})$

Aufgabe 2.5. Geben Sie für jede der folgenden Behauptungen an, ob die Behauptung wahr oder falsch ist. Beweisen Sie, dass Ihre Antwort korrekt ist.

(a) Für alle Mengen X, Y, Z gilt: Falls $X \subseteq Y$ und $Y \subsetneqq Z$, dann $X \subsetneqq Z$.

(b) Für alle Mengen X, Y, Z gilt: Falls $X \subseteq Y$ und $Y \not\subseteq Z$, dann $X \not\subseteq Z$.

(c) Für alle Mengen X, Y, Z gilt: Falls $X \cup Y \subseteq Z$, dann $X \subseteq Z$ und $Y \subseteq Z$.

(d) Für alle Mengen X, Y, Z gilt: Falls $X \cap Y \subseteq Z$, dann $X \subseteq Z$ oder $Y \subseteq Z$.

(e) Für alle Mengen X, Y, Z gilt: Falls $X \in Y$ und $Y \in Z$, dann $X \in Z$.

Aufgabe 2.6.

(a) Sind die folgenden Gleichungen korrekt für alle Mengen U, V und W? Begründen Sie Ihre Antwort durch die Betrachtung von Venn-Diagrammen.

(i) $(U \cap V) \cup W = (U \cup W) \cap (V \cup W)$

(ii) $(U \cup V) \setminus (U \cap V) = (U \setminus V) \cap (V \setminus U)$

(b) Beweisen Sie, dass Ihre Antworten aus Teil (a) korrekt sind.

Aufgabe 2.7.

(a) Beweisen Sie: Falls M eine endliche Teilmenge einer unendlichen Menge U ist, so ist das Komplement von M in U unendlich.

(b) Beweisen Sie Satz 2.9(e).

(c) Beweisen Sie Satz 2.21(b).

(d) Es seien m Mengen $M_1, \ldots, M_m$ für ein $m \in \mathbb{N}_{\geqslant 1}$ gegeben. Beweisen Sie die folgende Aussage:

> Falls die Summe der Kardinalitäten der Mengen $M_1, \ldots, M_m$ größer als $n \in \mathbb{N}$ ist, so existiert eine Menge $M \in \{M_1, \ldots, M_m\}$, deren Kardinalität größer als $\frac{n}{m}$ ist.

(e) Beweisen Sie Satz 2.38(b).

Aufgabe 2.8. Beweisen Sie alle Aussagen von Satz 2.10.

Aufgabe 2.9.

(a) Es seien die Mengen $A_1 := \{1, 2, 3\}$, $A_2 := \{2, 3, 4\}$, $A_3 := \{3, 4, 5\}$ und $A_4 := \{4, 5, 6\}$ gegeben. Beschreiben Sie die folgenden Mengen in extensionaler Form.

(i) $\displaystyle\bigcup_{i=1}^{3} A_i$

(ii) $\displaystyle\bigcap_{j=1}^{4} A_j$

(iii) $\displaystyle\bigcup_{k=2}^{4} (A_k \setminus A_{k-1})$

(b) Berechnen Sie den Wert der folgenden Ausdrücke.

(i) $\displaystyle\sum_{i=1}^{5} 2i$

(ii) $\displaystyle\prod_{j=4}^{6} (3j + 1)$

(iii) $\displaystyle\sum_{k=2}^{4} \prod_{\ell=1}^{3} k\ell$

Aufgabe 2.10. Geben Sie für jede der folgenden Funktionen f an, ob die Funktion injektiv, surjektiv und/oder bijektiv ist. Geben Sie jeweils auch das Bild von f an.

(a) $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x) := x - 4$ für alle $x \in \mathbb{Z}$.

(b) $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x) := 2 \cdot x$ für alle $x \in \mathbb{Z}$.

(c) $f : \mathbb{Z} \to \{1, -1\}$ mit $f(x) := (-1)^x$ für alle $x \in \mathbb{Z}$.

(d) $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x) := x^2$ für alle $x \in \mathbb{Z}$.

(e) $f : \mathbb{N} \to \mathbb{N}_{\geqslant 1}$ mit $f(x) := x + 1$ für alle $x \in \mathbb{N}$.

(f) $f : A^* \to \mathbb{N}$ für eine beliebige Menge A mit $|A| = 1$ und $f(w) := |w|$ für alle $w \in A^*$.

(g) $f : A^* \to \mathbb{N}$ für eine beliebige Menge A mit $|A| \geqslant 2$ und $f(w) := |w|$ für alle $w \in A^*$.

Aufgabe 2.11. Seien A, B und C Mengen und sei $f : A \to B$ eine Funktion von A nach B und $g : B \to C$ eine Funktion von B nach C. Wir definieren die Funktion $h : A \to C$ als Komposition, d.h. Hintereinanderausführung, von f und g als $h(x) := g(f(x))$ f.a. $x \in A$. Beweisen Sie die Gültigkeit der folgenden Aussagen:

(a) Wenn f und g surjektiv sind, so ist auch h surjektiv.

(b) Wenn f und g injektiv sind, so ist auch h injektiv.

(c) Wenn f und g bijektiv sind, so ist auch h bijektiv.

(d) Wenn h surjektiv ist, so ist auch g surjektiv.

(e) Wenn h injektiv ist, so ist auch f injektiv.

(f) Was lässt sich über f und g sagen, wenn h bijektiv ist? Beweisen Sie Ihre Aussage.

Aufgabe 2.12. Seien X und Y Mengen, und sei $f : X \to Y$ eine beliebige Funktion. Für jedes $U \subseteq X$ sei $f(U) := \{f(u) : u \in U\}$; die Menge $f(U)$ wird *Bild von U bzgl. f* genannt. Für jedes $V \subseteq Y$ sei $f^{-1}(V) := \{x \in X : f(x) \in V\}$; die Menge $f^{-1}(V)$ wird *Urbild von V bzgl. f* genannt.

Welche der folgenden Aussagen sind für alle Mengen X, Y, alle Funktionen $f : X \to Y$, alle Mengen $A, B \subseteq X$ und alle Mengen $C, D \subseteq Y$ wahr, welche sind falsch? Begründen Sie Ihre Antwort durch einen Beweis oder ein

Gegenbeispiel. Können Sie die falschen Aussagen durch Modifikation oder Hinzufügen von Bedingungen wahr machen?

(a) $f^{-1}(f(A)) = A$

(b) $f(f^{-1}(C)) = C$

(c) $f(A) \subseteq C \implies A \subseteq f^{-1}(C)$

(d) $A \subseteq f^{-1}(C) \implies f(A) \subseteq C$

(e) $f(A) \supseteq C \implies A \supseteq f^{-1}(C)$

(f) $A \supseteq f^{-1}(C) \implies f(A) \supseteq C$

(g) $f(A) \subseteq f(B) \implies A \subseteq B$

(h) $f^{-1}(C) \subseteq f^{-1}(D) \implies C \subseteq D$

(i) $f(\overline{A}) = \overline{f(A)}$

(j) $f^{-1}(\overline{C}) = \overline{f^{-1}(C)}$

(k) $f(A \cup B) = f(A) \cup f(B)$

(l) $f(A \cap B) = f(A) \cap f(B)$

(m) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$

(n) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$

Aufgabe 2.13.* Seien X und Y endliche, nicht-leere Mengen mit $|X| = |Y|$ und $f : X \to Y$ eine beliebige Funktion. Zeigen Sie, dass f genau dann injektiv ist, wenn es surjektiv ist.

Hinweis: Zeigen Sie zuerst, dass für eine endliche Menge X eine Funktion $f : X \to Y$ genau dann injektiv ist, wenn $|X| = |\text{Bild}(f)|$ gilt.

Aufgabe 2.14. Beweisen Sie Satz 2.46 durch Widerspruch.

Aufgabe 2.15. Betrachten Sie die beiden folgenden Algorithmen zur Sortierung der Komponenten eines Tupels $t = (a_1, \ldots, a_{2^k})$ der Länge 2^k, d.h. mit 2^k Komponenten, wobei $k \in \mathbb{N}$.

Algorithmus 1 (Bei Eingabe eines Tupels $t = (a_1, \ldots, a_{2^k})$)

1. Falls $k = 0$, dann gib t als Ergebnis zurück.
2. Sei t_1 die Ausgabe von **Algorithmus 1** bei Eingabe des Tupels $(a_1, \ldots, a_{2^{k-1}})$.
3. Sei t_2 die Ausgabe von **Algorithmus 1** bei Eingabe des Tupels $(a_{2^{k-1}+1}, \ldots, a_{2^k})$.
4. Gib **merge**(t_1, t_2) zurück.

Hierbei ist **merge**() eine Funktion, die bei Eingabe zweier sortierter Tupel t_1 und t_2 mit jeweils 2^{k-1} Komponenten ein sortiertes Tupel mit 2^k Komponenten zurückgibt. Man kann sich leicht überlegen, dass die Funktion **merge**() so implementiert werden kann, dass sie nicht mehr als $3 \cdot 2^k$ Schritte benötigt. Deshalb braucht **Algorithmus 1** insgesamt für ein Tupel der Länge 2^k nicht mehr als $f_1(k) = 2f_1(k-1) + 3 \cdot 2^k + 4$ Schritte, wobei $f_1(0) = 2$.

Algorithmus 2 (Bei Eingabe eines Tupels $t = (a_1, \ldots, a_{2^k})$)

1. Wiederhole für jedes i von 1 bis $(2^k - 1)$:
2. Wiederhole für jedes j von 1 bis $(2^k - i)$:
3. Falls $a_j > a_{j+1}$, dann tausche die Komponenten a_j und a_{j+1} in t.
4. Gib t zurück.

Insgesamt braucht **Algorithmus 2** für ein Tupel der Länge 2^k nicht mehr als $f_2(k) = 3 \cdot 2^{2k} + 2^k - 1$ Schritte.

(a) Welcher der beiden Algorithmen läuft im Allgemeinen schneller? D.h. welche der beiden Funktionen f_1 und f_2 liefert kleinere Funktionswerte?

(b) Beweisen Sie, dass Ihre Antwort aus (a) korrekt ist. Das heißt, falls Sie in (a) geantwortet haben, dass **Algorithmus** i im Allgemeinen schneller als **Algorithmus** j ist, dann finden Sie eine Zahl $n_0 \in \mathbb{N}$ und beweisen Sie per Induktion nach n, dass für alle $n \in \mathbb{N}$ mit $n > n_0$ gilt: $f_i(n) < f_j(n)$.

Aufgabe 2.16. Beweisen Sie die Aussagen von Satz 2.54 mittels vollständiger Induktion.

Aufgabe 2.17.

(a) Beantworten Sie die Frage am Ende der Bemerkung 2.58. Beweisen Sie, dass Ihre Antwort korrekt ist.

(b) Beweisen Sie per vollständiger Induktion die folgende Aussage:

Für alle $n \in \mathbb{N}$ ist $(n^5 - n)$ durch 5 teilbar.

Aufgabe 2.18.

(a) Beweisen Sie Bemerkung 2.59.

(b) Zeigen Sie die zweite Behauptung von Beispiel 2.61.

(c) Beweisen Sie Satz 2.64(a).

Aufgabe 2.19. Betrachten Sie das Alphabet $\Sigma := \{\mathtt{M}, \mathtt{I}, \mathtt{U}\}$. Die Sprache $L \subseteq \Sigma^*$ sei auf die folgende Art rekursiv definiert:[7]
Basisregel:

(B1) $\mathtt{MI} \in L$.

Rekursive Regeln: Für alle $w, w' \in \Sigma^*$ gilt:

(R1) Ist $w\mathtt{I} \in L$, so ist auch $w\mathtt{IU} \in L$,

(R2) ist $\mathtt{M}w \in L$, so ist auch $\mathtt{M}ww \in L$,

(R3) ist $w\mathtt{III}w' \in L$, so ist auch $w\mathtt{U}w' \in L$,

(R4) ist $w\mathtt{UU}w' \in L$, so ist auch $ww' \in L$.

(a) Geben Sie für die folgenden Aussagen an, ob Sie wahr oder falsch sind. Begründen Sie jeweils Ihre Antwort.

(i) $\mathtt{MIU} \in L$.

(ii) $\mathtt{UMII} \in L$.

(iii) $\mathtt{MUII} \in L$.

(iv) $\mathtt{MU} \in L$.

(b) Beweisen Sie per Induktion über die Definition der Menge L, dass für jedes Wort $w \in L$ gilt: Die Anzahl $|w|_{\mathtt{I}}$ der Vorkommen des Symbols $\mathtt{I}$ in w ist *nicht* durch 3 teilbar.

[7] Diese Sprache L wird im Buch *Gödel, Escher, Bach* von Douglas R. Hofstadter betrachtet.

Aufgabe 2.20. Beweisen Sie die Bemerkung am Ende von Bemerkung 2.77, also dass für jede Wahl von $n_0, \tilde{n}_0 \in \mathbb{N}$ und alle $n_i, \tilde{n}_i \in \{0, 1, \ldots, 9\}$ (f.a. $i \in \mathbb{N}_{\geqslant 1}$) die beiden Ausdrücke

$$n_0\,,\, n_1\, n_2\, n_3 \cdots \qquad \text{und} \qquad \tilde{n}_0\,,\, \tilde{n}_1\, \tilde{n}_2\, \tilde{n}_3 \cdots$$

genau dann *dieselbe* reelle Zahl beschreiben, wenn gilt:

- $n_i = \tilde{n}_i$ für alle $i \in \mathbb{N}$, oder
- es gibt ein $j \in \mathbb{N}$ s.d. gilt:
  - f.a. $i < j$ ist $n_i = \tilde{n}_i$ und
    $\tilde{n}_j = n_j + 1$ und
    f.a. $i > j$ ist $n_i = 9$ und $\tilde{n}_i = 0$, oder
  - f.a. $i < j$ ist $n_i = \tilde{n}_i$ und
    $n_j = \tilde{n}_j + 1$ und
    f.a. $i > j$ ist $\tilde{n}_i = 9$ und $n_i = 0$.

Aufgabe 2.21. Geben Sie für jede der Zahlen null, eins, ..., zehn die Darstellung zur Basis n (ohne führende Nullen) für jedes $n \in \{3, 4, 5\}$ an.

Aufgabe 2.22. Betrachten Sie den Beweis von Satz 2.78 und arbeiten Sie die Beweisdetails zum zweiten Fall, also dem Fall $a_k < b_k$, aus.

Aufgabe 2.23. Sei $s \in \mathbb{N}_{\geqslant 1}$. Gegeben sei folgende rekursiv definierte Funktion:[8] Für alle $n \in \mathbb{N}$ sei

$$g_s(n) := \begin{cases} s, & \text{falls } n = 0 \\ \frac{1}{2} \cdot g_s(n-1), & \text{falls } g_s(n-1) \text{ gerade und } n \geqslant 1 \\ 3 \cdot g_s(n-1) + 1, & \text{falls } g_s(n-1) \text{ ungerade und } n \geqslant 1 \end{cases}$$

Berechnen Sie $g_5(5)$ und $g_{23}(15)$.

[8] Bei dieser Funktion handelt es sich um die sogenannte *Collatz-Funktion* für den Startwert $s \in \mathbb{N}_{\geqslant 1}$. Es ist kein konkreter Startwert s bekannt, für den g_s nicht irgendwann den Wert 1 erreicht. Es ist eine offene Forschungsfrage, ob tatsächlich *für jedes* $s \in \mathbb{N}_{\geqslant 1}$ ein $n_s \in \mathbb{N}$ existiert, sodass $g_s(n_s) = 1$.

Kapitel 3

Graphen und Bäume

Folie 124

Bei Modellierungsaufgaben geht es oft darum, *Objekte* sowie *Beziehungen* zwischen Objekten zu beschreiben. Graphen und Bäume eignen sich dazu oft besonders gut.
Anschaulich besteht ein Graph aus *Knoten* und *Kanten:*

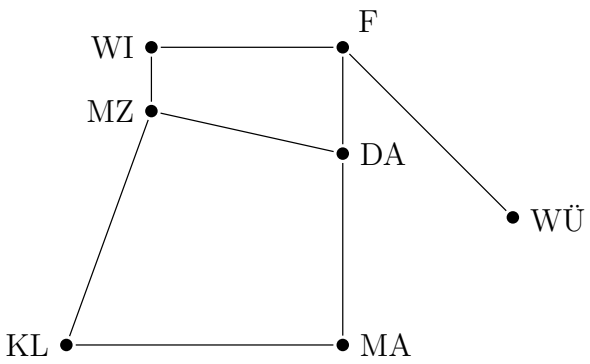
- „Knoten“ repräsentieren dabei „gleichartige Objekte“.
- „Kanten“ repräsentieren Beziehungen zwischen je zwei „Objekten“.

Je nach Aufgabenstellung werden *ungerichtete* Graphen oder *gerichtete* Graphen verwendet.
Bäume sind Graphen mit bestimmten Eigenschaften.

Folie 125

Beispiel 3.1.

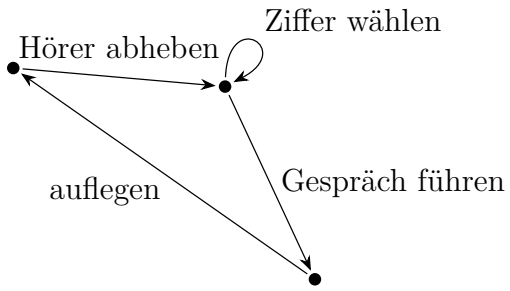
(a) Skizze eines *ungerichteten* Graphen, der die Autobahnverbindungen zwischen einigen Städten darstellt:



DA	$\widehat{=}$	Darmstadt
F	$\widehat{=}$	Frankfurt
KL	$\widehat{=}$	Kaiserslautern
MA	$\widehat{=}$	Mannheim
MZ	$\widehat{=}$	Mainz
WI	$\widehat{=}$	Wiesbaden
WÜ	$\widehat{=}$	Würzburg

Folie 126

(b) Skizze eines *gerichteten* Graphen, der den prinzipiellen Ablauf eines Telefonats darstellt:



3.1 Gerichtete und ungerichtete Graphen

Grundlegende Definitionen

Folie 127

Ungerichtete Graphen

Definition 3.2.
Ein *ungerichteter Graph* $G = (V, E)$ besteht aus einer Menge V, die *Knotenmenge* von G genannt wird, und einer Menge

$$E \subseteq \big\{\{i, j\} : i \in V, j \in V, i \neq j\big\},$$

die *Kantenmenge* von G genannt wird. Die Elemente aus V heißen *Knoten* von G (auch: „Ecken“; englisch: *vertices*, singular: vertex); die Elemente aus E heißen *Kanten* von G (englisch: *edges*, singular: edge).
Ein ungerichteter Graph G heißt *endlich*, falls seine Knotenmenge endlich ist.

Folie 128

Beispiel 3.3. $G = (V, E)$ mit

$$V := \{ \text{MZ}, \text{WI}, \text{MA}, \text{DA}, \text{KL}, \text{F}, \text{WÜ} \} \quad \text{und}$$

$$E := \{ \{\text{MZ}, \text{WI}\}, \{\text{WI}, \text{F}\}, \{\text{F}, \text{DA}\}, \{\text{F}, \text{WÜ}\}, \{\text{MZ}, \text{DA}\}, \{\text{MZ}, \text{KL}\}, \{\text{KL}, \text{MA}\}, \{\text{DA}, \text{MA}\} \}$$

ist ein ungerichteter Graph, der die Autobahnverbindungen zwischen Mainz (MZ), Wiesbaden (WI), Mannheim (MA), Darmstadt (DA), Kaiserslautern (KL), Frankfurt (F) und Würzburg (WÜ) repräsentiert. Beispiel 3.1(a) zeigt diesen Graphen G in *graphischer Darstellung*: Knoten werden als Punkte dargestellt, Kanten als Verbindungslinien zwischen Punkten.

Folie 129

Beachte. Laut Definition 3.2 gibt es zwischen zwei Knoten i und j aus V

- *höchstens* eine Kante; diese wird mit $\{i, j\}$ bezeichnet und graphisch dargestellt als

- *keine* Kante, falls $i = j$ ist. In der graphischen Darstellung eines ungerichteten Graphen sind also „Schleifen“ der Form

  nicht erlaubt.

Jede Kante $\{i, j\}$ eines ungerichteten Graphen ist also eine 2-elementige Menge von Knoten des Graphen.

Folie 130

Bemerkung. In der Literatur wird zumeist die oben genannte Definition von ungerichteten Graphen verwendet. Davon abweichend erlauben einige Bücher in ungerichteten Graphen aber auch „Schleifen“ der Form

Notation 3.4. Sei $G = (V, E)$ ein ungerichteter Graph.

- Ein Knoten $v \in V$ heißt *inzident* mit einer Kante $e \in E$, falls $v \in e$.
- Die beiden mit einer Kante $e \in E$ inzidenten Knoten nennen wir die *Endknoten* von e, und wir sagen, dass e diese beiden Knoten *verbindet*.
- Zwei Knoten $v, w \in V$ heißen *benachbart* (bzw. *adjazent*), falls es eine Kante $e \in E$ gibt, deren Endknoten v und w sind (d.h. $e = \{v, w\}$).
- Falls v und w zwei benachbarte Knoten sind, so sagen wir auch: w ist ein *Nachbar* von Knoten v.

Definition 3.5 (Grad)**.**
Sei $G = (V, E)$ ein endlicher ungerichteter Graph und sei $v \in V$ ein Knoten von G. Der *Grad von v in G* (engl.: degree), kurz: $\mathrm{Grad}_G(v)$, ist die Anzahl der Kanten, die v als Endknoten haben. D.h.

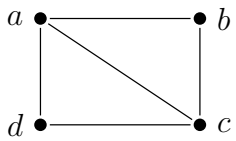
$$\mathrm{Grad}_G(v) \;=\; |\{e \in E \,:\, v \in e\}| \,.$$

Der *Grad von G* ist

$$\mathrm{Grad}(G) \;:=\; \max\{\mathrm{Grad}_G(v) \,:\, v \in V\} \,,$$

d.h. $\mathrm{Grad}(G)$ gibt den maximalen Grad eines Knotens von G an.[1]

Beispiel.
Für den Graphen G =



gilt: $\mathrm{Grad}_G(a) = 3$, $\mathrm{Grad}_G(b) = 2$, $\mathrm{Grad}_G(c) = 3$, $\mathrm{Grad}_G(d) = 2$ und $\mathrm{Grad}(G) = 3$.

Folie 134

Gerichtete Graphen

Definition 3.6.
Ein *gerichteter Graph* $G = (V, E)$ besteht aus einer Menge V, die *Knotenmenge* von G genannt wird, und einer Menge

$$E \subseteq \big\{(i,j) : i \in V, j \in V\big\},$$

die *Kantenmenge* von G genannt wird. Die Elemente aus V heißen *Knoten* (bzw. „Ecken“), die Elemente aus E heißen (gerichtete) *Kanten* von G.
Ein gerichteter Graph G heißt *endlich*, falls seine Knotenmenge endlich ist.

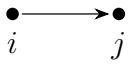
Folie 135

Beispiel 3.7. $G = (V, E)$ mit

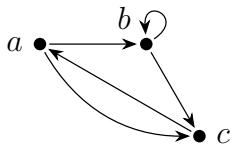
$$\begin{aligned} V &:= \{\, a, b, c \,\} \quad \text{und} \\ E &:= \big\{\, (a,b),\ (b,b),\ (b,c),\ (c,a),\ (a,c) \,\big\} \end{aligned}$$

ist ein gerichteter Graph.

In der *graphischen Darstellung* eines gerichteten Graphen werden Knoten werden als Punkte dargestellt. Eine Kante der Form (i, j) wird als Pfeil von Knoten i nach Knoten j dargestellt, also



Der gerichtete Graph aus Beispiel 3.7 lässt sich in graphischer Darstellung also wie folgt darstellen:



Folie 136

Notation 3.8. Sei $G = (V, E)$ ein gerichteter Graph.

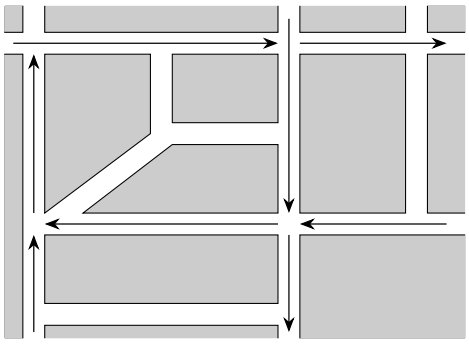
[1] Ist M eine endliche, nicht-leere Menge von Zahlen, so bezeichnet $\max M$ das größte Element von M.

- Ist $e = (i, j) \in E$, so heißt i der *Ausgangsknoten* von e und j der *Endknoten* von e, und wir sagen, dass e *von* i *nach* j *verläuft*.
- Ein Knoten $v \in V$ heißt *inzident* mit einer Kante $e \in E$, falls v der Ausgangs- oder der Endknoten von e ist.
- Zwei Knoten $v, w \in V$ heißen *benachbart* (bzw. *adjazent*), falls $(v, w) \in E$ oder $(w, v) \in E$.
- Eine Kante der Form (v, v) wird *Schleife* genannt. D.h.: Eine Schleife ist eine Kante, deren Ausgangs- und Endknoten identisch ist.

Folie 137

Modellierung durch gerichtete Graphen

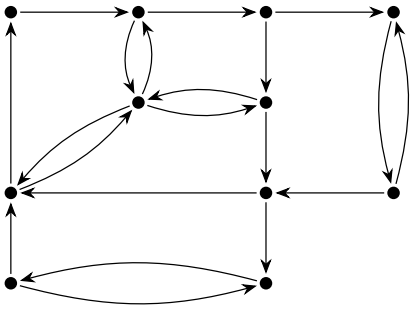
Beispiel 3.9.
In der folgenden Straßenkarte sind Einbahnstraßen durch Pfeile markiert.



Diese Straßenkarte können wir durch einen gerichteten Graphen repräsentieren, der für jede Straßenkreuzung einen Knoten enthält, und in dem es eine Kante von „Kreuzung“ i zu „Kreuzung“ j gibt, falls man von i nach j fahren kann, ohne zwischendurch eine weitere Kreuzung zu passieren.

Folie 138

Graphisch lässt sich dieser gerichtete Graph folgendermaßen darstellen:



Folie 139

Weitere Beispiele zur Modellierung durch Graphen:

- Computer-Netzwerk:
  Knoten repräsentieren Computer; Kanten repräsentieren Netzwerkverbindungen
- das World Wide Web:
  Knoten repräsentieren Webseiten; Kanten repräsentieren Hyperlinks

Folie 140

Definition 3.10.
Sei $G = (V, E)$ ein endlicher gerichteter Graph und sei $v \in V$ ein Knoten von G.

- Der *Ausgangsgrad* von v in G (engl.: out-degree), kurz: $\text{Aus-Grad}_G(v)$, ist die Anzahl der Kanten, die v als Ausgangsknoten haben. D.h.:

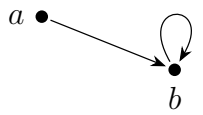
$$\text{Aus-Grad}_G(v) \;=\; |\{e \in E \,:\, \text{es ex. } v' \in V \text{ s.d. } e = (v, v')\}|.$$

- Der *Eingangsgrad* von v in G (engl.: in-degree), kurz: $\text{Ein-Grad}_G(v)$, ist die Anzahl der Kanten, die v als Eingangsknoten haben. D.h.:

$$\text{Ein-Grad}_G(v) \;=\; |\{e \in E \,:\, \text{es ex. } v' \in V \text{ s.d. } e = (v', v)\}|.$$

Folie 141

Beispiel.
Für den Graphen G =



gilt: $\text{Ein-Grad}_G(a) = 0$, $\text{Ein-Grad}_G(b) = 2$, $\text{Aus-Grad}_G(a) = 1$, $\text{Aus-Grad}_G(b) = 1$.

Folie 142

Verschiedene Arten der Darstellung von Graphen

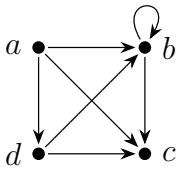
Bemerkung 3.11.
Es gibt mehrere Arten Graphen darzustellen, zum Beispiel

- *abstrakt*, durch Angabe der Knotenmenge V und der Kantenmenge E.

  Beispiel: $G_1 = (V_1, E_1)$ mit

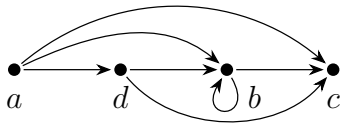
  $$\begin{aligned} V_1 &:= \{\, a,\ b,\ c,\ d \,\} \quad \text{und} \\ E_1 &:= \{\, (a,b),\ (a,c),\ (a,d),\ (b,b),\ (b,c),\ (d,b),\ (d,c) \,\}. \end{aligned}$$

- *graphisch* (bzw. *anschaulich*): Der obige Beispiel-Graph G_1 kann graphisch dargestellt werden durch



Folie 143

oder, äquivalent dazu, durch



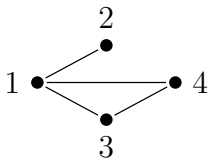
Folie 144

- durch Angabe einer *Adjazenzliste*, die zu jedem Knoten i eine Liste aller Knoten angibt, zu denen eine von i ausgehende Kante führt. Der Beispiel-Graph G_1 wird durch folgende Adjazenzliste repräsentiert:

Knoten	Nachfolger
a	b, c, d
b	b, c
c	
d	b, c

Folie 145

Auf die gleiche Art können auch *ungerichtete* Graphen durch eine Adjazenzliste repräsentiert werden. Beispielweise der Graph

$G_2 \quad := \quad$ 

durch die Adjazenzliste

Knoten	Nachbarn
1	2, 3, 4
2	1
3	1, 4
4	1, 3

Folie 146

- durch Angabe einer *Adjazenzmatrix*, d.h. einer Tabelle, deren Zeilen und Spalten mit Knoten beschriftet sind, und die in der mit Knoten i beschrifteten Zeile und der mit Knoten j beschrifteten Spalte
  - den Eintrag 1 hat, falls es eine Kante von Knoten i nach Knoten j gibt, und
  - den Eintrag 0 hat, falls es keine Kante von i nach j gibt.

  Beispielsweise sieht die Adjazenzmatrix des gerichteten Graphen G_1 wie folgt aus:

	a	b	c	d
a	0	1	1	1
b	0	1	1	0
c	0	0	0	0
d	0	1	1	0

Folie 147

Die Adjazenzmatrix des ungerichteten Graphen G_2 ist:

	1	2	3	4
1	0	1	1	1
2	1	0	0	0
3	1	0	0	1
4	1	0	1	0

Wege in Graphen

Folie 148

Definition 3.12 (Wege und Kreise)**.** [2]
Sei $G = (V, E)$ ein (gerichteter oder ungerichteter) Graph.

(a) Ein *Weg* in G ist ein Tupel

$$(v_0, \ldots, v_\ell) \ \in \ V^{\ell+1},$$

für ein $\ell \in \mathbb{N}$, so dass für alle $i \in \mathbb{N}$ mit $0 \leqslant i < \ell$ gilt:

- falls G ein gerichteter Graph ist, so ist $(v_i, v_{i+1}) \in E$,
- falls G ein ungerichteter Graph ist, so ist $\{v_i, v_{i+1}\} \in E$.

Das Tupel $(v_0, \ldots, v_\ell)$ wird dann *ein Weg von* v_0 *nach* v_ℓ genannt. ℓ ist die *Länge des Weges*. D.h.: Die *Länge* des Weges gibt an, wie viele *Kanten* auf dem Weg durchlaufen werden.

Beachte.
Gemäß dieser Definition ist für jedes $v \in V$ das Tupel (v) ein Weg der Länge 0 von v nach v.

Folie 149

(b) Ein Weg $(v_0, \ldots, v_\ell)$ heißt *einfach*, wenn kein Knoten mehr als einmal in dem Weg vorkommt — d.h. die Knoten $v_0, \ldots, v_\ell$ sind paarweise[3] verschieden, d.h. $|\{v_0, \ldots, v_\ell\}| = \ell{+}1$.

(c) Ein Weg $(v_0, \ldots, v_\ell)$ heißt *Kreis*, wenn $\ell \geqslant 1$ und $v_\ell = v_0$ ist.

(d) Ein Kreis $(v_0, \ldots, v_\ell)$ heißt *einfach*, wenn keine Kante mehrfach durchlaufen wird und — abgesehen vom Start- und Endknoten — kein Knoten mehrfach besucht wird. D.h.:

- In einem *gerichteten* Graphen G sind *einfache* Kreise genau die Wege der Form $(v_0, \ldots, v_\ell)$, für die gilt: $\ell \geqslant 1$ und $v_\ell = v_0$ und $|\{v_0, \ldots, v_{\ell-1}\}| = \ell$.

[2] Wir verwenden hier die Definitionen von Wegen und Kreisen wie sie in der Informatik üblich sind. In der mathematischen Graphentheorie werden die Begriffe für Abfolgen von Knoten, die durch Kanten verbunden sind, jedoch teilweise anders definiert.
Als Referenzwerk sei auf [Die06] verwiesen.

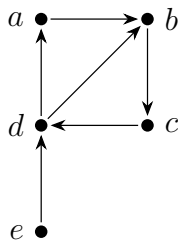
[3] Der Begriff „paarweise verschieden“ ist Mathematik-Jargon. Die Aussage „seien $x_1, \ldots, x_n$ paarweise verschieden“ bedeutet, dass $x_1, \ldots, x_n$ alle verschieden voneinander sind, d.h. $x_i \neq x_j$ f.a. $i, j \in \{1, \ldots, n\}$ mit $i \neq j$.

- In einem *ungerichteten* Graphen G sind *einfache* Kreise genau die Wege der Form $(v_0, \ldots, v_\ell)$, für die gilt: $\ell \geqslant 3$ und $v_\ell = v_0$ und $|\{v_0, \ldots, v_{\ell-1}\}| = \ell$.

Folie 150

Beispiel 3.13.

(a) Für den Graphen

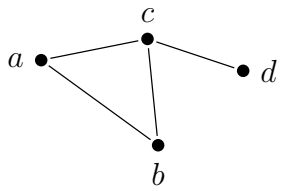


gilt:

- (e, d, b, c, d) ist ein Weg der Länge 4, aber kein einfacher Weg.
- (d, b, c, d) ist ein einfacher Kreis.
- (e, d, a, b) ist ein einfacher Weg.
- (b, d, a) ist kein Weg.
- (a, b, c, d, b, c, d, a) ist ein Kreis, aber kein einfacher Kreis.

Folie 151

(b) Für den Graphen



gilt:

- (a, b, c, a) ist ein einfacher Kreis.
- (c, d, c) ist ein Kreis, aber kein einfacher Kreis.
- (a, c, d) ist ein einfacher Weg.
- (c, b, a, c, d) ist ein Weg, aber kein einfacher Weg.

Folie 152

Definition 3.14 (azyklischer Graph, DAG)**.**

(a) Ein Graph heißt *azyklisch*, falls er keinen einfachen Kreis enthält.

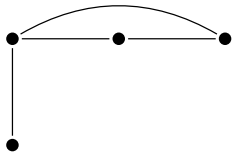
(b) Gerichtete azyklische Graphen werden im Englischen *directed acyclic graph*, kurz: *DAG*, genannt.

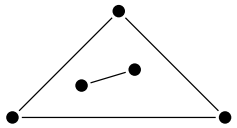
Folie 153

Definition 3.15 (zusammenhängend, stark zusammenhängend)**.**

(a) Ein ungerichteter Graph $G = (V, E)$ heißt *zusammenhängend*, wenn für alle Knoten $v, w \in V$ gilt: Es gibt in G einen Weg von v nach w.

Beispiel.

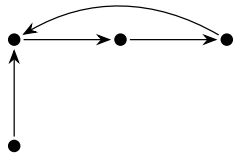
Der Graph  ist zusammenhängend.

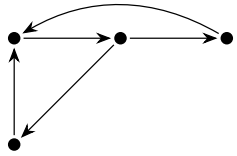
Der Graph  ist nicht zusammenhängend.

Folie 154

(b) Ein gerichteter Graph $G = (V, E)$ heißt *stark zusammenhängend*, wenn für alle Knoten $v, w \in V$ gilt: Es gibt in G einen Weg von v nach w.

Beispiel.

Der Graph  ist *nicht* stark zusammenhängend (da es z.B. keinen Weg vom Knoten links oben zum Knoten links unten gibt).

Der Graph  ist stark zusammenhängend.

Definition 3.16 (Zusammenhangskomponente, starke Zusammenhangskomponente)**.**

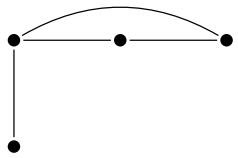
(a) Sei $G = (V, E)$ ein ungerichteter Graph. Ein Graph $G' = (V', E')$ heißt *Zusammenhangskomponente* von G, falls die folgenden Bedingungen erfüllt sind:

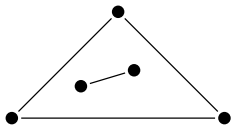
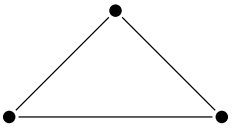
(1) G' ist ein Teilgraph von G, d.h. $V' \subseteq V$ und $E' \subseteq E$,

(2) G' ist zusammenhängend und

(3) für jeden zusammenhängenden Teilgraphen $G'' = (V'', E'')$ von G mit $V' \subseteq V''$ und $E' \subseteq E''$ gilt: $V' = V''$ und $E' = E''$.

Beispiel.

$G =$  hat nur eine Zusammenhangskomponente, nämlich G selbst.

$G =$  hat zwei Zusammenhangskomponenten, nämlich  und 

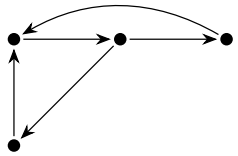
(b) Sei $G = (V, E)$ ein gerichteter Graph. Ein Graph $G' = (V', E')$ heißt *starke Zusammenhangskomponente* von G, falls die folgenden Bedingungen erfüllt sind:

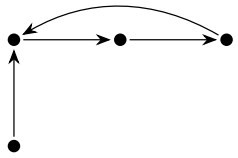
(1) G' ist ein Teilgraph von G,

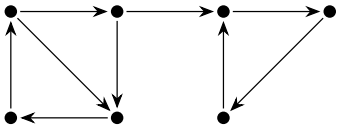
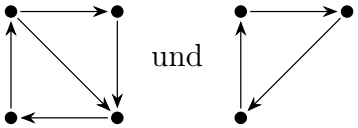
(2) G' ist stark zusammenhängend und

(3) für jeden stark zusammenhängenden Teilgraphen $G'' = (V'', E'')$ von G mit $V' \subseteq V''$ und $E' \subseteq E''$ gilt: $V' = V''$ und $E' = E''$.

Beispiel.

$G =$  hat nur eine starke Zusammenhangskomponente, nämlich G selbst.

$G =$  hat zwei starke Zusammenhangskomponenten, nämlich  und •

$G =$  hat zwei starke Zusammenhangskomponenten, nämlich 

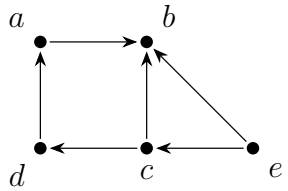
Folie 156

Definition 3.17 (Hamilton-Kreise und Hamilton-Wege)**.**
Sei $G = (V, E)$ ein (gerichteter oder ein ungerichteter) Graph.

(a) Ein Weg $W = (v_0, \ldots, v_\ell)$ heißt *Hamilton-Weg*, wenn jeder *Knoten* aus V genau einmal in W vorkommt.

(b) Ein *Hamilton-Kreis* ist ein einfacher Kreis $W = (v_0, \ldots, v_\ell)$, für den gilt: $\ell \geqslant 1$ und $(v_0, \ldots, v_{\ell-1})$ ist ein Hamilton-Weg.

Beispiel. Der Graph G



hat einen Hamilton-Weg, nämlich $(\mathrm{e}, \mathrm{c}, \mathrm{d}, \mathrm{a}, \mathrm{b})$, aber keinen Hamilton-Kreis (da Aus-Grad$_G(b) = 0$ ist).

Folie 157

Travelling Salesman Problem

Ein Anwendungsbeispiel:
Beim Problem des *Handlungsreisenden* (engl.: *Travelling Salesman Problem*, kurz: *TSP*) geht es darum, eine Rundreise durch n Städte so durchzuführen, dass jede Stadt genau 1 mal besucht wird. Es geht also darum, einen Hamilton-Kreis zu finden. Das Problem, zu einem gegebenen Graphen zu entscheiden, ob er einen Hamilton-Kreis besitzt, ist algorithmisch ein schwieriges Problem: Man kann zeigen, dass es NP-vollständig ist.

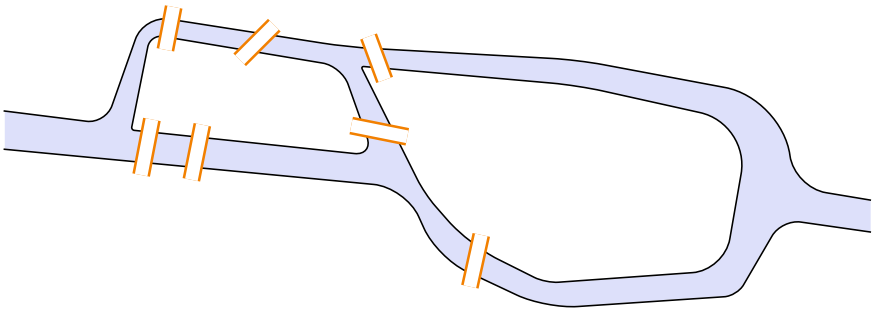
Folie 158

Im Gegensatz zu *Hamilton-Wegen* (bei denen es darum geht, einen Weg zu finden, der jeden *Knoten* des Graphen genau einmal besucht), geht es bei den im Folgenden betrachteten *Euler-Wegen* darum, einen Weg zu finden, der jede *Kante* des Graphen genau einmal besucht.

Folie 159

Königsberger Brückenproblem

Beispiel 3.18.
In der Stadt Königsberg gab es im 18. Jahrhundert 7 Brücken über den Fluss Pregel, die das linke Ufer, das rechte Ufer und 2 Inseln auf die in der folgenden Skizze dargestellten Art miteinander verbanden.

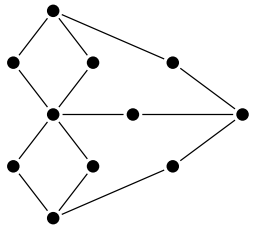


Frage. Gibt es einen Spaziergang, der jede der 7 Brücken genau einmal überquert und zum Ausgangspunkt zurückkehrt?

Die obige Skizze lässt sich folgendermaßen durch einen ungerichteten Graphen modellieren: für jedes Ufer, jede Insel und jede Brücke gibt es einen Knoten; Kanten zeigen direkte Verbindungen an.

Folie 160

Die Skizze wird also durch folgenden Graphen repräsentiert:

$G_{\text{Königsberg}} :=$ 

Die Frage nach dem „Spaziergang“ entspricht dann gerade der Frage:

Gibt es in $G_{\text{Königsberg}}$ einen *Euler-Kreis*?

Folie 161

Definition 3.19 (Euler-Kreise und Euler-Wege)**.**
Sei $G = (V, E)$ ein ungerichteter Graph.

(a) Ein Weg $W = (v_0, \ldots, v_\ell)$ heißt *Euler-Weg*, wenn W jede Kante aus E genau einmal durchläuft, d.h. wenn es für jedes $e \in E$ genau ein $i \in \{0, \ldots, \ell - 1\}$ gibt, so dass $e = \{v_i, v_{i+1}\}$.

(b) Ein Weg $W = (v_0, \ldots, v_\ell)$ heißt *Euler-Kreis*, wenn W ein Euler-Weg ist und $v_0 = v_\ell$ ist.

Satz 3.20 (Existenz von Euler-Kreisen und Euler-Wegen)**.**
Sei $G = (V, E)$ ein ungerichteter, zusammenhängender Graph, dessen Knotenmenge endlich ist. Dann gilt:

(a) G besitzt einen Euler-Kreis
$\iff$
jeder Knoten von G hat einen geraden Grad (d.h. ist mit einer geraden Anzahl von Kanten inzident).

(b) G besitzt einen Euler-Weg, der kein Euler-Kreis ist
$\iff$
es gibt in G genau zwei Knoten mit ungeradem Grad.

Beweis.

(a) „$\Longrightarrow$“: Sei $K = (v_0, \ldots, v_\ell)$ ein Euler-Kreis. Insbesondere gilt: $v_0 = v_\ell$.

Schritt 1: Jeder Knoten $v \in \{v_0, \ldots, v_{\ell-1}\}$ hat geraden Grad, denn: Sei $v \in \{v_0, \ldots, v_{\ell-1}\}$ beliebig. Zu jedem $i \in \{0, \ldots, \ell-1\}$ mit $v = v_i$ gibt es im Euler-Kreis K zwei verschiedene Kanten, nämlich

- $\{v_{i-1}, v_i\}$ und $\{v_i, v_{i+1}\}$, falls $i \neq 0$, bzw.
- $\{v_0, v_1\}$ und $\{v_{\ell-1}, v_0\}$, falls $i = 0$ (beachte: $v_0 = v_\ell$).

Da der Euler-Kreis K jede Kante von G genau einmal enthält, gilt somit Folgendes: Ist $k = |\{i \in \{0, \ldots, \ell-1\} : v = v_i\}|$ (d.h. k gibt an, wie oft v im Tupel $(v_0, \ldots, v_{\ell-1})$ vorkommt), so ist $\text{Grad}_G(v) = 2 \cdot k$. Daher hat jeder Knoten $v \in \{v_0, \ldots, v_{\ell-1}\}$ geraden Grad.

Schritt 2: $\{v_0, \ldots, v_{\ell-1}\} = V$, denn:
Laut Voraussetzung ist G zusammenhängend. Für beliebige Knoten $v, w \in V$ gilt daher: es gibt in G einen Weg von v nach w. Da K ein Euler-Kreis ist, enthält K sämtliche Kanten, die auf dem Weg von v nach w vorkommen. Insbesondere gilt also f.a. $v, w \in V$, dass $v, w \in \{v_0, \ldots, v_{\ell-1}\}$.

Zusammenfassung: Aus den Schritten 1 und 2 folgt direkt, dass jeder Knoten von G geraden Grad hat.

„$\Longleftarrow$“: Sei G ein zusammenhängender ungerichteter Graph, in dem jeder Knoten geraden Grad hat. Es sei

$$W \;=\; (v_0, \ldots, v_\ell)$$

ein Weg *maximaler Länge* in G, der *keine Kante(n) mehrfach* enthält. Da wir W nicht mehr verlängern können, liegen alle mit v_ℓ inzidenten Kanten auf W. Da laut unserer Voraussetzung die Anzahl dieser Kanten gerade ist, folgt $v_\ell = v_0$.

Zu zeigen: W ist ein Euler-Kreis.

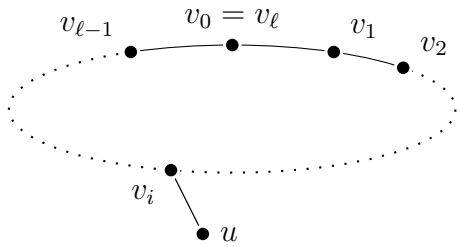
Angenommen, W ist *kein* Euler-Kreis.

Dann gibt es in G eine Kante e', die nicht auf W liegt. Da G zusammenhängend ist, gibt es einen Weg, der von einem Endknoten von e' zu einem zu W gehörenden Knoten führt. Sei e die erste Kante auf diesem Weg, die einen Endpunkt in W hat. Sei v_i der zu e inzidente Knoten aus W und sei $u \in V$ der andere zu e inzidente Knoten, d.h. $e = \{u, v_i\}$. Dann ist der Weg

$$W' \;:=\; (u, v_i, v_{i+1}, \ldots, v_{\ell-1}, v_0, v_1, \ldots, v_i)$$

ein Weg der Länge $\ell+1$, der keine Kante(n) mehrfach enthält.

Skizze für W:



Dies widerspricht aber der Tatsache, dass W ein Weg *maximaler* Länge ist.

(b) Die Richtung „$\Longrightarrow$“ folgt analog zu (a): Sei $K = (v_0, \ldots, v_\ell)$ ein Euler-Weg, der kein Euler-Kreis ist. Man sieht leicht, dass die beiden Endknoten von K ungeraden Grad haben, und dass alle anderen Knoten geraden Grad haben.

Zum Beweis der Richtung „$\Longleftarrow$“ kann man (a) verwenden: Seien x und y die beiden Knoten von G, die ungeraden Grad haben. Wir betrachten den Graphen $G' := (V', E')$ mit $V' := V \cup \{z\}$ und $E' := E \cup \{\{x, z\},\ \{y, z\}\}$, wobei z ein „neuer“ Knoten ist, der nicht zu V gehört.

Offensichtlich hat jeder Knoten in G' geraden Grad. Außerdem ist G' zusammenhängend (da G zusammenhängend ist). Aus (a) folgt, dass G' einen Euler-Kreis besitzt. Wegen $\text{Grad}_{G'}(z) = 2$ wird z auf diesem Kreis genau einmal besucht. Durch Entfernen der Kanten $\{x, z\}$ und $\{z, y\}$ erhält man einen Euler-Weg in G, der die beiden Knoten x und y als Anfangs- und Endpunkt hat. □

Folie 162

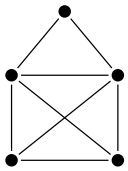
Lösung des Königsberger Brückenproblems

Beispiel 3.21.
Mit Hilfe von Satz 3.20 können wir das Königsberger Brückenproblem aus Beispiel 3.18 leicht lösen: Es gibt *keinen* Spaziergang, der jede der 7 Brücken genau einmal überquert und zum Ausgangspunkt zurückkehrt.

Beweis. Ein solcher Spaziergang würde gerade einem Euler-Kreis im Graphen $G_{\text{Königsberg}}$ entsprechen. Dieser Graph besitzt aber 4 Knoten von ungeradem Grad und kann daher laut Satz 3.20(a) keinen Euler-Kreis besitzen. □

Beispiel 3.22.
Unter Verwendung von Satz 3.20 kann man auch die folgende Frage leicht lösen.

Frage: Kann man die Figur



in einem Zug nachzeichnen? D.h: Besitzt dieser Graph einen Euler-Weg?

Unter Verwendung von Satz 3.20 kann man die Frage leicht beantworten, indem man nachzählt, wie viele Knoten von ungeradem Grad es gibt. Im obigen Graphen gibt es genau 2 Knoten von ungeradem Grad. Gemäß Satz 3.20 besitzt G also einen Euler-Weg, der kein Euler-Kreis ist.

Ähnlichkeit zweier Graphen

Teilgraphen und induzierte Teilgraphen

Die folgende Definition formalisiert, wann ein Graph G' in einem Graphen G „enthalten“ ist.

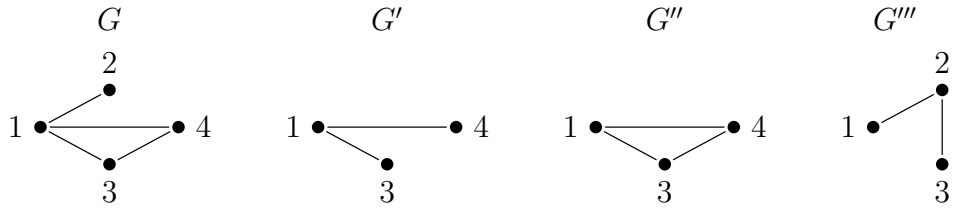
Definition 3.23.
Seien $G = (V, E)$ und $G' = (V', E')$ zwei (gerichtete oder ungerichtete) Graphen.

(a) G' heißt *Teilgraph von* G, falls $V' \subseteq V$ und $E' \subseteq E$.

(b) Sei $W \subseteq V$. Der *von* W *induzierte Teilgraph von* G ist der Graph $G|_W$ mit Knotenmenge W und Kantenmenge $E|_W := \{e \in E : \text{alle mit } e \text{ inzidenten Knoten liegen in } W\}$.

(c) $G' = (V', E')$ heißt *induzierter Teilgraph von* G, falls $V' \subseteq V$ und $E' = \{e \in E : \text{alle mit } e \text{ inzidenten Knoten liegen in } V'\}$ (d.h.: $V' \subseteq V$ und G' ist genau der von V' induzierte Teilgraph von G).

Beispiel. Wir betrachten die folgenden Graphen:



Dann ist

- G' ein Teilgraph von G, aber kein induzierter Teilgraph von G.
- G'' ein induzierter Teilgraph von G.
- G''' kein Teilgraph von G.

Folie 165

Gleichheit von Graphen

Definition 3.24.
Zwei Graphen $G = (V, E)$ und $G' = (V', E')$ sind *gleich* (kurz: $G = G'$), falls sie dieselbe Knotenmenge und dieselbe Kantenmenge besitzen. D.h.:

$$G = G' \quad :\Longleftrightarrow \quad V = V' \text{ und } E = E'.$$

Beispielsweise sind die beiden Graphen

nicht gleich, da sie unterschiedliche Knotenmengen besitzen. Intuitiv sind die beiden Graphen aber *„prinzipiell gleich“* (Fachbegriff: *isomorph*, kurz: $G \cong G'$), da der zweite Graph aus dem ersten durch Umbenennung der Knoten entsteht. Der Begriff der Isomorphie wird durch die folgende Definition präzisiert.

Isomorphie von Graphen

Definition 3.25.
Seien $G = (V, E)$ und $G' = (V', E')$ zwei (gerichtete oder ungerichtete) Graphen. G und G' heißen *isomorph* (kurz: $G \cong G'$, in Worten: G ist isomorph zu G'), falls es eine bijektive Abbildung $f : V \to V'$ gibt, so dass für alle Knoten $i \in V$ und $j \in V$ gilt:

- falls G und G' gerichtet sind:

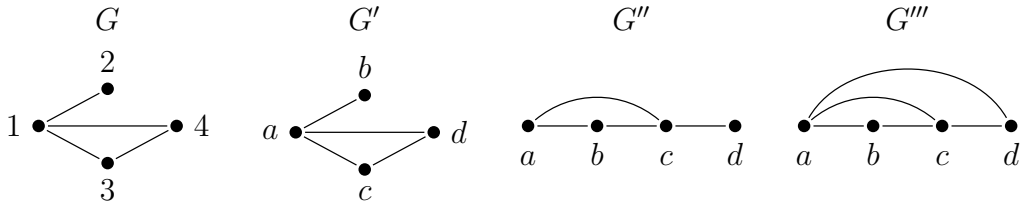
$$(i, j) \in E \quad \Longleftrightarrow \quad \big(f(i), f(j)\big) \in E'$$

- falls G und G' ungerichtet sind:

$$\{i, j\} \in E \quad \Longleftrightarrow \quad \{f(i), f(j)\} \in E'.$$

Eine solche Abbildung f wird *Isomorphismus von G nach G'* genannt.

Beispiel. Es seien:



Dann gilt:

- $G \cong G'$ via $f\colon \{1, 2, 3, 4\} \to \{a, b, c, d\}$ mit $f(1) = a$, $f(2) = b$, $f(3) = d$, $f(4) = c$.

  Ein weiterer Isomorphismus von G nach G' ist die Abbildung $g : \{1, 2, 3, 4\} \to \{a, b, c, d\}$ mit $g(1) = a$, $g(2) = b$, $g(3) = c$, $g(4) = d$.

- $G \cong G''$ via $f\colon \{1, 2, 3, 4\} \to \{a, b, c, d\}$ mit $f(1) = c$, $f(2) = d$, $f(3) = a$, $f(4) = b$.

  Ein weiterer Isomorphismus von G nach G'' ist die Abbildung $g : \{1, 2, 3, 4\} \to \{a, b, c, d\}$ mit $g(1) = c$, $g(2) = d$, $g(3) = b$, $g(4) = a$.

- G'' ist nicht isomorph zu G''', kurz: $G'' \ncong G'''$, da G''' *mehr* Kanten als G'' hat.

Markierte Graphen

Folie 167

Bemerkung 3.26.
Viele Modellierungsaufgaben erfordern, dass den Knoten oder den Kanten eines Graphen weitere Informationen zugeordnet werden. Dies wird durch so genannte *Markierungsfunktionen* für Knoten oder Kanten formalisiert:

(a) Eine *Knotenmarkierung* eines (gerichteten oder ungerichteten) Graphen $G = (V, E)$ ist eine Abbildung

$$m\colon V \to W,$$

wobei W ein geeigneter Wertebereich ist. In dem Graph aus Beispiel 3.1(a) könnte man beispielsweise eine Knotenmarkierung *Einwohnerzahl*: $V \to \mathbb{N}$ einführen, die jedem Knoten die Einwohnerzahl der zugehörigen Stadt zuordnet.

(b) Eine *Kantenmarkierung* von G ist eine Abbildung

$$m\colon E \to W,$$

wobei W ein geeigneter Wertebereich ist. In dem Graph aus Beispiel 3.1(a) könnte man beispielsweise eine Kantenmarkierung *Entfernung*: $E \to \mathbb{N}$ einführen, die jeder Kante die Länge (in km) des von der Kante repräsentierten Autobahnteilstücks zuordnet.

Folie 168

Multigraphen

Kantenmarkierungen kann man auch dazu verwenden, um auszudrücken, dass es zwischen zwei Knoten mehr als eine Kante gibt. Die Markierungsfunktion gibt dann an, für wie viele Verbindungen die eine Kante des Graphen steht:

Definition 3.27.
Ein *Multigraph* (G, m) besteht aus einem (gerichteten oder ungerichteten) Graphen $G = (V, E)$ und einer Kantenmarkierung $m\colon E \to \mathbb{N}$.

Beispiel. Sei $G = (V, E)$ der Graph mit $V = \{a, b, c\}$ und $E = \{\{a, b\}, \{b, c\}, \{c, a\}\}$. Sei $m : E \to \mathbb{N}$ mit $m(\{a, b\}) = 1$, $m(\{b, c\}) = 1$ und $m(\{c, a\}) = 2$. Dann ist (G, m) ein Multigraph, der graphisch wie folgt dargestellt werden kann:

Zuordnungsprobleme

Wir betrachten zunächst zwei typische Beispiele von Zuordnungsproblemen.

Folie 169

Beispiel 3.28.

(a) In einem Tennisverein sollen die Vereinsmitglieder für ein Turnier zu Doppelpaarungen zusammengestellt werden. Dabei möchte man jeweils nur befreundete Personen als „Doppel“ zusammen spielen lassen.

Um diese Aufgabe zu lösen, modellieren wir die Situation durch den ungerichteten Graphen $G_T := (V_T, E_T)$ mit

$$\begin{aligned} V_T &:= \{\, x \,:\, x \text{ ist ein Vereinsmitglied} \,\} \\ E_T &:= \{\, \{x, y\} \,:\, x \text{ und } y \text{ sind befreundete Vereinsmitglieder} \,\}. \end{aligned}$$

Das *Ziel* ist, eine größtmögliche Anzahl von Doppelpaarungen zu finden. D.h.: Wir wollen eine möglichst große Menge $E' \subseteq E_T$ finden, so dass kein Vereinsmitglied Endpunkt von mehr als einer Kante aus E' ist.

Folie 170

(b) Eine Gruppe unterschiedlich ausgebildeter Piloten soll so auf Flugzeuge verteilt werden, dass jeder das ihm zugeteilte Flugzeug fliegen kann.

Auch hier modellieren wir die Situation durch einen ungerichteten Graphen $G_F := (V_F, E_F)$ mit

$$\begin{aligned} V_F &:= \{x \,:\, x \text{ ist ein Pilot}\} \,\dot\cup\, \{y \,:\, y \text{ ist ein Flugzeug}\}, \\ E_F &:= \{\, \{x, y\} \,:\, \text{Pilot } x \text{ kann Flugzeug } y \text{ fliegen} \,\}. \end{aligned}$$

Das *Ziel* ist, einen Flugplan aufzustellen, so dass jeder Pilot das ihm zugeteilte Flugzeug fliegen kann. D.h.: Wir wollen eine möglichst große Menge $E' \subseteq E_F$ finden, so dass kein Element aus V_F Endpunkt von mehr als einer Kante in E' ist.

Die gesuchten Kantenmengen E' aus (a) und (b) werden *Matching* genannt:

Folie 171

Matchings

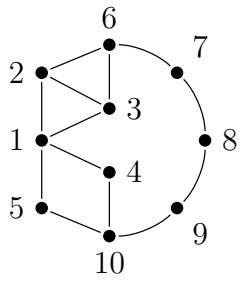
Definition 3.29.
Sei $G = (V, E)$ ein ungerichteter Graph. Eine Kantenmenge $E' \subseteq E$ heißt *Matching* (bzw. *Paarung* bzw. *Menge unabhängiger Kanten*), falls kein Knoten aus V Endpunkt von mehr als einer Kante aus E' ist.

Ziel in Beispiel 3.28 (a) und (b) ist es, ein Matching maximaler Größe zu finden, d.h. ein Matching, das so viele Kanten wie möglich enthält.

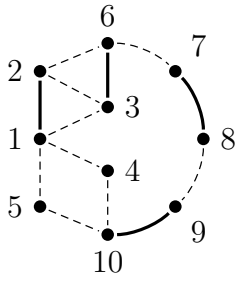
Folie 172

Beispiel 3.30. In einem Tennisverein mit 10 Mitgliedern und „Freundschaftsgraph“

G_T =

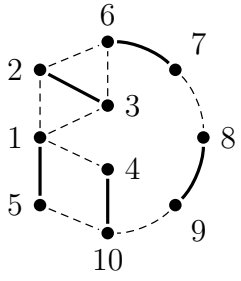


sind z.B. die folgenden beiden Kantenmengen Matchings:



$$E' = \{ \{1,2\}, \{3,6\}, \{7,8\}, \{9,10\} \}$$

und



$$E'' = \{ \{1,5\}, \{4,10\}, \{8,9\}, \{6,7\}, \{2,3\} \}.$$

Folie 173

In Beispiel 3.28(b) sollten Piloten auf Flugzeuge verteilt werden. Die Knotenmenge des zugehörigen Graphen G_F bestand aus zwei verschiedenen Arten von Objekten (nämlich einerseits Piloten und andererseits Flugzeuge), und Kanten konnten jeweils nur zwischen Objekten unterschiedlicher Art verlaufen (also zwischen Piloten und Flugzeugen, nicht aber zwischen Piloten und Piloten bzw. Flugzeugen und Flugzeugen). Solche Graphen werden *bipartite Graphen* genannt:

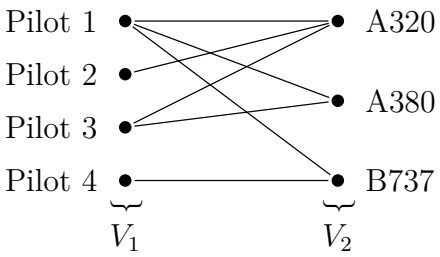
Folie 174

Bipartite Graphen

Definition 3.31.
Ein ungerichteter Graph $G = (V, E)$ heißt *bipartit*, wenn seine Knotenmenge V so in zwei disjunkte Teilmengen V_1 und V_2 zerlegt werden kann (d.h. $V = V_1 \dot\cup V_2$), dass jede Kante aus E einen Endknoten in V_1 und einen Endknoten in V_2 hat.

Beispiel 3.32.

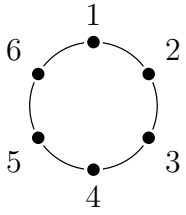
(a) Der Graph



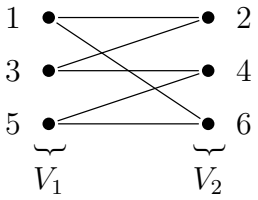
ist bipartit mit $V_1 = \{\text{Pilot 1}, \text{Pilot 2}, \text{Pilot 3}, \text{Pilot 4}\}$ und $V_2 = \{\text{A320}, \text{A380}, \text{B737}\}$.

Folie 175

(b) Der Graph

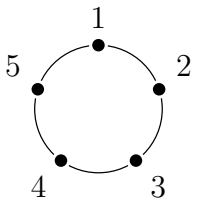


ist bipartit mit $V_1 = \{1, 3, 5\}$ und $V_2 = \{2, 4, 6\}$. Der Graph lässt sich auch wie folgt graphisch darstellen:



Folie 176

(c) Der Graph



ist *nicht* bipartit.

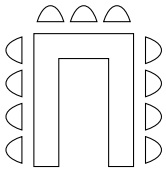
Beweis: Durch Widerspruch. Angenommen, er ist doch bipartit. Dann seien V_1 und V_2 die beiden disjunkten Teilmengen der Knotenmenge, so dass jede Kante des Graphen einen Endknoten in V_1 und einen Endknoten in V_2 hat. Wir können o.B.d.A. annehmen, dass $1 \in V_1$ ist (falls nicht, vertauschen wir einfach V_1 und V_2). Dann muss aber gelten: $2 \in V_2$, $3 \in V_1$, $4 \in V_2$ und $5 \in V_1$, also $V_1 = \{1, 3, 5\}$ und $V_2 = \{2, 4\}$. Im Graphen gibt es aber auch eine Kante zwischen 1 und 5, und beide Knoten gehören zu V_1. Dies ist ein Widerspruch zu der Annahme, dass jede Kante einen Endpunkt in V_1 und einen Endpunkt in V_2 hat. $\square$

Allgemein gilt: Ist $n \in \mathbb{N}_{\geqslant 1}$ und ist G ein Kreis auf n Knoten (wie in (b) für $n = 6$ und in (c) für $n = 5$), so gilt:

$$G \text{ ist bipartit} \quad \Longleftrightarrow \quad n \text{ ist gerade.}$$

Wir betrachten ein weiteres typisches Beispiel für ein Zuordnungsproblem:

Beispiel 3.33 (Sitzordnung bei einer Familienfeier)**.**
Die Gäste einer Familienfeier sollen so an einer hufeisenförmigen Tafel



platziert werden, dass niemand neben jemanden sitzt, den er nicht leiden kann.

Lösungsansatz:

Schritt 1: Stelle den *Konfliktgraphen* $G = (V, E)$ auf, wobei

$$V := \{x : \text{Person } x \text{ soll zur Feier kommen}\} \text{ und}$$
$$E := \left\{ \{x, y\} : \begin{array}{l} \text{Person } x \text{ kann Person } y \text{ nicht leiden oder} \\ \text{Person } y \text{ kann Person } x \text{ nicht leiden} \end{array} \right\}$$

d.h. Kanten im Konfliktgraphen zeigen auf, wer im Konflikt mit wem steht.

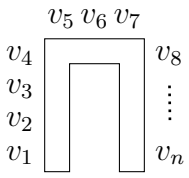
Schritt 2: Bilde das *Komplement des Konfliktgraphen*, d.h. betrachte den Graphen $\tilde{G} = (\tilde{V}, \tilde{E})$ mit

$$\tilde{V} := V \quad \text{und}$$
$$\tilde{E} := \big\{ \{x, y\} : x, y \in V,\, x \neq y,\, \{x, y\} \notin E \big\},$$

d.h. Kanten in $\tilde{G}$ zeigen an, wer prinzipiell neben wem platziert werden könnte.

Schritt 3: Suche einen Hamilton-Weg in $\tilde{G}$.

Wenn $(v_1, \ldots, v_n)$ (mit $n = |\tilde{V}|$) ein Hamilton-Weg in $\tilde{G}$ ist, dann kann man die Sitzordnung folgendermaßen festlegen:



Falls es in $\tilde{G}$ keinen Hamilton-Weg gibt, so weiß man, dass es *keine Möglichkeit gibt*, die geladenen Gäste so an einer hufeisenförmigen Tafel zu platzieren, dass niemand neben jemandem sitzt, den er nicht leiden kann.

Folie 179

Ein möglicher Ausweg ist, die Gäste an *mehrere* Tische zu verteilen. Dies kann wie folgt modelliert werden:

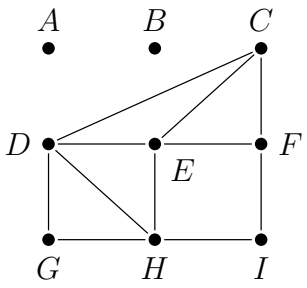
Beispiel 3.34 (Sitzordnung bei einer Familienfeier, Teil 2)**.**
Die Gäste einer Familienfeier sollen so an mehreren Tischen platziert werden, dass Personen, die sich nicht leiden können, an verschiedenen Tischen sitzen. Dabei sollen so wenig Tische wie möglich verwendet werden. Diese Aufgabe kann folgendermaßen modelliert werden: Die verfügbaren Tische werden mit den Zahlen $1, 2, 3, \ldots$ durchnummeriert. Die geladenen Gäste und die herrschenden Konflikte zwischen Gästen werden durch den in Beispiel 3.33 betrachteten Konfliktgraphen $G = (V, E)$ repräsentiert. Die Zuordnung, wer an welchem Tisch sitzen soll, wird durch eine Knotenmarkierung $m\colon V \to \mathbb{N}_{\geqslant 1}$ repräsentiert, wobei $m(x) = i$ bedeutet, dass Person x am Tisch i sitzen soll.
Das *Ziel* ist, eine *konfliktfreie Knotenmarkierung* $m\colon V \to \mathbb{N}_{\geqslant 1}$ zu finden. Dabei soll $|\text{Bild}(m)|$ möglichst klein sein — dies entspricht dem Ziel, die Gäste an möglichst wenige Tische zu verteilen.

Folie 180

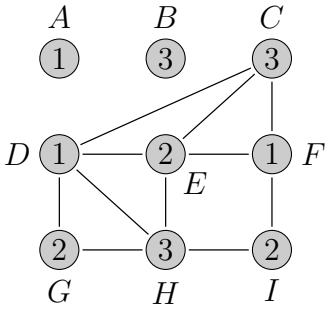
Konfliktfreie Knotenmarkierungen

Definition 3.35.
Sei $G = (V, E)$ ein ungerichteter Graph. Eine Funktion $m\colon V \to \mathbb{N}$ heißt *konfliktfreie Knotenmarkierung* (bzw. konfliktfreie *Färbung*), wenn für jede Kante $\{x, y\} \in E$ gilt: $m(x) \neq m(y)$.

Beispiel 3.36. Um Beispiel 3.34 fortzuführen, betrachten wir eine Familienfeier mit Gästen A, B, C, D, E, F, G, H, I und folgendem Konfliktgraphen:

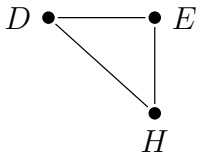


Die folgende Graphik gibt eine konfliktfreie Knotenmarkierung $m\colon V \to \mathbb{N}$ an, wobei für jeden Knoten $v \in V$ der Wert $m(v)$ in den Kreis geschrieben ist, der den Knoten v repräsentiert.



Folie 181

Für die hier gegebene Markierung m gilt $|\text{Bild}(m)| = 3$, die Gäste werden also an 3 Tische verteilt. Dies ist optimal, da der Konfliktgraph ein Dreieck, z.B.



als Teilgraph enthält — deshalb muss für jede konfliktfreie Knotenmarkierung m' gelten: $|\text{Bild}(m')| \geqslant 3$.

Folie 182

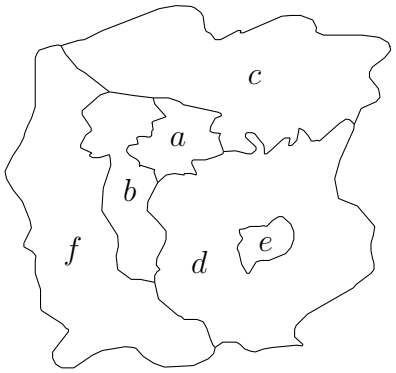
Bemerkung 3.37 (4-Farben-Problem)**.**
Ein sehr bekannter Vertreter dieser Art von Markierungs- oder Färbungsaufgaben ist das so genannte *4-Farben-Problem*. Dabei handelt es sich um die Frage, wie viele verschiedene Farben nötig sind, um jede Landkarte so einzufärben, dass zwei Staaten, die ein Stück gemeinsamer

Grenze haben, durch unterschiedliche Farben dargestellt werden. 1976 wurde bewiesen, dass vier Farben ausreichen. Der Beweis basiert auf einer Fallunterscheidung mit mehr als 1000 Fällen, die mit Hilfe eines Computerprogramms analysiert wurden.

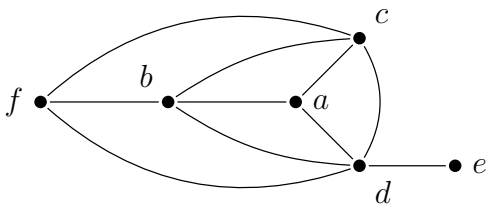
Das Problem, eine Landkarte einzufärben, kann durch einen ungerichteten Graphen modelliert werden, dessen Knoten gerade die Staaten repräsentieren, und bei dem es eine Kante zwischen zwei Staaten gibt, falls diese eine gemeinsame Grenze besitzen. Ziel ist, eine konfliktfreie Knotenmarkierung m zu finden, bei der $|\text{Bild}(m)|$ so klein wie möglich ist.

Folie 183

Beispiel:
Wir betrachten eine kleine Landkarte



und den zugehörigen Konfliktgraphen:



Knoten $\widehat{=}$ Staaten,
Kanten $\widehat{=}$ Staaten mit gemeinsamer Grenze

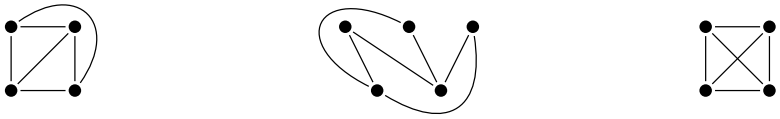
Da bei den vier Knoten a, b, c, d paarweise jeder zu jedem benachbart ist, muss eine konfliktfreie Färbung diesen vier Knoten vier verschiedene Farben zuordnen — für a, b, c, d etwa *rot*, *gelb*, *grün*, *blau*. Da f außerdem mit b, c, d benachbart ist, muss f dann wieder *rot* gefärbt sein; e kann jede Farbe außer *blau* erhalten.

Planare Graphen

Die aus Landkarten entstehenden Konfliktgraphen haben eine besondere Eigenschaft: sie sind *planar*.

Definition 3.38.
Ein Graph G heißt *planar*, wenn er so in die Ebene gezeichnet werden kann, dass seine Kanten sich nicht kreuzen.

Beispiele für planare Graphen sind:



Der dritte Graph ist planar, da er wie der erste Graph kreuzungsfrei in die Ebene gezeichnet werden kann.

Beispiele für nicht-planare Graphen sind:

Die chromatische Zahl eines Graphen

Bemerkung 3.39.
Die Anzahl verschiedener „Farben“ bzw. „Markierungen“, die nötig sind, um einen Graphen $G = (V, E)$ konfliktfrei zu färben (bzw. zu markieren), nennt man die *chromatische Zahl*, kurz: $\chi(G)$. Die präzise Definition ist[4]

$$\chi(G) \;:=\; \min\left\{ |\text{Bild}(m)| \;:\; \begin{array}{l} m : V \to \mathbb{N} \text{ ist eine konfliktfreie} \\ \text{Knotenmarkierung für } G \end{array} \right\}.$$

Weitere Beispiele für Zuordnungsprobleme, die durch Graphen modelliert werden können, finden sich in den Übungsaufgaben.

[4] Ist M eine endliche, nicht-leere Menge von Zahlen, so bezeichnet $\min M$ das kleinste Element von M.

3.2 Bäume

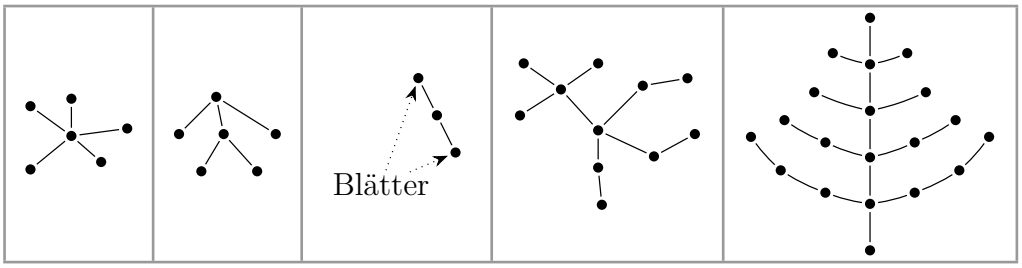
Eine für die Informatik besonders wichtige Art von Graphen sind die so genannten *Bäume*. Wir betrachten im Folgenden zunächst ungerichtete Bäume und danach gerichtete Bäume.

Ungerichtete Bäume

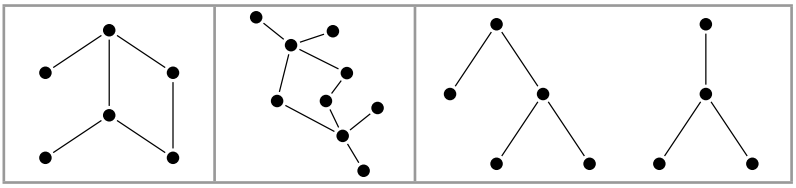
Folie 186

Definition 3.40 (ungerichteter Baum)**.**
Ein *ungerichteter Baum* ist ein ungerichteter, zusammenhängender Graph $G = (V, E)$, der keinen einfachen Kreis enthält.
Diejenigen Knoten in V, die den Grad $\leqslant 1$ haben, heißen *Blätter* des Baums.

Beispiel. Folgende Graphen sind Bäume:



Folgende Graphen sind keine Bäume:



Folie 187

Beobachtung 3.41. *Ist $B = (V, E)$ ein ungerichteter Baum, so gilt für alle Knoten $x, y \in V$:*

Es gibt in B genau einen einfachen Weg von x nach y.

Denn: B ist ein ungerichteter Baum, d.h. B ist zusammenhängend und enthält keinen einfachen Kreis. Da B zusammenhängend ist, gibt es mindestens einen einfachen Weg von x nach y. Angenommen, $(v_0, \ldots, v_\ell)$ und $(v'_0, \ldots, v'_{\ell'})$ sind zwei verschiedene einfache Wege von x nach y. Insbesondere gilt dann $v_0 = x = v'_0$ und $v_\ell = y = v'_{\ell'}$.

Skizze:

Dann ist aber $(v_0, \ldots, v_\ell, v'_{\ell'-1}, \ldots, v'_0)$ ein Kreis. Dieser Kreis enthält einen einfachen Kreis. Dann kann B aber kein Baum sein. Widerspruch. □

Folie 188

Satz 3.42.
Jeder endliche ungerichtete Baum $B = (V, E)$ mit $V \neq \emptyset$ besitzt mindestens ein Blatt.

Beweis. Sei $B = (V, E)$ ein endlicher ungerichteter Baum mit $V \neq \emptyset$.
Sei $W := (v_0, \ldots, v_\ell)$ ein einfacher Weg maximaler Länge in B. Dann ist $\ell \geqslant 0$, da $V \neq \emptyset$. Außerdem ist $\ell < |V|$, da W einfach ist (d.h. die in W vorkommenden Knoten $v_0, \ldots, v_\ell$ sind paarweise verschieden — und in V gibt es nur $|V|$ viele verschiedene Knoten). Wir betrachten zwei Fälle:

Fall 1: $\ell = 0$.
Da B ein Baum ist (d.h. insbesondere zusammenhängend) und $W = (v_0)$ ein einfacher Weg maximaler Länge, muss dann $V = \{v_0\}$ und $E = \emptyset$ sein. Insbesondere ist v_0 ein Blatt von B.

Fall 2: $\ell \geqslant 1$.
Dann ist $v_{\ell-1}$ ein Nachbar von v_ℓ. Angenommen, v_ℓ ist kein Blatt. Dann hat v_ℓ einen weiteren Nachbarn, den wir im Folgenden u nennen.
Falls u nicht in W vorkommt, so ist $(v_0, \ldots, v_\ell, u)$ ein einfacher Weg, der länger ist als W. Dies widerspricht unserer Wahl von W als einfachem Weg maximaler Länge.
Falls u in W vorkommt, so gibt es ein i mit $u = v_i$ und $0 \leqslant i < \ell - 1$ (da u ein von den Knoten v_ℓ und $v_{\ell-1}$ verschiedener Knoten ist). Dann ist $(v_i, \ldots, v_{\ell-1}, v_\ell, v_i)$ ein einfacher Kreis in B. Dies widerspricht aber der Tatsache, dass B ein ungerichteter Baum ist.
Insgesamt kann es also keinen von $v_{\ell-1}$ verschiedenen Nachbarn u von v_ℓ geben. D.h. v_ℓ ist ein Blatt. □

Der folgende Satz, für dessen Beweis wir Satz 3.42 benutzen, besagt, dass die Anzahl der Kanten eines ungerichteten Baums durch die Anzahl der Knoten genau festgelegt ist.

Satz 3.43 (Anzahl der Kanten eines Baums)**.**
Für jeden endlichen ungerichteten Baum $B = (V, E)$ mit $V \neq \emptyset$ gilt:
$|E| = |V| - 1$.

Beweis. Per Induktion nach $n := |V|$.

Induktionsanfang: $n = 1$

Der einzige ungerichtete Baum $B = (V, E)$ mit $|V| = 1$ ist der Graph • mit $E = \emptyset$. Für diesen Graphen gilt: $|E| = 0 = 1 - 1 = |V| - 1$.

Induktionsschritt: $n \to n{+}1$

Sei $n \in \mathbb{N}$ mit $n \geqslant 1$ beliebig.

Induktionsannahme:
Für jeden ungerichteten Baum $B' = (V', E')$ mit $V' \neq \emptyset$ und $|V'| \leqslant n$ gilt: $|E'| \;=\; |V'| - 1$.

Behauptung:
Für jeden ungerichteten Baum $B = (V, E)$ mit $V \neq \emptyset$ und $|V| = n{+}1$ gilt: $|E| \;=\; |V| - 1$.

Beweis: Sei $B = (V, E)$ ein ungerichteter Baum mit $|V| = n{+}1$. Gemäß Satz 3.42 besitzt B (mindestens) ein Blatt, das wir im Folgenden u nennen. Da B zusammenhängend ist und $|V| = n{+}1 \geqslant 2$ ist, besitzt u einen Nachbarn v in B — und da u ein Blatt ist, ist v der einzige Nachbar von u in B.
Sein nun B' der Graph, der aus B entsteht, indem wir den Knoten u und die von v zu u führende Kante löschen. D.h., $B' = (V', E')$ mit $V' := V \setminus \{u\}$ und $E' := E \setminus \{\{v, u\}\}$. Man sieht leicht, dass B' zusammenhängend ist und keinen einfachen Kreis enthält. D.h., B' ist ein Baum. Außerdem ist $|V'| = n$. Aus der Induktionsannahme folgt daher, dass $|E'| = |V'| - 1$ ist. Insgesamt gilt daher für den Baum B:

$$|E| \;=\; |E'| + 1 \;=\; (|V'| - 1) + 1 \;=\; |V'| \;=\; |V| - 1.$$

□

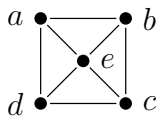
Folie 190

Spannbäume

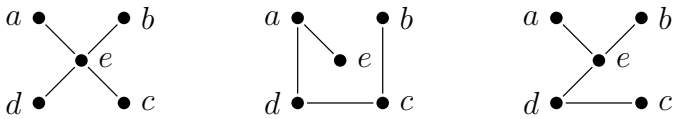
Bäume finden sich als Teilgraphen von zusammenhängenden Graphen. Besonders wichtig für die Informatik sind die so genannten *Spannbäume*.

Definition 3.44.
Sei $G = (V, E)$ ein ungerichteter Graph. Ein Graph $G' = (V', E')$ heißt *Spannbaum von* G, falls G' ein ungerichteter Baum mit $V' = V$ und $E' \subseteq E$ ist.

Beispiel 3.45. Der Graph



hat u.a. folgende Spannbäume:



Folie 191

Jeder zusammenhängende Graph besitzt einen Spannbaum. Es gilt:

Satz 3.46. *Sei $G = (V, E)$ ein ungerichteter Graph, dessen Knotenmenge endlich ist. Dann gilt:*

Es gibt (mindestens) einen Spannbaum von G
$$\Longleftrightarrow$$
G ist zusammenhängend.

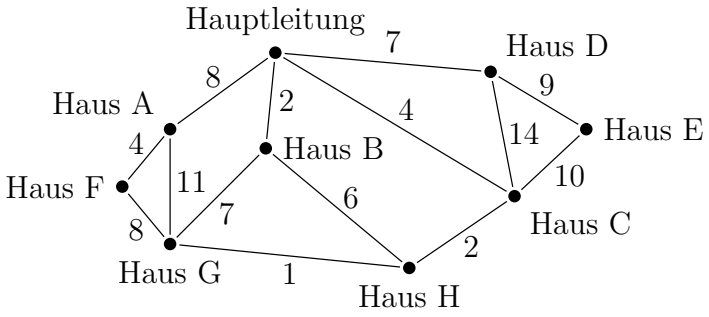
Beweis. „$\Longrightarrow$“: klar. „$\Longleftarrow$“: Übungsaufgabe. □

Folie 192

Geht man von einem zusammenhängenden Graphen zu einem seiner Spannbäume über, so verkleinert man gemäß Satz 3.43 die Kantenmenge von $|E|$ auf $|V| - 1$ Kanten, ohne dabei den Zusammenhang des Graphen aufzugeben. Mit dem Begriff des Spannbaums wird also ein „bezüglich der Kantenzahl kostengünstigerer Zusammenhang“ modelliert.
Manche konkreten Probleme lassen sich durch Graphen modellieren, deren Kanten mit bestimmten Werten markiert sind, so dass zur Lösung des Problems ein Spannbaum gesucht wird, bei dem die Summe seiner Kantenmarkierungen so klein wie möglich ist. Dazu betrachten wir das folgende Beispiel.

Folie 193

Beispiel 3.47 (Kabelfernsehen)**.** Eine Firma will Leitungen zum Empfang von Kabelfernsehen in einem neuen Wohngebiet verlegen. Der folgende Graph skizziert das Wohngebiet:



Knoten entsprechen dabei einzelnen Häusern bzw. der Hauptleitung, die aus einem bereits verkabelten Gebiet heranführt. Eine Kante zwischen zwei Knoten zeigt an, dass es prinzipiell möglich ist, eine direkte Leitung zwischen den beiden Häusern zu verlegen. Der Wert, mit dem die Kante markiert ist, beschreibt, wie teuer (in 1000 €) es ist, diese Leitung zu verlegen.

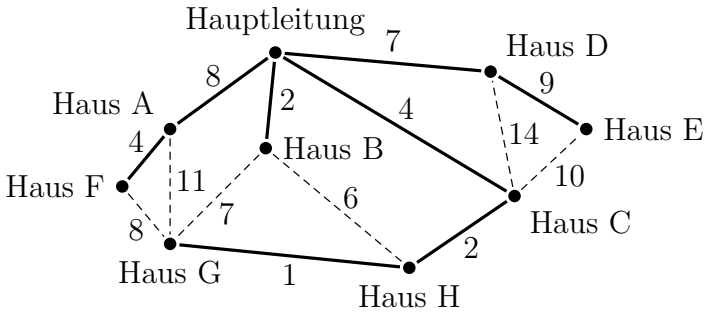
Folie 194

Ziel ist, Leitungen so zu verlegen, dass

(1) jedes Haus ans Kabelfernsehen angeschlossen ist und

(2) die Kosten für das Verlegen der Leitungen so gering wie möglich sind.

Es wird also ein Spannbaum gesucht, bei dem die Summe seiner Kantenmarkierungen so klein wie möglich ist. Ein solcher Spannbaum wird *minimaler Spannbaum* (engl.: *minimum spanning tree*) genannt. Die im Folgenden **fett** gezeichneten Kanten geben die Kanten eines minimalen Spannbaums an:



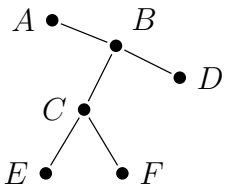
Verlegt die Firma genau diese Leitungen, so hat sie das neue Wohngebiet mit den geringstmöglichen Kosten ans Kabelfernsehen angeschlossen.

Gerichtete Bäume

Folie 195

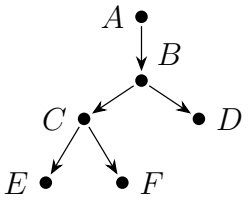
Einen *gerichteten Baum* erhält man, indem man in einem ungerichteten Baum einen Knoten als „Wurzel“ auswählt und alle Kanten in die Richtung orientiert, die von der Wurzel weg führt.

Beispiel 3.48. Ungerichteter Baum:



- Zugehöriger gerichteter Baum mit Wurzel A:

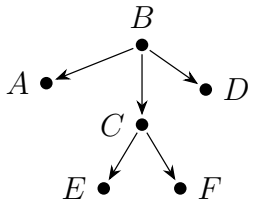
$G_A :=$



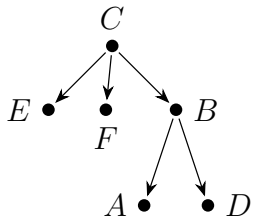
Folie 196

- Zugehöriger gerichteter Baum mit Wurzel B:

$G_B :=$



- Zugehöriger gerichteter Baum mit Wurzel C:

$G_C :=$ 

Folie 197

Die präzise Definition des Begriffs „gerichteter Baum“ ist wie folgt:

Definition 3.49 (gerichteter Baum)**.**
Ein gerichteter Graph $G = (V, E)$ heißt *gerichteter Baum*, falls er folgende Eigenschaften hat:

(1) G besitzt genau einen Knoten $w \in V$ mit Ein-Grad$_G(w) = 0$.
Dieser Knoten wird *Wurzel* genannt.

(2) Für jeden Knoten $v \in V$ gilt: Es gibt in G einen Weg von der Wurzel zum Knoten v.

(3) Für jeden Knoten $v \in V$ gilt: Ein-Grad$_G(v) \leqslant 1$.

Folie 198

Definition 3.50 (Blätter, innere Knoten, Höhe)**.**

(a) Sei $B = (V, E)$ ein gerichteter Baum. Diejenigen Knoten, deren Aus-Grad 0 ist, heißen *Blätter*.

Beispiel: In Beispiel 3.48 hat G_A die Blätter D, E, F. G_B hat die Blätter A, D, E, F und G_C die Blätter A, D, E, F.

(b) Diejenigen Knoten eines gerichteten Baums, die weder Wurzel noch Blätter sind, heißen *innere Knoten*.

(c) Sei $B = (V, E)$ ein gerichteter Baum. Die *Höhe* (bzw. *Tiefe*, engl.: height, depth) von B ist die Länge eines längsten Weges in B.

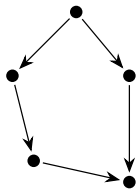
Beispiel: In Beispiel 3.48 hat G_A die Höhe 3, G_B die Höhe 2 und G_C die Höhe 2.

Folie 199

Beobachtung 3.51.

(a) Jeder gerichtete Baum ist ein gerichteter azyklischer Graph (kurz: DAG, vgl. Definition 3.14). Aber es gibt gerichtete azyklische Graphen, die keine gerichteten Bäume sind.

Beispiel:



ist ein DAG, aber kein gerichteter Baum.

Folie 200

(b) Für jeden gerichteten Baum $B = (V, E)$, dessen Knotenmenge endlich und nicht-leer ist, gilt:

$$|E| \;=\; |V| - 1.$$

Dies folgt unmittelbar aus Satz 3.43, da der ungerichtete Graph, der entsteht, indem man in B die Kantenorientierung „vergisst“ (d.h. jede gerichtete Kante (i, j) durch die ungerichtete Kante $\{i, j\}$ ersetzt), ein ungerichteter Baum ist.

Folie 201

Alternativ zu Definition 3.49 kann man die gerichteten Bäume, deren Knotenmenge endlich und nicht-leer ist, auch folgendermaßen definieren:

Definition 3.52 (gerichtete Bäume, rekursive Definition)**.**
Die Klasse der gerichteten Bäume mit endlicher, nicht-leerer Knotenmenge ist rekursiv wie folgt definiert:

Basisregel: Ist V eine Menge mit $|V| = 1$, so ist $B := (V, \emptyset)$ ein gerichteter Baum.

Skizze: $B :=$ •

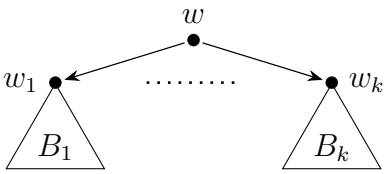
Der (eindeutig bestimmte) Knoten in V heißt *Wurzel* von B.
Die *Höhe* von B ist 0.

Rekursive Regel: Ist $k \in \mathbb{N}_{\geqslant 1}$, sind $B_1 = (V_1, E_1), \ldots, B_k = (V_k, E_k)$ gerichtete Bäume mit paarweise disjunkten Knotenmengen[5], sind $w_1 \in V_1, \ldots, w_k \in V_k$ die Wurzeln von $B_1, \ldots, B_k$, und ist w ein Element, das nicht in $V_1 \cup \cdots \cup V_k$ liegt, dann ist der Graph $B = (V, E)$ mit

$$V := \{w\} \cup V_1 \cup \cdots \cup V_k \quad \text{und}$$
$$E := E_1 \cup \cdots \cup E_k \cup \{\, (w, w_i) \,:\, i \in \{1, \ldots, k\} \,\}$$

ein gerichteter Baum.

Skizze: $B :=$

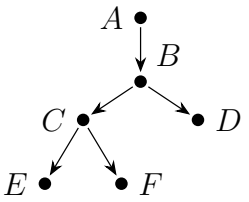


Der Knoten w heißt *Wurzel* von B.
Die *Höhe* von B ist $1 + \max\{h_1, \ldots, h_k\}$, wobei $h_1, \ldots, h_k \in \mathbb{N}$ die Höhen der gerichteten Bäume $B_1, \ldots, B_k$ sind.

Notation 3.53 (Kinder eines Knotens)**.**
Sei $B = (V, E)$ ein gerichteter Baum und sei $v \in V$ ein beliebiger Knoten in B. Die Knoten $v' \in V$, zu denen von v aus eine Kante führt (d.h. $(v, v') \in E$), heißen *Kinder* von v.

Beispiel. Im Graphen

$G_A =$



aus Beispiel 3.48 gilt: Knoten A hat genau ein Kind, nämlich B; Knoten B hat genau zwei Kinder, nämlich C und D; Knoten C hat genau zwei Kinder, nämlich E und F; und die Knoten D, E, F haben keine Kinder.

Folie 204

Eine besondere Rolle bei der Modellierung spielen Bäume, bei denen jeder Knoten höchstens zwei Kinder hat.

Definition 3.54 (Binärbaum, vollständiger Binärbaum)**.**

(a) Ein gerichteter Baum $B = (V, E)$ heißt *Binärbaum*, falls für jeden Knoten $v \in V$ gilt: Aus-Grad$_B(v) \leqslant 2$.

(b) Ein Binärbaum $B = (V, E)$ heißt *vollständiger Binärbaum*, falls gilt:

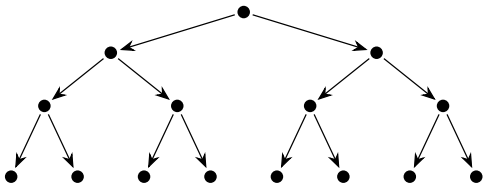
(1) Jeder Knoten, der kein Blatt ist, hat Aus-Grad 2, und

(2) es gibt eine Zahl $h \in \mathbb{N}$, so dass für jedes Blatt $v \in V$ gilt: Der Weg von der Wurzel zum Blatt v hat die Länge h.

Beispiel 3.55. Der Graph G_A aus Beispiel 3.48 ist ein Binärbaum, aber kein vollständiger Binärbaum. Der Graph G_B aus Beispiel 3.48 ist kein Binärbaum.

Folie 205

Der folgende Graph B_3 ist ein *vollständiger Binärbaum* der Höhe 3:



Folie 206

Zwischen der Höhe, der Anzahl der Blätter und der Anzahl der Knoten eines Binärbaums besteht der folgende wichtige Zusammenhang:

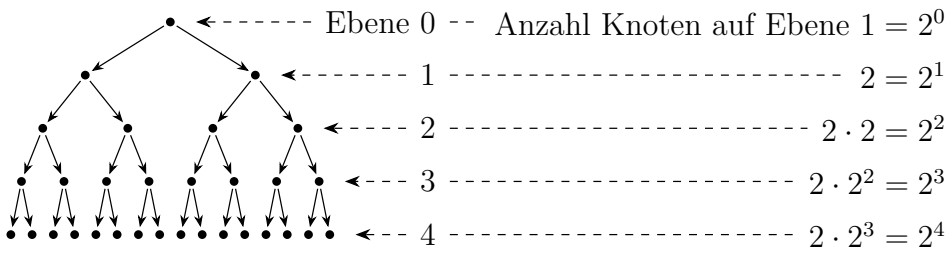
Satz 3.56. *Sei $h \in \mathbb{N}$.*

(a) Jeder vollständige Binärbaum der Höhe h hat genau 2^h Blätter und genau $2^{h+1} - 1$ Knoten.

(b) Jeder Binärbaum der Höhe h hat höchstens 2^h Blätter und höchstens $2^{h+1} - 1$ Knoten.

Beweis. (a) *Skizze:*

[5] D.h. $V_i \cap V_j = \emptyset$ f.a. $i, j \in \{1, \ldots, k\}$ mit $i \neq j$.



Anhand dieser Skizze sieht man leicht, dass ein vollständiger Binärbaum der Höhe h genau 2^h Blätter und

$$2^0 + 2^1 + 2^2 + \cdots + 2^h \overset{\text{Satz 2.52}}{=} 2^{h+1} - 1$$

Knoten besitzt.

Den formalen Beweis führen wir per Induktion nach h:

INDUKTIONSANFANG: $h = 0$:
Für jeden gerichteten Baum $B = (V, E)$ der Höhe 0 gilt: $|V| = 1$ und $|E| = 0$. D.h. B besteht aus genau einem Knoten, der gleichzeitig Wurzel und (einziges) Blatt des Baums ist. D.h: B hat genau $1 = 2^0 = 2^h$ Blätter und genau $1 = 2 - 1 = 2^1 - 1 = 2^{h+1} - 1$ Knoten.

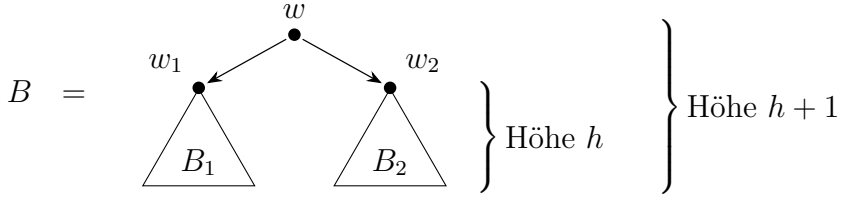
INDUKTIONSSCHRITT: $h \to h + 1$:
Sei $h \in \mathbb{N}$ beliebig.

Induktionsannahme: Jeder vollständige Binärbaum der Höhe h hat genau 2^h Blätter und genau $2^{h+1} - 1$ Knoten.

Behauptung: Jeder vollständige Binärbaum der Höhe $h{+}1$ hat genau 2^{h+1} Blätter und genau $2^{h+2} - 1$ Knoten.

Beweis: Sei $B = (V, E)$ ein vollständiger Binärbaum der Höhe $h{+}1$, und sei $w \in V$ die Wurzel von B. Wegen $h{+}1 \geqslant 1$ hat w genau 2 Kinder. Seien $w_1 \in V$ und $w_2 \in V$ diese beiden Kinder von w. Für $i \in \{1, 2\}$ sei V_i die Menge aller Knoten aus V, zu denen von w_i aus ein Weg führt; und sei $B_i := (V_i, E_i)$ der induzierte Teilgraph von B mit Knotenmenge V_i.

Skizze:



Offensichtlich ist sowohl B_1 als auch B_2 ein vollständiger Binärbaum der Höhe h. Gemäß Induktionsannahme hat jeder der beiden Bäume B_1 und B_2 genau 2^h Blätter und genau $2^{h+1} - 1$ Knoten.

Der Baum B hat daher genau $2^h + 2^h = 2^{h+1}$ Blätter und genau $1 + (2^{h+1} - 1) + (2^{h+1} - 1) = 2 \cdot 2^{h+1} - 1 = 2^{h+2} - 1$ Knoten.

(b) Analog. Details: Übungsaufgabe.

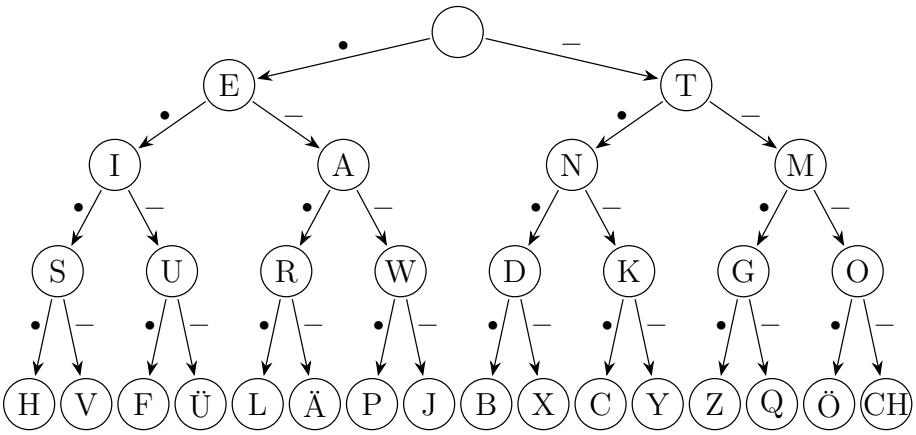
□

Modellierungsbeispiele

Gerichtete Bäume mit Knoten- oder Kantenmarkierungen können auf vielfältige Arten zur Modellierung genutzt werden.

Folie 207

Beispiel 3.57. Folgen von Entscheidungen können in vielen Zusammenhängen durch gerichtete markierte Bäume modelliert werden. Solche Bäume heißen *Entscheidungsbäume*. Durch einen solchen Entscheidungsbaum erhält man beispielsweise eine kompakte Darstellung des *Morse-Codes*. Im Morse-Code wird jeder Buchstabe durch eine Folge von kurzen und langen Signalen repräsentiert. Ein „kurzes Signal“ wird im folgenden Baum als Kantenmarkierung „•“ dargestellt; ein „langes Signal“ wird als „–“ dargestellt. Insgesamt wird der Morsecode durch folgenden Entscheidungsbaum repräsentiert: $M :=$



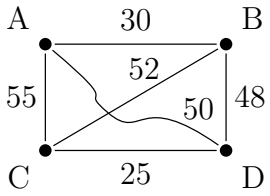
Eine eingehende Meldung aus kurzen und langen Signalen wird entschlüsselt, indem man an der Wurzel des Baums M beginnt und bei einem kurzen Signal nach links, bei einem langen nach rechts weitergeht. Eine längere Pause zeigt an, dass ein Buchstabe vollständig übermittelt ist.

Folie 208

In jedem Entscheidungsbaum modellieren die Knoten einen Zwischenstand bei der Entscheidungsfindung. Sie können entsprechend markiert sein, z.B. mit dem codierten Buchstaben des Morse-Codes. Die Kanten, die von einem Knoten ausgehen, modellieren die Alternativen, aus denen in dem durch den Knoten repräsentierten „Zustand“ eine ausgewählt werden kann. Beim Morse-Code ist das jeweils ein kurzes oder ein langes Signal, das als Kantenmarkierung angegeben wird.

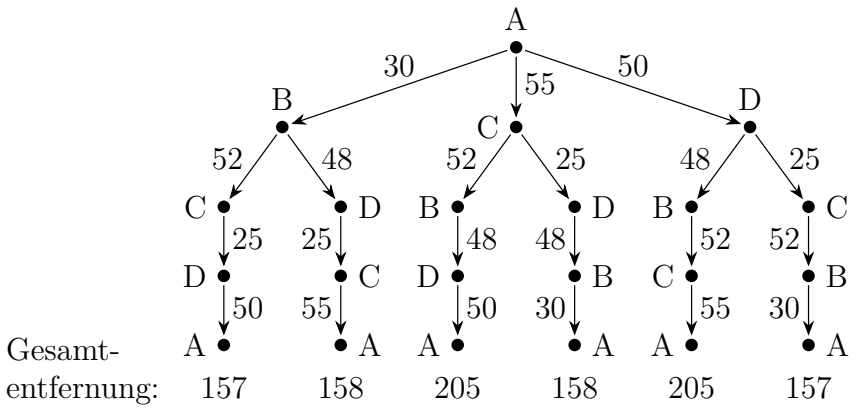
Folie 209

Beispiel 3.58. Markierte Bäume können auch genutzt werden, um den Lösungsraum kombinatorischer Probleme darzustellen. Als Beispiel betrachten wir einen Handlungsreisenden, der einen möglichst kurzen Rundweg finden soll, auf dem er jede der Städte A, B, C, D besucht. Die Entfernungen (in km) zwischen den Städten sind als Kantenmarkierungen des folgenden Graphen gegeben:



Der folgende Baum repräsentiert alle möglichen in Stadt A startenden Rundwege:

Folie 210



Jeder Weg von der Wurzel zu einem Blatt repräsentiert dabei einen Rundweg, auf dem jede der Städte genau einmal besucht wird. Die Kantenmarkierungen geben die Entfernungen zwischen einzelnen Städten wieder. Eine zusätzliche Knotenmarkierung an jedem Blatt gibt die Gesamtlänge des entsprechenden Rundwegs an. Die beiden kürzesten Rundwege für unseren Handlungsreisenden sind also

$$(A, B, C, D, A) \quad \text{und} \quad (A, D, C, B, A).$$

Folie 211

Bemerkung 3.59. Nach dem gleichen Schema kann man auch Zugfolgen in Spielen modellieren: Jeder Knoten des Entscheidungsbaums modelliert einen Spielzustand. Die von dort ausgehenden Kanten geben an, welche Möglichkeiten für den nächsten Zug bestehen. Solche Darstellungen werden z.B. in Schachprogrammen verwendet, um die Folgen der anstehenden Entscheidung zu analysieren und zu bewerten.

Beachte. Bei der Modellierung von Spielabläufen können manche „Spielzustände“ (z.B. Konfigurationen eines Schachbretts) auf unterschiedlichen Wegen (d.h. Spielverläufen) erreicht werden, und trotzdem „im Sinne des Spiels“ den selben Zustand beschreiben. In solchen Fällen könnte man im Entscheidungsbaum die zugehörigen Knoten zu einem einzigen Knoten zusammenfassen. Damit geht dann allerdings die Baum-Eigenschaft verloren, und es entsteht ein allgemeiner gerichteter Graph, der auch Kreise enthalten kann. Ein Kreis entspricht dann der Situation, dass eine Folge von Spielzügen in einen Zustand zurückführt, der früher schon einmal durchlaufen wurde.

3.3 Einige spezielle Arten von Graphen

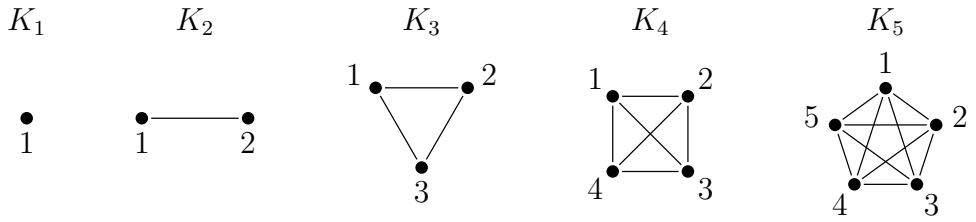
In diesem Abschnitt werden einige spezielle Arten von Graphen vorgestellt, die eine wichtige Rolle in der Informatik spielen.

Spezielle ungerichtete Graphen

Folie 212

Definition 3.60 (Der vollständige Graph K_n)**.**
Sei $n \in \mathbb{N}_{\geqslant 1}$. Der *vollständige ungerichtete Graph* K_n hat Knotenmenge $\{1, \ldots, n\}$ und Kantenmenge $\big\{\, \{i, j\} \,:\, i, j \in \{1, \ldots, n\},\, i \neq j \,\big\}$.

Beispiele.



Beobachtung 3.61. *Der Graph K_n hat n Knoten und* $\dfrac{n \cdot (n-1)}{2}$ *Kanten.*

Folie 213

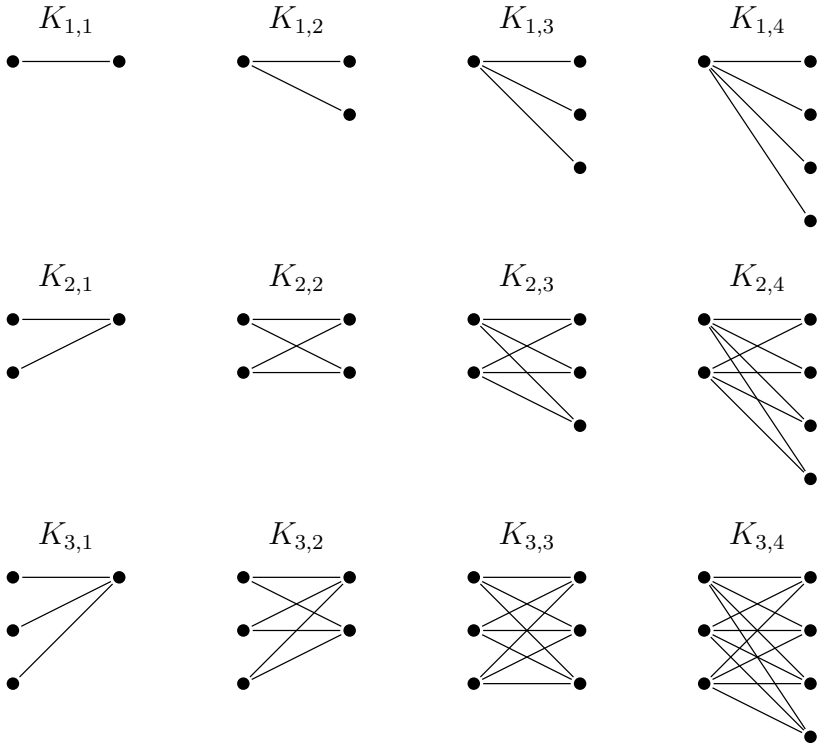
Definition 3.62 (Der vollständige bipartite Graph $K_{m,n}$)**.**
Seien $m, n \in \mathbb{N}_{\geqslant 1}$. Der *vollständige ungerichtete bipartite Graph* $K_{m,n}$ hat Knotenmenge

$$\big\{\, (1,i) \,:\, i \in \{1,\ldots,m\} \,\big\} \;\cup\; \big\{\, (2,j) \,:\, j \in \{1,\ldots,n\} \,\big\}$$

und Kantenmenge

$$\big\{\, \{\, (1,i),\, (2,j) \,\} \,:\, i \in \{1,\ldots,m\},\; j \in \{1,\ldots,n\} \,\big\}.$$

Beispiele.



Beobachtung 3.63. *Der Graph $K_{m,n}$ hat $m+n$ Knoten und $m \cdot n$ Kanten.*

Folie 214

Notation 3.64. Ein ungerichteter Graph G mit endlicher, nicht-leerer Knotenmenge heißt

(a) *vollständig*, falls es ein $n \in \mathbb{N}_{\geqslant 1}$ gibt, so dass $G \cong K_n$ (d.h. G ist isomorph zu K_n).

(b) *vollständig bipartit*, falls es Zahlen $m, n \in \mathbb{N}_{\geqslant 1}$ gibt, so dass $G \cong K_{m,n}$.

Spezielle gerichtete Graphen

Folie 215

Gemäß Definition 3.6 („gerichteter Graph“) und Definition 2.26(c) („k-stellige Relation“) kann jeder gerichtete Graph $G = (V, E)$ als eine 2-stellige Relation über V aufgefasst werden, da die Kantenmenge E von G ja gerade eine Teilmenge von $V^2 = V \times V$ ist. Umgekehrt können wir natürlich auch jede 2-stellige Relation R über einer Menge V als gerichteten Graph mit Knotenmenge V und Kantenmenge R auffassen. *Gerichtete Graphen mit Knotenmenge V sind also dasselbe wie 2-stellige Relationen über einer Menge V.*

Von besonderem Interesse sind 2-stellige Relationen, die eine oder mehrere der folgenden Eigenschaften besitzen:

Folie 216

Definition 3.65.
Sei E eine 2-stellige Relation über einer Menge V (d.h. $G = (V, E)$ ist ein gerichteter Graph).

(a) E heißt *reflexiv*, falls für alle $v \in V$ gilt:

$$(v, v) \in E. \qquad \text{(Skizze: } v \text{)}$$

(b) E heißt *symmetrisch*, falls f.a. $v, w \in V$ gilt:

$$\text{Wenn } (v, w) \in E, \text{ dann auch } (w, v) \in E.$$

(D.h.: Zu jeder Kante $v \longrightarrow w$ gibt es auch eine „Rückwärtskante“ $v \longleftarrow w$.)

(c) E heißt *antisymmetrisch*, falls f.a. $v, w \in V$ gilt:

$$\text{Wenn } (v,w) \in E \text{ und } (w,v) \in E, \text{ dann } v = w.$$

(D.h: Ist $v \neq w$, so gibt es in E allenfalls eine der beiden Kanten $v \longrightarrow w$ und $v \longleftarrow w$.)

Folie 217

(d) E heißt *konnex*, falls f.a. $v, w \in V$ mit $v \neq w$ gilt:

$$(v,w) \in E \quad \text{oder} \quad (w,v) \in E.$$

(d.h.: Ist $v \neq w$, so liegt mindestens eine der beiden Kanten $v \longrightarrow w$ und $v \longleftarrow w$ in E.)

(e) E heißt *transitiv*, falls f.a. $v, w, u \in V$ gilt:

$$\text{Ist } (v,w) \in E \text{ und } (w,u) \in E, \text{ so auch } (v,u) \in E.$$

Äquivalenzrelationen

Folie 218

Definition 3.66 (Äquivalenzrelation)**.**
Eine *Äquivalenzrelation* auf einer Menge V ist eine 2-stellige Relation über V, die *reflexiv*, *transitiv* und *symmetrisch* ist.

Beispiel 3.67. Beispiele für Äquivalenzrelationen:

(a) *Gleichheit:* Für jede Menge M ist

$$E \;:=\; \{\, (m,m) \,:\, m \in M \,\}$$

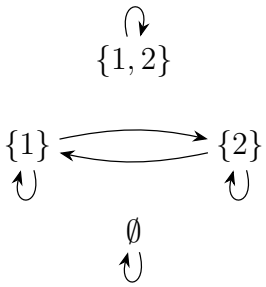
eine Äquivalenzrelation auf M. Die Aussage „$(x,y) \in E$“ entspricht gerade der Aussage „$x = y$“.

(b) *Gleichmächtigkeit:* Für jede endliche Menge M ist

$$E \;:=\; \{\, (A,B) \,:\, A \subseteq M,\, B \subseteq M,\, |A| = |B| \,\}$$

eine Äquivalenzrelation auf der Menge $\mathcal{P}(M)$.

Skizze für $M = \{1, 2\}$:



Folie 219

(c) *Gleichmächtigkeit:* Die Relation

$$E := \left\{ (A, B) \,:\, \begin{array}{l} A \subseteq \mathbb{R},\ B \subseteq \mathbb{R},\ A \text{ und } B \text{ sind gleichmächtig} \\ \text{(d.h. es gibt eine bijektive Abbildung von } A \text{ nach } B) \end{array} \right\}$$

ist eine Äquivalenzrelation auf der Menge $\mathcal{P}(\mathbb{R})$.

(d) *Isomorphie:* Die Relation

$$E := \{\, (G, H) \,:\, G \text{ und } H \text{ sind ungerichtete Graphen mit } G \cong H \,\}$$

ist eine Äquivalenzrelation auf der Klasse aller ungerichteten Graphen.

Folie 220

Äquivalenzklassen

Bemerkung 3.68. Sei E eine Äquivalenzrelation auf einer Menge V. Für jedes $v \in V$ bezeichnet

$$[v]_E \;:=\; \{\, w \in V \,:\, (v, w) \in E \,\}$$

die *Äquivalenzklasse* von v bezüglich E. D.h.: Die Äquivalenzklasse $[v]_E$ besteht aus allen Elementen von V, die laut E „äquivalent“ zu v sind.
Eine Menge $W \subseteq V$ heißt *Äquivalenzklasse* (bzgl. E), falls es ein $v \in V$ mit $W = [v]_E$ gibt. Das Element v wird dann ein *Vertreter* seiner Äquivalenzklasse W genannt.

Folie 221

Man sieht leicht, dass für alle $v, w \in V$ gilt: Entweder $[v]_E = [w]_E$ oder $[v]_E \cap [w]_E = \emptyset$.
Falls V endlich und nicht leer ist, folgt daraus, dass es eine Zahl $k \in \mathbb{N}_{\geqslant 1}$ und Äquivalenzklassen $W_1, \ldots, W_k$ geben muss, so dass $V = W_1 \,\dot\cup\, \cdots \,\dot\cup\, W_k$ ist. Die Zahl k wird auch *Index* von E genannt. D.h.: Der Index einer Äquivalenzrelation gibt an, wie viele verschiedene Äquivalenzklassen es gibt.
Beispielsweise hat die Gleichmächtigkeits-Relation auf der Potenzmenge $\mathcal{P}(M)$ einer endlichen Menge M (Beispiel 3.67(b)) den Index $|M| + 1$.

Ordnungsrelationen

Folie 222

Definition 3.69 (Ordnungen)**.**
Sei E eine 2-stellige Relation über einer Menge V.

(a) E heißt *Präordnung*, falls E *reflexiv und transitiv* ist.

(b) E heißt *partielle Ordnung*, falls E *reflexiv, transitiv und antisymmetrisch* ist.

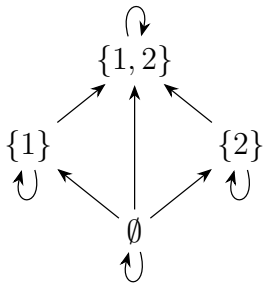
(c) E heißt *lineare Ordnung* (oder *totale Ordnung*), falls E *reflexiv, transitiv, antisymmetrisch und konnex* ist.

Beispiel 3.70.

(a) $\leqslant$ ist eine *lineare Ordnung* auf $\mathbb{N}$ (und $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$).
Ebenso ist $\geqslant$ eine lineare Ordnung auf $\mathbb{N}$ (und $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$).

(b) Für jede Menge M sind $\subseteq$ und $\supseteq$ *partielle Ordnungen* auf der Potenzmenge $\mathcal{P}(M)$ (aber keine linearen Ordnungen falls $|M| \geqslant 2$ ist).

Skizze für „$\subseteq$“ bei $M = \{1, 2\}$:

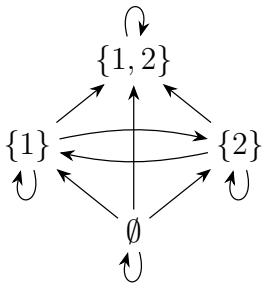


(c) Für jede Menge M ist

$$E := \left\{ (A,B) \;:\; \begin{array}{l} A, B \subseteq M, \;\; A \text{ ist höchstens so mächtig wie } B \\ \text{(d.h. es gibt eine injektive Abbildung von } A \text{ nach } B) \end{array} \right\}$$

eine *Präordnung* auf $\mathcal{P}(M)$ (aber keine partielle Ordnung falls $|M| \geqslant 2$).

Skizze für $M = \{1,2\}$:



Die reflexive und transitive Hülle einer Relation

Definition 3.71 (reflexive und transitive Hülle)**.**
Sei $G = (V, E)$ ein gerichteter Graph. Die *reflexive und transitive Hülle* (bzw. der *reflexive und transitive Abschluss*) von E auf V ist die rekursiv wie folgt definierte Relation $E^* \subseteq V \times V$:

Basisregeln:

- F.a. $v \in V$ ist $(v, v) \in E^*$.
- F.a. $(v, w) \in E$ ist $(v, w) \in E^*$.

Rekursive Regel:

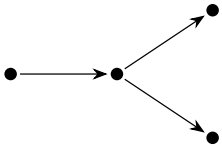
- Sind $(v, w) \in E^*$ und $(w, u) \in E^*$, so ist auch $(v, u) \in E^*$.

Das heißt: Der reflexive und transitive Abschluss von E auf V ist die kleinste Obermenge von E, die reflexiv und transitiv ist.

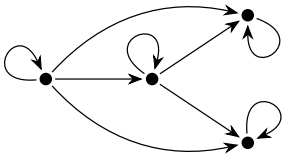
Folie 225

Beispiel.

$G = (V, E)$:=



$G^* = (V, E^*)$:



Folie 226

Beobachtung 3.72. *Sei $G = (V, E)$ ein gerichteter Graph und seien $v, w \in V$. Dann sind die beiden folgenden Aussagen äquivalent:*

(a) $(v, w) \in E^*$, wobei E^* die reflexive und transitive Hülle von E auf V ist.

(b) Es gibt in G einen Weg von v nach w.

Beweis. Übungsaufgabe. □

3.4 Der Satz von Cantor-Bernstein-Schröder

Folie 227

Dieser Abschnitt ist dem Beweis dessen gewidmet, was wir in Bemerkung 2.65 angekündigt hatten:

Satz 3.73 (Satz von Cantor-Bernstein-Schröder)**.**
Seien A und B beliebige Mengen. Wenn es eine injektive Abbildung $f : A \to B$ und eine injektive Abbildung $g : B \to A$ gibt, dann gibt es auch eine bijektive Abbildung $h : A \to B$.

Beweisidee: Wir betrachten hier den Fall, dass $A \cap B = \emptyset$ ist.
Es sei $G = (V, E)$ der ungerichtete Graph mit

$$\begin{aligned} V &:= A \dot\cup B \\ E &:= \{\, \{a, f(a)\} \,:\, a \in A \,\} \;\cup\; \{\, \{b, g(b)\} \,:\, b \in B \,\} \end{aligned}$$

Für jeden Knoten $v \in V$ gilt offensichtlicherweise: $\mathrm{Grad}_G(v) \in \{1, 2\}$ — d.h. v hat mindestens einen und höchsten zwei Nachbarn in G.
Außerdem ist G bipartit, da $A \cap B = \emptyset$ ist und jede Kanten einen Endpunkt in A und einen Endpunkt in B hat. Insbesondere gilt daher: Jeder Weg in G besucht immer abwechselnd Knoten aus A und Knoten aus B.

Jede Zusammenhangskomponente von G ist von genau einer der folgenden Formen:

(1) sie ist ein unendlicher Weg, der in einem Knoten $b \in B$ startet,

(2) sie ist ein unendlicher Weg, der in einem Knoten $a \in A$ startet,

(3) sie ist ein nach beiden Seiten unendlicher Weg,

(4) sie ist ein Kreis.

Wir wählen die Funktion $h : A \to B$ wie folgt:

- für jedes $a \in A$, das in einer Zusammenhangskomponente vom Typ (2), (3) oder (4) liegt, setzen wir $h(a) := f(a)$.

- für jedes $a \in A$, das in einer Zusammenhangskomponente vom Typ (1) liegt, setzen wir $h(a) := b'$, wobei b' derjenige Knoten ist, der in dem Weg, der die Zusammenhangskomponente bildet, direkt „links“ neben a liegt. Genauer: Die Zusammenhangskomponente ist von der Form

$$v_0 - w_0 - v_1 - w_1 - v_2 - w_2 - \cdots - v_i - w_i - v_{i+1} - w_{i+1} - \cdots$$

  wobei gilt:

  - f.a. $i \in \mathbb{N}$ ist $v_i \in B$ und $w_i \in A$,
  - $v_0 \in B \setminus \text{Bild}(f)$,
  - f.a. $i \in \mathbb{N}$ ist $g(v_i) = w_i$ und $f(w_i) = v_{i+1}$.

  Da a in dieser Zusammenhangskomponente liegt, gibt es ein $i \in \mathbb{N}$, so dass $a = w_i$ ist. Wir setzen $h(a) := v_i$ — d.h. $h(a)$ ist derjenige Knoten $b' \in B$, für den gilt: $g(b') = a$.

Man kann sich nun davon überzeugen, dass diese Funktion $h : A \to B$ bijektiv ist.

Formaler Beweis:

Schritt 1: Wir zeigen, dass die Aussage von Satz 3.73 für den Spezialfall gilt, dass $A \cap B = \emptyset$ ist.

Hierfür folgen wir der oben geschilderten Beweisidee. Gemäß Voraussetzung sind injektive Funktionen $f : A \to B$ und $g : B \to A$ gegeben.
Sei $B_0 := B \setminus \text{Bild}(f)$. Für jedes $b \in B_0$ setze $v_{b,0} := b$, und für alle $i \in \mathbb{N}$ setze $w_{b,i} := g(v_{b,i})$ und $v_{b,i+1} := f(w_{b,i})$. Per Induktion nach i erhält man: $v_{b,i} \in B$ und $w_{b,i} \in A$ f.a. $i \in \mathbb{N}$.

Behauptung 1: Für alle $b, b' \in B_0$ und alle $i, j \in \mathbb{N}$ mit $(b, i) \neq (b', j)$ gilt: $v_{b,i} \neq v_{b',j}$ und $w_{b,i} \neq w_{b',j}$.

Beweis: Seien $b, b' \in B_0$ beliebig. Wir führen einen Beweis durch Widerspruch. Angenommen, es gibt $i, j \in \mathbb{N}$ mit $(b, i) \neq (b', j)$, so dass $v_{b,i} = v_{b',j}$ oder $w_{b,i} = w_{b',j}$. Dann wählen wir solche i, j so, dass deren Summe $i+j$ so klein wie möglich ist.[6]

Fall 1: $v_{b,i} \neq v_{b',j}$.
Gemäß unserer Wahl von i, j muss dann $w_{b,i} = w_{b',j}$ sein.
Es gilt: $w_{b,i} = g(v_{b,i})$ und $w_{b',j} = g(v_{b',j})$. Also ist $g(v_{b,i}) = g(v_{b',j})$. Da g injektiv ist, gilt $v_{b,i} = v_{b',j}$. Dies widerspricht Fall 1. Somit kann Fall 1 nicht eintreten.

Fall 2: $v_{b,i} = v_{b',j}$.

Falls $i = j = 0$, so ist $v_{b,i} = b$ und $v_{b',j} = b'$; also $b = b'$. Dies steht im Widerspruch dazu, dass $(b, i) \neq (b', j)$ ist.

Falls $i > 0$ und $j > 0$, so ist $v_{b,i} = f(w_{b,i-1})$ und $v_{b',j} = f(w_{b',j-1})$. Also ist $f(w_{b,i-1}) = f(w_{b',j-1})$. Da f injektiv ist, gilt $w_{b,i-1} = w_{b',j-1}$. Aber da $(i-1) + (j-1) < i+j$ ist, widerspricht dies der Minimalität von $i+j$.

Falls $i > 0$ und $j = 0$ ist, so ist $v_{b,i} = f(w_{b,i-1})$ und $v_{b',j} = b'$. Somit erhalten wir den Widerspruch, dass $v_{b,i} \in \text{Bild}(f)$ und $v_{b,i} = b' \in B_0 = B \setminus \text{Bild}(f)$ ist.

Falls $i = 0$ und $j > 0$ ist, so erhalten wir denselben Widerspruch.

Insgesamt erhalten wir, dass Fall 2 nicht eintreten kann.

[6] Diese Beweismethode wird auch „*Prinzip des kleinsten Verbrechers*“ genannt: Man nimmt an, es gäbe ein Gegenbeispiel. Dann nimmt man ein Gegenbeispiel, das kleinstmöglich ist (gemäß eines geeignet gewählten Größenbegriffs). Und dann zeigt man, dass es doch ein noch kleineres Gegenbeipiel geben muss. Dies ist dann ein Widerspruch, aus dem man schließt, dass kein Gegenbeispiel existiert.

Beide Fälle führen zu einem Widerspruch. Dies beendet den Beweis von Behauptung 1. $\square_{Beh.1}$

Folie 231

Für jedes $b \in B_0$ sei $Z_b := \{v_{b,i} : i \in \mathbb{N}\} \cup \{w_{b,i} : i \in \mathbb{N}\}$.

Als direkte Folgerung aus Behauptung 1 erhalten wir:

Aussage A: Für alle $b, b' \in B_0$ mit $b \neq b'$ gilt: $Z_b \cap Z_{b'} = \emptyset$.

Aussage B: Für alle $b \in B_0$ und alle $i, j \in \mathbb{N}$ mit $i \neq j$ gilt: $v_{b,i} \neq v_{b,j}$ und $w_{b,i} \neq w_{b,j}$.

Wir setzen $S := \bigcup_{b \in B_0} Z_b$. Wir definieren nun die Funktion $h : A \to B$:

- Für jedes $a \in A$ mit $a \notin S$ sei $h(a) := f(a)$.
- Für jedes $a \in A$ mit $a \in S$ wählen wir $h(a)$ wie folgt: Gemäß Aussage A gibt es genau ein $b \in B_0$ s.d. $a \in Z_b$. Gemäß Aussage B gibt es genau ein $i \in \mathbb{N}$ s.d. $a = w_{b,i}$.

  Wir setzen $h(a) := v_{b,i}$. (Beachte, dass $g(v_{b,i}) = a$ ist.)

Folie 232

Behauptung 2: h ist surjektiv.

Beweis: Betrachte ein beliebiges $b \in B$. Wir müssen ein $a \in A$ finden, so dass $h(a) = b$ ist.

Fall 1: $b \in S$.
Gemäß Aussage A gibt es genau ein $b' \in B_0$ s.d. $b \in Z_{b'}$.
Gemäß Aussage B gibt es genau ein $i \in \mathbb{N}$ s.d. $b = v_{b',i}$.
Sei $a := w_{b',i}$. Dann ist $a \in A \cap S$, und gemäß unserer Definition der Funktion h ist $h(a) = v_{b',i} = b$.

Fall 2: $b \notin S$
Wegen $B_0 \subseteq S$ gilt insbesondere: $b \notin B_0 = B \setminus \text{Bild}(f)$. Somit ist $b \in \text{Bild}(f)$, d.h. es gibt ein $a \in A$ mit $f(a) = b$.
Falls $a \notin S$, so gilt gemäß unserer Definition der Funktion h, dass $h(a) = b$. Um den Beweis abzuschließen, müssen wir nur noch zeigen, dass tatsächlich $a \notin S$ gilt. Wir führen einen Beweis durch Widerspruch. Angenommen, $a \in S$. Dann gibt es ein $b' \in B_0$ und ein $i \in \mathbb{N}$, so dass $a = w_{b',i}$. Aber dann ist $b = f(a) = f(w_{b',i}) = v_{b',i+1} \in Z_{b'} \subseteq S$. D.h. $b \in S$. Dies steht im Widerspruch zu Fall 2. Insgesamt ist der Beweis von Behauptung 2 beendet. $\square_{Beh.2}$

Behauptung 3: h ist injektiv.

Beweis: Betrachte beliebige $a, a' \in A$ mit $h(a) = h(a')$. Wir müssen zeigen, dass $a = a'$ ist.

Fall 1: $a, a' \notin S$.
Gemäß unserer Definition der Funktion h ist dann $h(a) = f(a)$ und $h(a') = f(a')$. Aus $h(a) = h(a')$ folgt: $f(a) = f(a')$. Da f injektiv ist, ist $a = a'$.

Fall 2: $a, a' \in S$.
Dann gibt es $b, b' \in B_0$ und $i, j \in \mathbb{N}$ so dass $a = w_{b,i}$ und $a' = w_{b',j}$.
Gemäß unserer Definition der Funktion h ist $h(a) = v_{b,i}$ und $h(a') = v_{b',j}$.
Aus $h(a) = h(a')$ folgt: $v_{b,i} = v_{b',j}$. Behauptung 1 liefert, dass $(b, i) = (b', j)$ ist. Daraus folgt: $a = w_{b,i} = w_{b',j} = a'$.

Fall 3: $a \in S$ und $a' \notin S$.
Wegen $a \in S$ gibt es ein $b \in B_0$ und ein $i \in \mathbb{N}$ s.d. $a = w_{b,i}$.
Gemäß unserer Definition der Funktion h gilt: $h(a) = v_{b,i}$ und $h(a') = f(a')$.
Wegen $h(a) = h(a')$ gilt: $v_{b,i} = f(a')$. Insbesondere ist $v_{b,i} \in \text{Bild}(f)$. Daher ist $i \neq 0$, da $v_{b,0} = b \in B_0 = B \setminus \text{Bild}(f)$ ist.
Wegen $i \geqslant 1$ ist $v_{b,i} = f(w_{b,i-1})$.
Wir erhalten: $f(w_{b,i-1}) = v_{b,i} = f(a')$. Da f injektiv ist, ist $w_{b,i-1} = a'$.
Insbesondere ist also $a' \in Z_b \subseteq S$. Dies steht im Widerspruch zu Fall 3 (da $a' \notin S$ ist). Somit kann Fall 3 nicht eintreten.

Fall 4: $a' \in S$ und $a \notin S$.
Dieser Fall kann analog zu Fall 3 behandelt werden (durch Vertauschen der Rollen von a und a').

Insgesamt erhalten wir, dass die Fälle 3 und 4 nicht eintreten können; und in den Fällen 1 und 2 gilt $a = a'$. Dies beendet den Beweis von Behauptung 3. $\square_{Beh.3}$

Insgesamt erhalten wir, dass die Funktion $h : A \to B$ bijektiv ist. Dies beendet den Beweis für *Schritt 1*.

Schritt 2: Wir zeigen nun, dass die Aussage von Satz 3.73 auch für den Fall gilt, in dem $A \cap B \neq \emptyset$ ist.

Gemäß Voraussetzung gibt es injektive Funktionen $f : A \to B$ und $g : B \to A$.
Wir setzen $\hat{A} := A \times \{1\}$ und $\hat{B} := B \times \{2\}$. Dann ist $\hat{A} \cap \hat{B} = \emptyset$.
Wir definieren die Funktionen $\hat{f} : \hat{A} \to \hat{B}$ und $\hat{g} : \hat{B} \to \hat{A}$ wie folgt: Für jedes $a \in A$ und jedes $b \in B$ ist $\hat{f}(a, 1) := (f(a), 2)$ und $\hat{g}(b, 2) := (g(b), 1)$.
Da f und g injektiv sind, sind auch $\hat{f}$ und $\hat{g}$ injektiv.

Wegen $\hat{A} \cap \hat{B} = \emptyset$, gibt es gemäß der in *Schritt 1* bereits bewiesenen Aussage eine bijektive Funktion $\hat{h} : \hat{A} \to \hat{B}$.
Daraus generieren wir eine Funktion $h : A \to B$ wie folgt: Für jedes $a \in A$ betrachte $u_a := \hat{h}(a, 1)$. Klar: $u_a \in \hat{B} = B \times \{2\}$ — d.h.: es gibt ein $b \in B$ so dass $u_a = (b, 2)$. Wir setzen $h(a) := b$.
Da $\hat{h}$ bijektiv ist, kann man sich leicht davon überzeugen, dass auch h bijektiv ist. Dies beendet den Beweis von *Schritt 2*.

Insgesamt ist der formale Beweis von Satz 3.73 beendet. $\square_{\textit{Satz 3.73}}$

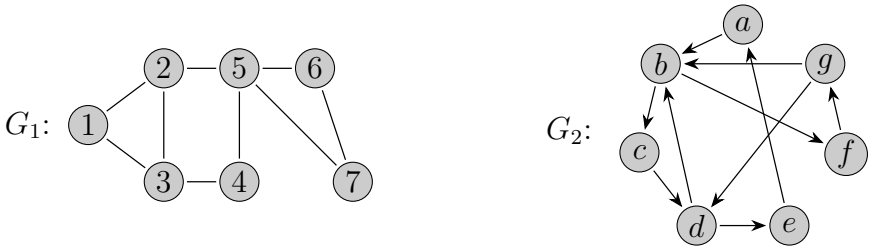
3.5 Literaturhinweise

Als vertiefende Lektüre sei Kapitel 1.2 in [Juk08], Kapitel 5 in [KB05], Kapitel 11 in [MM00], Teile der Kapitel 0–4 und 8 in [Die06], sowie Teile der Kapitel 7–10 und 13 in [LPV03] empfohlen. Eine umfassende Einführung in die Graphentheorie gibt das Lehrbuch [Die06].

Quellennachweis: Abschnitte 3.1–3.3 sind dem Vorlesungsskript [Sch13] entnommen; viele der in diesem Kapitel angegebenen Modellierungsbeispiele sind dem Buch [KB05] entnommen.

3.6 Übungsaufgaben

Aufgabe 3.1. Es seien die folgenden beiden Graphen G_1 und G_2 gegeben:



(a) Geben Sie für jeden der beiden Graphen G_1 und G_2 die Knotenmenge und die Kantenmenge an. Repräsentieren Sie außerdem jeden der beiden Graphen durch eine Adjazenzmatrix und eine Adjazenzliste.

(b) Geben Sie einen Weg von Knoten 2 nach Knoten 4 in G_1 an, der *nicht* einfach ist. Geben Sie außerdem einen Kreis in G_1 an, der *nicht* einfach ist und durch den Knoten 2 verläuft.

(c) Ist G_1 zusammenhängend? Ist G_2 stark zusammenhängend? Ist G_2 azyklisch?
Begründen Sie jeweils Ihre Antwort.

(d) Überprüfen Sie für jeden der folgenden Graphen $G \in \{G_3, G_4, G_5\}$, ob Folgendes gilt:

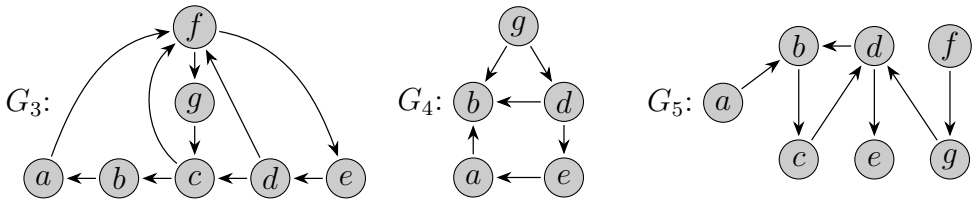
(i) $G = G_2$,

(ii) G ist ein Teilgraph von G_2,

(iii) G ist ein induzierter Teilgraph von G_2,

(iv) Es existiert ein Isomorphismus zwischen G und G_2.

Begründen Sie jeweils Ihre Antwort.

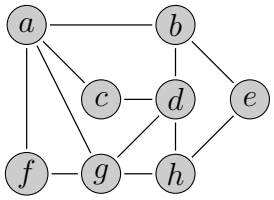


(e) Geben Sie die starken Zusammenhangskomponenten von G_5 an.

Aufgabe 3.2. Betrachten Sie den ungerichteten Graphen G auf der rechten Seite.

(a) Geben Sie die Knotenmenge V und die Kantenmenge E des Graphen G an. Repräsentieren Sie G außerdem durch eine Adjazenzmatrix und eine Adjazenzliste.

(b) Geben Sie einen Euler-Weg in G an.
Besitzt G auch einen Euler-Kreis? Beweisen Sie die Korrektheit Ihrer Antwort.



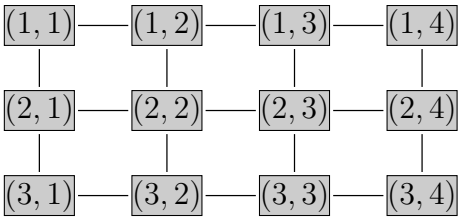
(c) Geben Sie einen Hamilton-Kreis in G an.

Aufgabe 3.3. Für $m, n \in \mathbb{N}_{\geqslant 1}$ sei das $(m \times n)$-*Gitter* der Graph

$G_{m\times n} = (V_{m\times n}, E_{m\times n})$ mit

$$\begin{aligned} V_{m\times n} &:= \big\{\, (i,j) \,:\, i,j \in \mathbb{N}, 1 \leqslant i \leqslant m,\, 1 \leqslant j \leqslant n \,\big\}, \\ E_{m\times n} &:= \big\{\, \{(i,j),(i,j+1)\} \,:\, i,j \in \mathbb{N}, 1 \leqslant i \leqslant m,\, 1 \leqslant j < n \,\big\} \cup \\ &\qquad \big\{\, \{(i,j),(i+1,j)\} \,:\, i,j \in \mathbb{N}, 1 \leqslant i < m,\, 1 \leqslant j \leqslant n \,\big\}. \end{aligned}$$

Das (3×4)-Gitter $G_{3\times 4}$ sieht z.B. wie folgt aus:



(a) Überprüfen Sie, ob $G_{3\times 4}$ bipartit ist. Falls $G_{3\times 4}$ bipartit ist, so geben Sie zwei disjunkte Knotenmengen $V_1, V_2 \subseteq V_{3\times 4}$ mit $V_1 \cup V_2 = V_{3\times 4}$ an, so dass jede Kante aus $E_{3\times 4}$ einen Knoten aus V_1 und einen Knoten aus V_2 miteinander verbindet. Falls $G_{3\times 4}$ nicht bipartit ist, so begründen Sie dies.

(b) Geben Sie ein Matching maximaler Größe in $G_{3\times 4}$ an.

(c) Geben Sie einen Hamilton-Kreis in $G_{3\times 4}$ an.

(d) Für welche $m, n \in \mathbb{N}$ mit $n, m \geqslant 3$ besitzt $G_{m\times n}$ einen Hamilton-Kreis, für welche nicht? Begründen Sie Ihre Antwort. Ein vollständiger Beweis ist nicht notwendig.

Hinweis: Stellen Sie sich vor, dass die Knoten des Gitters so mit den Farben rot oder blau eingefärbt sind, dass benachbarte Knoten unterschiedliche Farben besitzen. Jeder Weg durch das Gitter besucht daher immer abwechselnd einen blauen und einen roten Knoten.

(e) Was passiert, wenn n, m auch die Werte 1 oder 2 annehmen können?

Aufgabe 3.4.* Sei $n \in \mathbb{N}$ mit $n \geqslant 2$ und $G_{n\times n}$ das $(n \times n)$-Gitter. Betrachten Sie die Menge P aller Wege in $G_{n\times n}$, die in $(1,1)$ beginnen und in (n,n) enden, keinen Knoten unterhalb der Diagonalen besuchen und die in jedem „Schritt“ ausschließlich nach rechts oder nach unten wandern. Das heißt, P ist die Menge aller Wege $(v_1, \ldots, v_\ell)$ mit $v_1 = (1,1)$, $v_\ell = (n,n)$ und für alle $i \in \{1, \ldots, \ell - 1\}$ gilt mit $v_i = (x,y)$, dass $x \leqslant y$ und entweder $v_{i+1} = (x{+}1, y)$ oder $v_{i+1} = (x, y{+}1)$.
Berechnen Sie $|P|$ und beweisen Sie, dass Ihre Antwort korrekt ist.

Aufgabe 3.5. Auf dem Weihnachtsmarkt von Großdorf sollen insgesamt 8 Stände rund um den Marktplatz arrangiert werden. Die 8 Stände setzen sich folgendermaßen zusammen:

- Ein Stand, in dem die traditionelle Weihnachtskrippe aufgebaut ist;
- Zwei Stände, an denen Kunsthandwerk verkauft wird: Einer der beiden Stände ist die Töpferei, der andere bietet Holzschmuck aus dem Erzgebirge an;
- Zwei Glühweinstände, einer davon wird von Herrn Max, der andere von Frau Peters betrieben;
- Drei Essensstände, einer davon verkauft Crêpes, der andere Waffeln und der dritte Steaks vom Holzkohlegrill.

Bei der Platzierung der 8 Stände um den Marktplatz ist Folgendes zu beachten: Neben die Weihnachtskrippe darf keiner der Glühweinstände platziert werden. Essensstände dürfen nicht nebeneinander stehen, die beiden Glühweinstände dürfen ebenfalls nicht nebeneinander platziert werden, und selbiges gilt auch für die beiden Kunsthandwerkstände. Aus Sicherheitsgründen darf der Holzkohlegrill weder neben die Weihnachtskrippe noch neben den Stand mit dem Holzschmuck aus dem Erzgebirge gestellt werden. Herr Max ist mit den Besitzern des Holzkohlegrills und der Töpferei befreundet und möchte daher unbedingt die beiden als Nachbarn haben. Außerdem ist zu beachten, dass sich der Betreiber des Waffelstands weder mit Frau Peters noch mit dem Besitzer der Töpferei verträgt und daher auf keinen Fall neben einem der beiden platziert werden will.

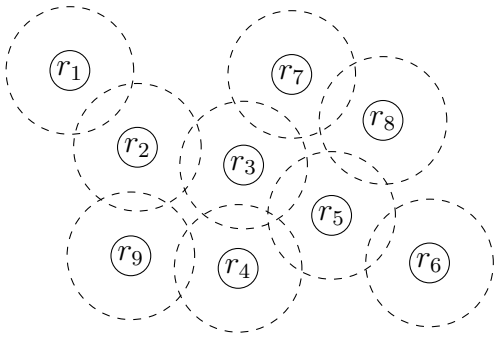
(a) Stellen Sie den Konfliktgraph und das Komplement des Konfliktgraphen auf.

(b) Gibt es im Komplement des Konfliktgraphen einen Hamiltonkreis? Falls ja, dann geben Sie einen solchen Hamiltonkreis an. Falls nein, dann begründen Sie, warum es keinen gibt.

(c) Geben Sie, falls möglich, eine Platzierung der 8 Stände rund um den Marktplatz an, mit der alle zufrieden sind.

Aufgabe 3.6. Es seien die Radiostationen $r_1, \ldots, r_9$ gegeben, denen jeweils eine Sendefrequenz zugeordnet werden soll. Radiostationen, die zu dicht beieinander liegen, dürfen allerdings nicht die gleiche Frequenz erhalten.

Das nebenstehende Diagramm stellt die Lage der einzelnen Radiostationen dar. Um jede Station ist ein gestrichelter Kreis eingezeichnet, der die Reichweite einer Radiostation repräsentiert. Schneiden sich die Kreise von zwei Radiostationen r_i und r_j, so liegen r_i und r_j zu dicht beieinander und dürfen nicht die gleiche Frequenz zugeordnet bekommen.



(a) Geben Sie den Konfliktgraphen an, der als Knotenmenge die Radiostationen besitzt und bei dem eine Kante zwischen zwei Radiostationen r_i und r_j anzeigt, dass r_i und r_j nicht die gleiche Frequenz benutzen dürfen.

(b) Sei $G = (V, E)$ der Konfliktgraph aus Aufgabenteil (a). Geben Sie eine konfliktfreie Knotenmarkierung $m : V \to \mathbb{N}$ für G an, die möglichst wenige verschiedene Markierungen benutzt, das heißt, $|\text{Bild}(m)|$ soll minimal sein.

(c) Wie viele verschiedene Frequenzen werden für die Radiostationen $r_1, \ldots, r_9$ mindestens benötigt? Das heißt, wie groß ist die chromatische Zahl des Konfliktgraphen?

Begründen Sie jeweils Ihre Antwort.

Aufgabe 3.7. Ein ungerichteter endlicher Graph $G = (V, E)$ wird *kubisch* genannt, wenn für alle seine Knoten $v \in V$ gilt: $\text{Grad}_G(v) = 3$.

(a) Geben Sie jeweils einen zusammenhängenden kubischen Graphen mit 4, 6 und 8 Knoten in graphischer Darstellung an.

(b) Beweisen Sie, dass für jede gerade natürliche Zahl $n \geqslant 4$ ein zusammenhängender kubischer Graph mit n Knoten existiert.

Aufgabe 3.8.

(a) Beweisen Sie die Rückrichtung von Satz 3.46.

(b) Beweisen Sie Satz 3.56(b).

Aufgabe 3.9.

(a) Betrachten Sie die Relation $R := \{(a,a),(a,b),(a,c),(b,b),(b,c)\}$ über der Menge $A := \{a,b,c,d\}$. Welche Paare $(x,y) \in A \times A$ müssen zu R mindestens hinzugefügt werden, um aus R eine Relation zu erhalten, die jeweils:

(i) reflexiv ist?

(ii) symmetrisch ist?

(iii) antisymmetrisch ist?

(b) Betrachten Sie die folgenden Relationen R_i über der jeweiligen Menge M_i für $i \in \{1,2\}$.

(i) $M_1 := \{1,2,3,4,5\}$,
$R_1 := \{(1,1),(1,2),(2,2),(2,3),(3,3),(4,4),(4,5),(5,4),(5,5)\}$.

(ii) $M_2 := \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\}$,
$R_2 := \{(\clubsuit,\spadesuit),(\clubsuit,\heartsuit),(\clubsuit,\diamondsuit),(\spadesuit,\heartsuit),(\spadesuit,\diamondsuit),(\heartsuit,\diamondsuit)\}$.

Stellen Sie R_1 und R_2 durch einen gerichteten Graphen dar. Geben Sie für jedes $i \in \{1,2\}$ und für jede der Eigenschaften „reflexiv“, „symmetrisch“, „antisymmetrisch“, „konnex“, „transitiv“ an, ob die Relation R_i diese Eigenschaft besitzt oder nicht.

(c) Für einen gerichteten Baum $B = (V,E)$ definieren wir die Relation

$$R_B := \{(x,y) \in V \times V \,:\, \text{es gibt einen Weg von } x \text{ nach } y \text{ in } B\}$$

(i) Beweisen Sie, dass R_B für jeden gerichteten Baum B eine partielle Ordnung ist.

(ii) Geben Sie gerichtete Bäume B_1 und B_2 mit jeweils mindestens 3 Knoten an, sodass

(1) R_{B_1} eine lineare Ordnung ist

(2) R_{B_2} keine lineare Ordnung ist.

Begründen Sie Ihre Antwort.

Aufgabe 3.10.

(a) Betrachten Sie die folgenden Relationen R_i über der jeweiligen Menge M_i für $i \in \{1, 2\}$.

(i) $M_1 := \{-4, -3, -2, -1, 0, 1, 2\}$,
$R_1 := \{(x, y) \in M_1 \times M_1 \,:\, x \cdot y \leqslant 3\}$.

(ii) $M_2 := \mathbb{N}_{\geqslant 1}$, $R_2 := \{(a, b) \in M_2 \times M_2 \,:\, \text{ggT}(a, b) > 1\}$, wobei $\text{ggT}(a, b)$ der größte gemeinsame Teiler der Zahlen a und b ist.

Geben Sie für jedes $i \in \{1, 2\}$ und jede der Eigenschaften „reflexiv“, „symmetrisch“, „antisymmetrisch“, „konnex“, „transitiv“ an, ob die Relation R_i diese Eigenschaft besitzt oder nicht.

(b) Sei A eine beliebige nicht-leere Menge. Für Worte über dem Alphabet A definieren wir die Relation

$$\text{Prä}_A := \{(a, b) \in A^* \times A^* \,:\, \text{ex. } c \in A^*, \text{ s.d. } ac = b\}.$$

Falls $(a, b) \in \text{Prä}_A$, so heißt a *Präfix* von b.

(i) Beweisen Sie, dass für jedes Alphabet A gilt: Prä_A ist eine partielle Ordnung auf A^*.

(ii) Geben Sie zwei konkrete Alphabete A_1 und A_2 an, sodass gilt:

(1) Prä_{A_1} ist eine lineare Ordnung.

(2) Prä_{A_2} ist keine lineare Ordnung.

Aufgabe 3.11. Beweisen Sie Beobachtung 3.72.

Kapitel 4

Kombinatorik

Folie 233

Kombinatorik ist ein Teilgebiet der Mathematik, bei dem die Anordnungsmöglichkeiten einer endlichen Menge vorgegebener Objekte studiert werden. Oft geht es darum, zu zählen, wie viele verschiedene Anordnungsmöglichkeiten oder wie viele verschiedene Objekte mit bestimmten Eigenschaften es gibt. Resultate und Methoden der Kombinatorik werden im Fach Informatik oft beim Entwurf und der Analyse von effizienten Algorithmen verwendet.

4.1 Kombinatorische Abzählregeln

Folie 234

Zunächst fassen wir einige grundlegende Abzähl-Regeln zusammen:

Regel 4.1.

(a) *Gleichheitsregel*:

Für endliche Mengen A, B gilt:
$|A| = |B| \iff$ es gibt eine bijektive Abbildung von A nach B.

(b) *Summenregel*:

Sei $k \in \mathbb{N}_{\geqslant 1}$ und seien $A_1, \ldots, A_k$ paarweise disjunkte endliche Mengen.
Dann gilt: $\left|\bigcup_{i=1}^{k} A_i\right| = \sum_{i=1}^{k} |A_i|$.

(c) *Zerlegungsregel*:

Seien A, B endliche Mengen und sei f eine Abbildung von A nach B.
Für jedes $b \in B$ sei[1] $f^{-1}(b) := \{a \in A : f(a) = b\}$. Es gilt:

[1] Die Menge $f^{-1}(b)$ wird das *Urbild von b unter f* genannt.

$|A| = \sum_{b \in B} |f^{-1}(b)|$.

(d) *Produktregel*:

Sei $k \in \mathbb{N}_{\geqslant 1}$ und seien $A_1, \ldots, A_k$ endliche Mengen. Dann gilt:
$|A_1 \times \cdots \times A_k| = \prod_{i=1}^{k} |A_i|$.

Beweis. (a) gilt gemäß Beobachtung 2.37(b).
(b) ist für $k = 1$ und $k = 2$ offensichtlich. Dies können wir als Induktionsanfang nutzen und erhalten dann ganz leicht auch den Induktionsschritt „$k \to k{+}1$“.
(c) folgt aus (b), denn: Sei $k := |B|$ und seien $b_1, \ldots, b_k$ so dass $B = \{b_1, \ldots, b_k\}$. Für jedes $i \in [k]$ sei $A_i := f^{-1}(b_i)$. Da f eine Abbildung ist, sieht man leicht, dass die Mengen $A_1, \ldots, A_k$ paarweise disjunkt sind und dass gilt: $A = \bigcup_{i=1}^{k} A_i$. Unter Verwendung von (b) erhalten wir:
$|A| = \left|\bigcup_{i=1}^{k} A_i\right| = \sum_{i=1}^{k} |A_i| = \sum_{i=1}^{k} |f^{-1}(b_i)|$.
(d) gilt gemäß Satz 2.21(b). □

4.2 Ziehen von Elementen aus einer Menge

Folie 235

Wie viele Möglichkeiten gibt es, k Objekte aus einer n-elementigen Menge zu ziehen?
Die Antwort auf diese Frage hängt davon ab, wie denn genau gezogen wird. Wir unterscheiden zwischen

Ziehen mit Zurücklegen: nachdem ein Element gezogen wurde, wird es in den „Lostopf“ zurückgelegt, so dass es bei späteren Zügen nochmals gezogen werden kann

Ziehen ohne Zurücklegen: nachdem ein Element gezogen wurde, ist es im „Lostopf“ nicht mehr verfügbar und kann in späteren Zügen daher nicht nochmals gezogen werden.

Und bei jeder dieser beiden Arten des Ziehens unterscheiden wir zwischen den beiden folgenden Varianten:

mit Berücksichtigung der Reihenfolge: beim Ergebnis wird die Reihenfolge berücksichtigt, in der die einzelnen Elemente gezogen wurden

ohne Berücksichtigung der Reihenfolge: beim Ergebnis kommt es nur darauf an, welche Elemente insgesamt gezogen wurden — aber die genaue Reihenfolge, in der diese Elemente gezogen wurden, ist egal.

Folie 236

Beispiele 4.2.

(a) Beim Ziehen der Lottozahlen handelt es sich um Ziehen ohne Zurücklegen und ohne Berücksichtigung der Reihenfolge.

(b) Wenn der Lostopf aus den Elementen $1, 2, 3$ besteht und wir $k := 2$ Elemente ziehen, dann sind folgende Ergebnisse möglich:

	mit Berücksichtigung der Reihenfolge	ohne Berücksichtigung der Reihenfolge
mit Zurücklegen	$(1,1)$, $(1,2)$, $(1,3)$, $(2,1)$, $(2,2)$, $(2,3)$, $(3,1)$, $(3,2)$, $(3,3)$	zwei mal die 1; die 1 und die 2; die 1 und die 3; zwei mal die 2; die 2 und die 3; zwei mal die 3
ohne Zurücklegen	$(1,2)$, $(1,3)$, $(2,1)$, $(2,3)$, $(3,1)$, $(3,2)$	$\{1,2\}$, $\{1,3\}$, $\{2,3\}$

Jede der 4 Varianten schauen wir uns im Folgenden etwas genauer an.

Ziehen mit Zurücklegen und mit Berücksichtigung der Reihenfolge

Folie 237

Wie viele Möglichkeiten gibt es, k Elemente aus einer n-elementigen Menge zu ziehen, wobei die Reihenfolge der Züge berücksichtigt wird und nach jedem Zug das gezogene Element wieder in den „Lostopf“ zurückgelegt wird?

Antwort:
Im ersten Zug gibt es n Möglichkeiten, da jedes der n Elemente, die sich im Lostopf befinden, gezogen werden können.
In jedem weiteren Zug gibt es wieder n Möglichkeiten, da sich ja bei jedem Zug weiterhin n Elemente im Lostopf befinden.

Die Menge der möglichen Endergebnisse ist genau die Menge aller k-Tupel, die über den n sich im Lostopf befindlichen Elemente gebildet werden können. Es gibt also beim *Ziehen mit Zurücklegen und mit Berücksichtigung der Reihenfolge* insgesamt

$$\underbrace{n \cdot n \cdots n}_{k \text{ mal}} \quad = \quad n^k$$

Möglichkeiten, k Elemente aus einer n-elementigen Menge zu ziehen.

Ziehen ohne Zurücklegen und mit Berücksichtigung der Reihenfolge

Folie 238

Wie viele Möglichkeiten gibt es, k Elemente aus einer n-elementigen Menge zu ziehen, wobei die Reihenfolge der Züge berücksichtigt wird, und nach jedem Zug das gezogene Element dauerhaft aus dem „Lostopf“ entfernt ist?

Antwort:
Im ersten Zug gibt es n Möglichkeiten, da jedes der n Elemente, die sich im Lostopf befinden, gezogen werden können.
Danach sind nur noch $n-1$ Elemente im Lostopf. Im zweiten Zug gibt es also nur noch $n-1$ Möglichkeiten, da nun jedes der $n-1$ Elemente des Lostopfs gezogen werden könnte.
Für jedes $i \in \{0, 1, \ldots, k-1\}$ gilt: Vor dem $(i+1)$-ten Zug befinden sich genau $n-i$ Elemente im Lostopf; und im $(i+1)$-ten Zug kann jedes dieser $n-i$ Elemente gezogen werden.
Es gibt also beim *Ziehen ohne Zurücklegen und mit Berücksichtigung der Reihenfolge* insgesamt

$$(n)_k \quad := \quad n \cdot (n-1) \cdots (n-k+1) \quad = \quad \frac{n!}{(n-k)!} \tag{4.1}$$

Möglichkeiten, k Elemente aus einer n-elementigen Menge zu ziehen.

Folie 239

Wenn der Lostopf zu Beginn aus den Elementen der Menge $M := \{1, \ldots, n\}$ besteht, gilt: Die Menge der möglichen Endergebnisse beim *Ziehen ohne Zurücklegen und mit Berücksichtigung der Reihenfolge* ist genau die Menge

$$\big\{ (a_1, \ldots, a_k) \in M^k \,:\, a_1, \ldots, a_k \text{ sind paarweise verschieden} \big\} .$$

Wir haben eben gerade ausgerechnet, dass Folgendes gilt:

$$\big|\big\{ (a_1, \ldots, a_k) \in [n]^k \,:\, a_1, \ldots, a_k \text{ paarw. versch.} \big\}\big| \;=\; (n)_k \tag{4.2}$$

Ziehen ohne Zurücklegen und ohne Berücksichtigung der Reihenfolge

Folie 240

Wie viele Möglichkeiten gibt es, k Elemente aus einer n-elementigen Menge zu ziehen, und zwar „ohne zurückzulegen und ohne Berücksichtigung der Reihenfolge“?

Antwort:
Dies entspricht gerade dem Szenario, in dem wir nur einmal in den Lostopf greifen und dabei auf einen Schlag k Elemente herausholen und uns als Ergebnis die Menge dieser k paarweise verschiedenen Elemente anschauen. Die Menge der möglichen Endergebnisse beim *Ziehen ohne Zurücklegen und ohne Berücksichtigung der Reihenfolge* von k Elementen aus einer n-elementigen Menge M ist also genau die Menge

$$\mathcal{P}_k(M) \quad := \quad \{X \subseteq M \,:\, |X| = k\}\,, \tag{4.3}$$

d.h. die *Menge aller k-elementigen Teilmengen von M*.

Folie 241

Binomialkoeffizienten

Definition 4.3. Für alle $n, k \in \mathbb{N}$ definieren wir:[2]

$$\binom{n}{k} \quad := \quad |\,\mathcal{P}_k([n])\,|\,. \tag{4.4}$$

$\binom{n}{k}$ (in Worten: „n über k“) wird *Binomialkoeffizient (zu n und k)* genannt; er ist definiert als die Anzahl der verschiedenen k-elementigen Teilmengen, die eine n-elementige Menge besitzt.

Beobachtung 4.4. *Für alle $n \in \mathbb{N}$ gilt:*

(a) $\binom{n}{0} = 1 = \binom{n}{n}$

denn: $[n]$ besitzt genau eine 0-elementige Teilmenge (nämlich $\emptyset$) und genau eine 1-elementige Teilmenge (nämlich $[n]$).

(b) Für alle $k \in \mathbb{N}$ mit $k > n$ gilt: $\binom{n}{k} = 0$

denn: Wegen $k > n$ gibt es keine einzige k-elementige Teilmenge von $[n]$. Also ist $\mathcal{P}_k([n]) = \emptyset$.

[2] Zur Erinnerung: $[n] = \{i \in \mathbb{N} \,:\, 1 \leqslant i \leqslant n\}$.

(c) $2^n = \sum_{k=0}^{n} \binom{n}{k}$

denn: $\mathcal{P}([n]) = \bigcup_{k=0}^{n} \mathcal{P}_k([n])$, und f.a. $k, k' \in \mathbb{N}$ mit $k, k' \leqslant n$ und $k \neq k'$ gilt: $\mathcal{P}_k([n]) \cap \mathcal{P}_{k'}([n]) = \emptyset$. Aus der Summenregel (Regel 4.1(b)) und Folgerung 2.39 folgt also:

$$2^n \quad = \quad |\mathcal{P}([n])| \quad = \quad \sum_{k=0}^{n} |\mathcal{P}_k([n])| \quad = \quad \sum_{k=0}^{n} \binom{n}{k} .$$

Folie 242

Pascal'scher Rekurrenzsatz

Satz 4.5. *Für alle $k, n \in \mathbb{N}$ mit $1 \leqslant k \leqslant n$ gilt:*

$$\binom{n+1}{k} \quad = \quad \binom{n}{k-1} + \binom{n}{k} .$$

Beweis. Sei $M := [n+1]$. Wir zerlegen die Menge $\mathcal{P}_k(M)$ aller k-elementigen Teilmengen von M wie folgt:

- A sei die Menge aller k-elementigen Teilmengen von M, die die Zahl $n+1$ enthalten.
- B sei die Menge aller k-elementigen Teilmengen von M, die die Zahl $n+1$ nicht enthalten.

  Offensichtlicherweise ist $B = \mathcal{P}_k([n])$. Also ist $|B| = \binom{n}{k}$.

Es gilt: A und B sind disjunkt, und $\mathcal{P}_k(M) = A \cup B$. Somit gilt gemäß der Summenregel (Regel 4.1(b)):

$$\binom{n+1}{k} \quad = \quad |\mathcal{P}_k(M)| \quad = \quad |A| + |B| \quad = \quad |A| + \binom{n}{k} .$$

Wir müssen nur noch zeigen, dass $|A| = \binom{n}{k-1}$ ist.
Dazu betrachten wir die Abbildung $f : \mathcal{P}_{k-1}([n]) \to A$ mit $f(X) := X \cup \{n+1\}$ f.a. $X \in \mathcal{P}_{k-1}([n])$. Man sieht leicht, dass f bijektiv ist. Aus der Gleichheitsregel (Regel 4.1(a)) folgt daher:

$$|A| \quad = \quad |\mathcal{P}_{k-1}([n])| \quad = \quad \binom{n}{k-1} .$$

□

Pascal'sches Dreieck

Aus dem Pascal'schen Rekurrenzsatz ergibt sich ein sehr effizienter Algorithmus, mit dem man bei Eingabe von n und k den Wert $\binom{n}{k}$ berechnen kann:
Wir bilden eine Tabelle, deren Zeilen wir mit den Zahlen $0, 1, \ldots n$ durchnummerieren; in Zeile i benutzen wir die Spalten $0, 1, \ldots, i$.
Ziel ist, in Zeile i und Spalte j den Wert $\binom{i}{j}$ einzutragen. Wir wissen, dass $\binom{i}{0} = \binom{i}{i} = 1$ für alle $i \in \mathbb{N}$ gilt. Somit können wir diese Einträge direkt in die Tabelle einfügen. Für die restlichen Einträge gehen wir die Zeilen in aufsteigender Reihenfolge durch. Den Eintrag $\binom{i+1}{j}$ in Zeile $i{+}1$ und Spalte j, für $1 \leqslant j \leqslant i$ erhalten wir gemäß dem Pascal'schen Rekurrenzsatz einfach als die Summe $\binom{i}{j-1} + \binom{i}{j}$ der Einträge in den Spalten $j{-}1$ und j der Zeile i. Daraus ergibt sich die folgende Tabelle (die fettgedruckten Einsen sind diejenigen Einträge, mit denen wir starten; danach gehen wir die einzelnen Zeilen nacheinander durch):

	0	1	2	3	4	5	6	7
0	**1**							
1	**1**	**1**						
2	**1**	2	**1**					
3	**1**	3	3	**1**				
4	**1**	4	6	4	**1**			
5	**1**	5	10	10	5	**1**		
6	**1**	6	15	20	15	6	**1**	
7	**1**	7	21	35	35	21	7	**1**

Die hier genutzte algorithmische Technik des Ausfüllens einer Tabelle, bei der man zum Berechnen des Eintrags in Zeile i und Spalte j auf Dinge zurückgreift, die man bereits vorher in die Tabelle eingetragen hat (hier: die Einträge in Zeile $i{-}1$ und den Spalten j und $j{-}1$), wird *dynamische Programmierung* genannt.

Binomische Formel

Satz 4.6. *Für alle $a, b \in \mathbb{R}$ und alle $n \in \mathbb{N}$ gilt:*

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

Beweis. Es gilt:

$$(a+b)^n \quad = \quad \underbrace{(a+b)\cdot \ \cdots \ \cdot (a+b)}_{n \text{ mal}} \ . \tag{4.5}$$

Wir multiplizieren dieses n-fache Produkt aus und gruppieren die einzelnen Summanden nach dem Term $a^k \cdot b^{n-k}$, für jedes $k \in \{0, \ldots, n\}$. Jedes einzelne $X \subseteq [n]$ repräsentiert wie folgt einen Summanden, den wir beim Ausmultiplizieren von (4.5) erhalten: für jede Position $i \in [n]$ wählen wir im i-ten Exemplar des Faktors $(a+b)$ beim Ausmultiplizieren von (4.5) den Wert a, falls $i \in X$, bzw. den Wert b, falls $i \notin X$ ist. Somit gilt:

$$\begin{aligned}
(a+b)^n &= \sum_{X \subseteq [n]} a^{|X|} \cdot b^{n-|X|} \\
&= \sum_{k=0}^{n} |\{X \subseteq [n] \ : \ |X| = k\}| \cdot a^k \cdot b^{n-k} \\
&= \sum_{k=0}^{n} |\mathcal{P}_k([n])| \cdot a^k \cdot b^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} \cdot a^k \cdot b^{n-k} \ .
\end{aligned}$$

□

Folie 245

Eine Formel zum Ausrechnen des Binomialkoeffizienten

Satz 4.7. *Für alle $k, n \in \mathbb{N}$ mit $k \leqslant n$ gilt:*

$$\binom{n}{k} \quad = \quad \frac{(n)_k}{k!} \quad = \quad \frac{n!}{k! \cdot (n-k)!}$$

Beweis. Sei $A := \{(a_1, \ldots, a_k) \in [n]^k \ : \ a_1, \ldots, a_k \text{ paarweise verschieden}\}$. Aus Gleichungen (4.1) und (4.2) wissen wir, dass Folgendes gilt:

$$|A| \quad = \quad (n)_k \quad = \quad \tfrac{n!}{(n-k)!}$$

Sei B die Menge aller *bijektiven* Abbildungen $f : [k] \to [k]$. Man kann sich leicht davon überzeugen (Details: Übungsaufgabe), dass $|B| = k!$ ist.

Betrachte ein beliebiges $X \in \mathcal{P}_k([n])$ und liste die Elemente $x_1, \ldots, x_k$ von X in aufsteigender Reihenfolge auf; für jedes $f \in B$ betrachte das Tupel $t_{X,f} := (x_{f(1)}, \ldots, x_{f(k)})$.
Sei die Abbildung $h : \mathcal{P}_k([n]) \times B \to A$ definiert durch $h(X, f) := t_{X,f}$ für alle $X \in \mathcal{P}_k([n])$ und alle $f \in B$. Man kann sich leicht davon überzeugen (Details: Übungsaufgabe), dass h *bijektiv* ist.
Aus der Gleichheitsregel (Regel 4.1(a)) folgt daher: $|\mathcal{P}_k([n]) \times B| = |A|$.
Unter Verwendung der Produktregel (Regel 4.1(d)) folgt:

$$(n)_k \quad = \quad |A| \quad = \quad |\mathcal{P}_k([n])| \cdot |B| \quad = \quad \binom{n}{k} \cdot k!$$

Insgesamt erhalten wir: $\binom{n}{k} = \frac{(n)_k}{k!} = \frac{n!}{k! \cdot (n-k)!}$. □

Folie 246

Weitere Eigenschaften der Binomialkoeffizienten

Satz 4.8. *Für alle $k, n \in \mathbb{N}$ mit $k \leqslant n$ gilt:*

(a) $\binom{n}{k} = \binom{n}{n-k}$

(b) Falls $k \neq 0$, so $\binom{n}{k} \geqslant \left(\frac{n}{k}\right)^k$.

(c) Falls $k \neq 0$, so $\binom{n}{k} < \left(\frac{en}{k}\right)^k$ *wobei e die Eulersche Zahl ist.*[3]

Beweis. (a) folgt direkt aus Satz 4.7.

Zu (b): Gemäß Satz 4.7 gilt:

$$\binom{n}{k} \quad = \quad \frac{(n)_k}{k!} \quad = \quad \frac{n}{k} \cdot \frac{n-1}{k-1} \cdot \frac{n-2}{k-2} \cdots \frac{n-(k-1)}{1} \tag{4.6}$$

Außerdem gilt für alle $i \in \{1, \ldots, k-1\}$

$$\frac{n-i}{k-i} \quad \geqslant \quad \frac{n}{k}\,, \tag{4.7}$$

denn: $k \leqslant n$, also $ki \leqslant ni$, also $nk - ki \geqslant nk - ni$, also $k(n-i) \geqslant n(k-i)$, also $\frac{n-i}{k-i} \geqslant \frac{n}{k}$.

[3] $e = 2{,}71828\cdots$

Aus (4.6) und (4.7) folgt:

$$\binom{n}{k} \geqslant \underbrace{\frac{n}{k} \cdot \frac{n}{k} \cdot \frac{n}{k} \cdots \frac{n}{k}}_{k \text{ mal}} = \left(\frac{n}{k}\right)^k$$

Zu (c): Wir nutzen den folgenden Sachverhalt, den wir hier nicht beweisen (der aber durch Aufmalen der Funktionsgraphen der Exponentialfunktion $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = e^x$ und der Funktion $g : \mathbb{R} \to \mathbb{R}$ mit $g(x) = 1 + x$ leicht eingesehen werden kann):

$$\text{Für jede Zahl } x \in \mathbb{R} \text{ mit } x \neq 0 \text{ gilt: } 1 + x < e^x. \tag{4.8}$$

Wenn $1+x \geqslant 0$ ist, folgt aus (4.8) auch für alle $n \in \mathbb{N}_{\geqslant 1}$, dass $(1 + x)^n < (e^x)^n = e^{x \cdot n}$. Wir wählen $x := \frac{k}{n}$ und erhalten:

$$e^k = e^{x \cdot n} > (1 + x)^n$$

Die binomische Formel liefert:

$$(1 + x)^n = \sum_{j=0}^{n} \binom{n}{j} \cdot x^j \geqslant \binom{n}{k} \cdot x^k$$

Insgesamt erhalten wir also:

$$e^k > \binom{n}{k} \cdot \left(\frac{k}{n}\right)^k$$

Also ist

$$\binom{n}{k} < \left(\frac{en}{k}\right)^k.$$

□

Ziehen mit Zurücklegen und ohne Berücksichtigung der Reihenfolge

Folie 247

Wie viele Möglichkeiten gibt es, k Elemente aus einer n-elementigen Menge zu ziehen, wobei nach jedem Zug das gezogene Element wieder in den „Lostopf“ zurückgelegt wird, aber beim Endergebnis die Reihenfolge der gezogenen Elemente nicht berücksichtigt wird?

Antwort:
Wenn der Lostopf aus den Elementen der Menge $M := [n]$ besteht, entspricht die Menge der möglichen Endergebnisse gerade der Menge aller

k-elementigen Multimengen über M, also aller Abbildungen $f : M \to \mathbb{N}$, für die gilt: $\sum_{x \in M} f(x) = k$.

Um zu zählen, wie viele solche Multimengen es gibt, nutzen wir den folgenden Trick: Wir repräsentieren eine k-elementige Multimenge $f : M \to \mathbb{N}$ durch das wie folgt definierte Wort w_f über dem Alphabet $\Sigma := \{a, b\}$:

$$w_f \quad := \quad a^{f(1)}\, b\, a^{f(2)}\, b\, \cdots\, b\, a^{f(n)}$$

Beispielsweise gilt für $n := 5$ und $k := 3$, dass das Wort *aabbbab* die Multimenge f mit $f(1) = 2$, $f(2) = f(3) = 0$, $f(4) = 1$ und $f(5) = 0$ repräsentiert.

Folie 248

Beachte: Für jede k-elementige Multimenge f über $[n]$ hat das Wort w_f die Länge $k+n-1$ und enthält genau $(n-1)$-mal den Buchstaben b. Und die Abbildung h, die jeder k-elementigen Multimenge f das Wort w_f zuordnet, ist eine Bijektion von der Menge der k-elementigen Multimengen von $[n]$ auf die Menge[4]

$$X \quad := \quad \left\{\, w \in \{a,b\}^* \,:\, |w| = k+n-1 \;\text{ und }\; |w|_b = n-1 \,\right\}$$

Nun ist $|X|$ genau die Anzahl der Möglichkeiten, aus der $(k+n-1)$-elementigen Menge aller Positionen des Wortes w diejenigen $n-1$ Positionen auszuwählen, an denen der Buchstabe b stehen soll. Also ist

$$|X| \quad = \quad \binom{k+n-1}{n-1}$$

Es gibt also beim *Ziehen mit Zurücklegen und ohne Berücksichtigung der Reihenfolge* insgesamt

$$\binom{k+n-1}{n-1}$$

Möglichkeiten, k Elemente aus einer n-elementigen Menge zu ziehen. Gemäß Satz 4.8(a) gilt: $\binom{k+n-1}{n-1} = \binom{k+n-1}{k} = \binom{n+k-1}{k}$.

4.3 Das Prinzip der Inklusion und Exklusion

Folie 249

Die Summenregel (Regel 4.1(b)) besagt, dass die Kardinalität der Vereinigung von paarweise disjunkten endlichen Mengen $A_1, \ldots, A_k$ genau die Summe der Kardinalitäten der Mengen $A_1, \ldots, A_k$ ist.

[4] $|w|_b$ bezeichnet die Anzahl der Vorkommen des Buchstabens b im Wort w.

Aber wie können wir $\left|\bigcup_{i=1}^{k} A_i\right|$ bestimmen, wenn die Mengen $A_1, \ldots, A_k$ *nicht* paarweise disjunkt sind?
Für $k = 2$ ist die Lösung ganz leicht:

$$|A_1 \cup A_2| \quad = \quad |A_1| + |A_2| - |A_1 \cap A_2| \,.$$

Das *Prinzip der Inklusion und Exklusion* (auch *Siebformel* genannt) verallgemeinert dies auf beliebige $k \in \mathbb{N}_{\geqslant 1}$:

Satz 4.9 (Prinzip der Inklusion und Exklusion; Siebformel)**.**
Sei $k \in \mathbb{N}_{\geqslant 1}$ und seien $A_1, \ldots, A_k$ beliebige endliche Mengen. Dann gilt:

$$\left|\bigcup_{i=1}^{k} A_i\right| \quad = \quad \sum_{\emptyset \neq I \subseteq [k]} (-1)^{|I|+1} \cdot \left|\bigcap_{i \in I} A_i\right| \,. \tag{4.9}$$

Beweis. Eine Möglichkeit, dies zu beweisen ist, per Induktion nach k vorzugehen. Details: Übungsaufgabe.

Wir geben hier einen anderen, rein kombinatorischen Beweis an: Wir zeigen für jedes beliebige $a \in \bigcup_{i=1}^{k} A_i$, dass a sowohl auf der linken Seite von (4.9) als auch auf der rechten Seite von (4.9) genau einmal gezählt wird. Daraus folgt dann direkt, dass die Gleichung (4.9) korrekt ist.

Wir nutzen dabei folgende Notation: Für jedes $I \subseteq [k]$ mit $I \neq \emptyset$ sei $A_I := \bigcap_{i \in I} A_i$.

Für den Rest des Beweises halten wir ein $a \in \bigcup_{i=1}^{k} A_i$ fest und setzen $J := \{j \in [k] \,:\, a \in A_j\}$. Offensichtlicherweise gilt f.a. $I \subseteq [k]$ mit $I \neq \emptyset$:

$$a \in A_I \quad \Longleftrightarrow \quad I \subseteq J$$

(denn: $a \in A_I \iff a \in A_i$ f.a. $i \in I \iff i \in J$ f.a. $i \in I \iff I \subseteq J$).

Offensichtlicherweise wird a auf der linken Seite von (4.9) genau einmal gezählt.

Wie oft wird a auf der rechten Seite von (4.9) gezählt?
Antwort: a schlägt bei genau denjenigen I mit $\emptyset \neq I \subseteq [k]$ zu Buche, für die $I \subseteq J$ gilt; und zwar für jedes solche I mit dem Wert $(-1)^{|I|+1}$. D.h.: Auf der rechten Seite von (4.9) wird a mit dem Wert

$$\sum_{\emptyset \neq I \subseteq J} (-1)^{|I|+1}$$

gezählt. Im Folgenden werden wir zeigen, dass diese Summe genau den Wert 1 ergibt. Dazu gruppieren wir die einzelnen Mengen I nach ihrer Mächtigkeit ℓ für jedes $\ell \in \{1, \ldots, n\}$ für $n := |J|$.
Wir wissen bereits, dass für jedes $\ell \in [n]$ gilt:

$$|\{I \subseteq J \,:\, |I| = \ell\}| \quad = \quad \binom{n}{\ell} \,.$$

Somit gilt:

$$\sum_{\emptyset \neq I \subseteq J} (-1)^{|I|+1} \quad = \quad \sum_{\ell=1}^{n} (-1)^{\ell+1} \cdot |\{I \subseteq J \,:\, |I| = \ell\}| \quad = \quad \sum_{\ell=1}^{n} (-1)^{\ell+1} \cdot \binom{n}{\ell} \,.$$

Wir nutzen die Binomische Formel für $(a+b)^n$ für $a := -1$ und $b := 1$, um diese Summe auszurechnen:

$$0 \;=\; (a+b)^n \;=\; \sum_{\ell=0}^{n} \binom{n}{\ell} a^\ell b^{n-\ell} \;=\; \sum_{\ell=0}^{n} \binom{n}{\ell} (-1)^\ell 1^{n-\ell} \;=\; \binom{n}{0} + \sum_{\ell=1}^{n} \binom{n}{\ell} (-1)^\ell \,.$$

Wir bringen $\binom{n}{0} = 1$ auf die linke Seite und erhalten dadurch:

$$-1 \quad = \quad \sum_{\ell=1}^{n} \binom{n}{\ell} (-1)^\ell \,.$$

Wir multiplizieren beide Seiten mit (-1) und erhalten:

$$1 \quad = \quad \sum_{\ell=1}^{n} \binom{n}{\ell} (-1)^{\ell+1} \quad = \quad \sum_{\ell=1}^{n} (-1)^{\ell+1} \cdot \binom{n}{\ell} \,.$$

Insgesamt erhalten wir, dass a auf der rechten Seite von (4.9) mit dem Wert

$$\sum_{\emptyset \neq I \subseteq J} (-1)^{|I|+1} \quad = \quad \sum_{\ell=1}^{n} (-1)^{\ell+1} \cdot \binom{n}{\ell} \quad = \quad 1$$

gezählt wird. Dies beendet den Beweis von Satz 4.9. □

Folie 250

Ein Anwendungsbeispiel der Siebformel

Beispiel 4.10. Wie viele Zahlen in der Menge $\{1, \ldots, 100\}$ gibt es, die ganzzahlig durch 2, 3 oder 5 teilbar sind?

Für jedes $k \in \mathbb{N}_{\geqslant 1}$ sei

$$V_k \quad := \quad \{\, i{\cdot}k \,:\, i \in \mathbb{N}_{\geqslant 1} \text{ und } i{\cdot}k \leqslant 100 \,\}$$

die Menge aller Vielfachen von k, die $\leqslant 100$ sind.
Die Antwort auf die obige Frage ist die Zahl $|V_2 \cup V_3 \cup V_5|$. Die Summenregel (Regel 4.1(b)) können wir nicht anwenden, da die Mengen nicht paarweise disjunkt sind. Aber wir können die Siebformel anwenden und erhalten:

$$\begin{aligned} & |V_2 \cup V_3 \cup V_5| \\ = \; & |V_2| + |V_3| + |V_5| - |V_2 \cap V_3| - |V_2 \cap V_5| - |V_3 \cap V_5| + |V_2 \cap V_3 \cap V_5|. \end{aligned}$$

Es gilt: $|V_k| = \lfloor \frac{100}{k} \rfloor$, also die größte natürliche Zahl j mit $j \leqslant \frac{100}{k}$. Somit ist $|V_2| = 50$, $|V_3| = 33$, $|V_5| = 20$.

Und	$V_2 \cap V_3 = V_6\,,$	also	$\lvert V_2 \cap V_3\rvert = \lvert V_6\rvert = \lfloor \frac{100}{6} \rfloor = 16\,.$
Analog ist	$V_2 \cap V_5 = V_{10}\,,$	also	$\lvert V_2 \cap V_5\rvert = \lvert V_{10}\rvert = 10\,;$
und	$V_3 \cap V_5 = V_{15}\,,$	also	$\lvert V_3 \cap V_5\rvert = \lvert V_{15}\rvert = \lfloor \frac{100}{15} \rfloor = 6\,;$
und	$V_2 \cap V_3 \cap V_5 = V_{30}\,,$	also	$\lvert V_2 \cap V_3 \cap V_5\rvert = \lfloor \frac{100}{30} \rfloor = 3\,.$

Insgesamt erhalten wir:

$$|V_2 \cup V_3 \cup V_5| \quad = \quad 50 + 33 + 20 - 16 - 10 - 6 + 3 \quad = \quad 74\,.$$

4.4 Prinzip des doppelten Abzählens

Folie 251

Bereits in einigen vorherigen Beweisen haben wir den folgenden, offensichtlichen Sachverhalt genutzt: Wenn wir eine endliche Liste von Zahlen gegeben haben und diese Zahlen aufsummieren wollen, ist egal in welcher genauen Reihenfolge wir die Zahlen addieren — es wird immer das gleiche Ergebnis herauskommen. Dies wird auch *Prinzip des doppelten Abzählens* genannt.

Regel 4.11 (Prinzip des doppelten Abzählens)**.**
Seien $n, m \in \mathbb{N}_{\geqslant 1}$. Es sei eine Tabelle gegeben, deren Zeilen mit $1, \ldots, n$ und deren Spalten mit $1, \ldots, m$ durchnummeriert sind. Für jedes $i \in [n]$ und $j \in [n]$ ist eine Zahl $a_{i,j} \in \mathbb{R}$ gegeben, die in der Tabelle in Zeile i und Spalte j eingetragen ist. Für jedes $i \in [n]$ sei z_i die Summe aller Einträge

in Zeile i, d.h. $z_i := \sum_{j=1}^{m} a_{i,j}$. Für jedes $j \in [m]$ sei s_j die Summe aller Einträge in Spalte j, d.h. $s_j := \sum_{i=1}^{n} a_{i,j}$. Dann gilt:

$$\sum_{i=1}^{n} z_i \quad = \quad \sum_{j=1}^{m} s_j \quad = \quad \sum_{(i,j)\in[n]\times[m]} a_{i,j} \; .$$

Beweis. Es gilt:

$$\sum_{i=1}^{n} z_i \quad = \quad \sum_{i=1}^{n}\sum_{j=1}^{m} a_{i,j} \quad = \quad \sum_{(i,j)\in[n]\times[m]} a_{i,j} \quad = \quad \sum_{j=1}^{n}\sum_{i=1}^{n} a_{i.j} \quad = \quad \sum_{j=1}^{n} s_j \; .$$

□

Folie 252

Ein typisches Anwendungsbeispiel des Prinzips des doppelten Abzählens ist der folgende Satz von Euler (1736).

Satz 4.12. *Für jeden endlichen ungerichteten Graphen $G = (V, E)$ gilt:*

$$\sum_{v\in V} \mathrm{Grad}_G(v) \quad = \quad 2 \cdot |E| \; .$$

D.h.: Die Summe der Grade aller Knoten von G ist genau 2 mal die Anzahl der Kanten von G.

Beweis. Wir nutzen das Prinzip des doppelten Abzählens (Regel 4.11) für $n := |V|$ und $m := |E|$. Sei $v_1, \ldots, v_n$ eine Auflistung aller Knoten von G und sei $e_1, \ldots, e_m$ eine Auflistung aller Kanten von G.
In die Tabelle A tragen wir in Zeile i und Spalte j den Eintrag

$$a_{i,j} \quad := \quad \begin{cases} 1 & \text{falls Knoten } v_i \text{ ein Endpunkt der Kante } e_j \text{ ist} \\ 0 & \text{sonst} \end{cases}$$

ein (für alle $i \in [n]$ und $j \in [m]$).
Für jedes $i \in [n]$ gilt dann: In Zeile i der Tabelle A stehen genau so viele Einsen wie es Kanten in G gibt, die den Knoten v_i als Endpunkt haben.
Somit gilt für $z_i := \sum_{j=1}^{n} a_{i,j}$, dass $z_i = \mathrm{Grad}_G(v_i)$ ist.
Daraus folgt, dass $\sum_{i=1}^{n} z_i = \sum_{v\in V} \mathrm{Grad}_G(v)$ die Summe der Grade aller Knoten von G ist.

Für jedes $j \in [m]$ gilt: In Spalte j der Tabelle A stehen genau 2 Einsen, nämlich in den beiden Zeilen, die den beiden Endpunkten der Kante e_j entsprechen. D.h. für jedes $j \in [m]$ gilt für $s_j := \sum_{i=1}^{n} a_{i,j}$, dass $s_j = 2$ ist. Somit ist $\sum_{j=1}^{m} s_j = 2 \cdot m = 2 \cdot |E|$.
Insgesamt erhalten wir:

$$2 \cdot |E| \;=\; \sum_{j=1}^{m} s_j \;\overset{\text{Regel 4.11}}{=}\; \sum_{i=1}^{n} z_i \;=\; \sum_{v \in V} \text{Grad}_G(v) \; .$$

□

Folie 253

Folgerung 4.13. *Für jeden endlichen ungerichteten Graphen $G = (V, E)$ gilt: Die Anzahl aller Knoten von G, deren Grad ungerade ist, ist gerade.*

Beweis. Durch Widerspruch. Angenommen, die Anzahl der Knoten von ungeradem Grad ist ungerade. Dann ist $\sum_{v \in V} \text{Grad}_G(v)$ ungerade. Aber Satz 4.12 besagt, dass $\sum_{v \in V} \text{Grad}_G(v) = 2 \cdot |E|$, also gerade ist. Widerspruch! □

Die Aussage von Folgerung 4.13 ist auch als *Handshaking Lemma* bzw. *Handschlaglemma* bekannt: Auf jeder Feier ist die Anzahl der Personen, die einer ungeraden Anzahl von Gästen zur Begrüßung die Hand schütteln, gerade.[5]

Folie 254

Wir betrachten ein weiteres Beispiel der Anwendung des Prinzips des doppelten Abzählens:

Beispiel 4.14. Sei X eine endliche Menge, sei $m \in \mathbb{N}_{\geqslant 1}$ und seien $M_1, \ldots, M_m \subseteq X$. Für jedes $x \in X$ sei $Anz(x) := |\{\, j \in [m] \,:\, x \in M_j \,\}|$, d.h. $Anz(x)$ gibt an, in wie vielen der Mengen $M_1, \ldots, M_m$ das Element x enthalten ist.

$$\textit{Behauptung:} \quad \sum_{x \in X} Anz(x) \;=\; \sum_{j \in [m]} |M_j|.$$

[5] Wir modellieren dies als ungerichteten Graphen: Jeder Knoten entspricht einem Gast, und es gibt genau dann eine Kante zwischen zwei Knoten v und w, wenn die Personen v und w sich zur Begrüßung die Hand schütteln.

Beweis. Sei $n := |X|$ und sei $x_1, \ldots, x_n$ eine Auflistung aller Elemente von X. Wir nutzen das Prinzip des doppelten Abzählens (Regel 4.11).
In die Tabelle A tragen wir in Zeile i und Spalte j den Eintrag

$$a_{i,j} \quad := \quad \begin{cases} 1 & \text{falls } x_i \in M_j \\ 0 & \text{sonst} \end{cases}$$

ein (für alle $i \in [n]$ und $j \in [m]$).
Für jedes $j \in [m]$ gilt: In Spalte j der Tabelle A steht in genau $|M_j|$ vielen Zeilen eine Eins; d.h. für $s_j := \sum_{i=1}^{n} a_{i,j}$ gilt: $s_j = |M_j|$.
Somit ist $\sum_{j=1}^{m} s_j = \sum_{j=1}^{m} |M_j|$.
Für jedes $i \in [n]$ gilt: In Zeile i der Tabelle A stehen genau so viele Einsen wie es Mengen aus $M_1, \ldots, M_m$ gibt, die x_i als Element enthalten. Somit gilt für $z_i := \sum_{j=1}^{n} a_{i,j}$, dass $z_i = Anz(x_i)$ ist.
Daraus folgt, dass $\sum_{i=1}^{n} z_i = \sum_{x \in X} Anz(x)$ ist.
Insgesamt erhalten wir:

$$\sum_{j=1}^{m} |M_j| \quad = \quad \sum_{j=1}^{m} s_j \quad \overset{\text{Regel 4.11}}{=} \quad \sum_{i=1}^{n} z_i \quad = \quad \sum_{x \in X} Anz(x) \; .$$

□

4.5 Das Schubfachprinzip

Folie 255

Das *Schubfachprinzip* (engl.: *Pigeonhole Principle*, „Taubenschlag-Prinzip“) beruht auf dem folgenden offensichtlichen Sachverhalt: Wenn man $N+1$ Dinge in N Schubfächer verteilt, dann wird es zwangsläufig ein Schubfach geben, in dem mindestens 2 Dinge landen. Dies lässt sich zu folgender Regel verallgemeinern:

Regel 4.15 (Schubfachprinzip)**.**
Seien $N, k \in \mathbb{N}_{\geqslant 1}$. Werden $\geqslant N \cdot k + 1$ Dinge auf N Schubfächer verteilt, so gibt es mindestens ein Schubfach, in dem mindestens $k+1$ Dinge landen.

Mathematisch präzise lässt sich dies wie folgt formulieren:[6]
Seien $N, k \in \mathbb{N}_{\geqslant 1}$, seien S und D Mengen mit $|S| = N$ und $|D| \geqslant N \cdot k + 1$, sei $f : D \to S$. Dann gilt: Es gibt ein $s \in S$ so dass $|f^{-1}(s)| \geqslant k+1$.

[6] S entspricht der Menge der Schubfächer, D entspricht der Menge der Dinge, die Funktion f gibt an, welches Ding in welches Schubfach verteilt wird. Für $s \in S$ ist $f^{-1}(s)$ dann die Menge der Dinge, die in Schubfach s landen.

Beweis. Sei $s_1, \ldots, s_N$ eine Auflistung aller Elemente von S. Für jedes $i \in [N]$ sei[7] $M_i := f^{-1}(s_i)$. Gemäß der Zerlegungsregel (Regel 4.1(c)) gilt:

$$|D| \;=\; \sum_{s \in S} \big|f^{-1}(s)\big| \;=\; \sum_{i=1}^{N} \big|f^{-1}(s_i)\big| \;=\; \sum_{i=1}^{N} |M_i| \,. \tag{4.10}$$

Wir müssen zeigen, dass es ein $i \in [N]$ gibt, so dass $|M_i| \geqslant k{+}1$ ist.
Wir führen einen Beweis durch Widerspruch und nehmen an, dass für alle $i \in [N]$ gilt: $|M_i| \leqslant k$.
Dann ist $\sum_{i=1}^{N} |M_i| \leqslant \sum_{i=1}^{N} k = N{\cdot}k$. Unter Verwendung von (4.10) erhalten wir: $|D| \leqslant N{\cdot}k$. Aber gemäß Voraussetzung ist $|D| \geqslant N{\cdot}k + 1$.
Widerspruch! □

Folie 256

Im Folgenden betrachten wir einige Beispiele zur Anwendung des Schubfachprinzips.

Beispiel 4.16. In jeder Menge von 13 Personen befinden sich zwei Personen, die im gleichen Monat Geburtstag haben.

Die 12 Monate Januar, …, Dezember sind hier die 12 Schubfächer, in die die 13 Personen verteilt werden.

Satz 4.17. *Für jeden endlichen ungerichteten Graphen $G = (V, E)$ mit $|V| \geqslant 2$ gilt: Es gibt zwei Knoten $v, w \in V$ mit $v \neq w$, die denselben Grad haben, d.h.* $\mathrm{Grad}_G(v) = \mathrm{Grad}_G(w)$.

Beweis. Sei $n := |V|$.

Fall 1: Es gibt keinen Knoten $u \in V$ vom Grad 0.
Dann gilt für alle Knoten $v \in V$: $\mathrm{Grad}_G(v) \in \{1, \ldots, n{-}1\}$ (denn: G ist ein ungerichteter Graph, also ist kein Knoten mit sich selbst benachbart; als Nachbarn eines Knotens $v \in V$ kommen also nur die $n{-}1$ Knoten in $V \setminus \{v\}$ in Frage).
D.h.: Wir haben n verschiedene Knoten in V; diese n Knoten werden auf $N := n{-}1$ Schubfächer namens $\{1, \ldots, n{-}1\}$ verteilt: Knoten v kommt in Schubfach $\mathrm{Grad}_G(v)$. Gemäß Schubfachprinzip müssen zwei Knoten im gleichen Schubfach landen, d.h. es gibt zwei Knoten vom gleichen Grad.
Genau das gleiche Argument können wir auch mathematisch formal aufschreiben:

[7] d.h.: M_i ist die Menge aller Dinge aus D, die in Schubfach s_i landen

Wir nutzen das Schubfachprinzip (Regel 4.15) für $S := \{1, \ldots, |V|-1\}$, $N := |S| = |V|-1$, $D := V$ und $k := 1$. Dann ist $|D| = N+1 = k \cdot N + 1$. Sei $f : D \to S$ die Funktion mit $f(v) := \text{Grad}_G(v)$ f.a. $v \in D$.

Gemäß Schubfachprinzip (Regel 4.15) gibt es ein $s \in S$ mit $|f^{-1}(s)| \geqslant k+1 = 2$. D.h.: Es gibt $v, w \in D = V$ mit $v \neq w$ und $\text{Grad}_G(v) = f(v) = f(w) = \text{Grad}_G(w)$.

Fall 2: Es gibt einen Knoten $u \in V$ vom Grad 0.
Dann gibt es keinen Knoten $v \in V$ vom Grad $|V|-1$, denn: u ist kein Nachbar von v und v ist auch kein Nachbar von sich selbst — also kommen nur die $|V|-2$ Knoten aus $V \setminus \{u, v\}$ als Nachbarn für Knoten v in Frage. Somit gilt für alle $v \in V$: $\text{Grad}_G(v) \in \{0, \ldots, |V|-2\}$.

Ähnlich wie in Fall 1 haben wir auch hier $n = |V|$ verschiedene Knoten in V; diese n Knoten werden auf $N := n-1$ Schubfächer namens $\{0, \ldots, n-2\}$ verteilt: Knoten v kommt in Schubfach $\text{Grad}_G(v)$. Gemäß Schubfachprinzip müssen zwei Knoten im gleichen Schubfach landen, d.h. es gibt zwei Knoten vom gleichen Grad.

Mathematisch formal können wir dieses Argument wie folgt aufschreiben:
Wir nutzen das Schubfachprinzip (Regel 4.15) für $S := \{0, \ldots, |V|-2\}$, $N := |S| = |V|-1$, $D := V$ und $k := 1$. Dann ist $|D| = N+1 = k \cdot N + 1$. Sei $f : D \to S$ die Funktion mit $f(v) := \text{Grad}_G(v)$ f.a. $v \in D$.

Gemäß Schubfachprinzip (Regel 4.15) gibt es ein $s \in S$ mit $|f^{-1}(s)| \geqslant k+1 = 2$. D.h.: Es gibt $v, w \in D = V$ mit $v \neq w$ und $\text{Grad}_G(v) = f(v) = f(w) = \text{Grad}_G(w)$. □

Folie 257

Im nächsten Anwendungsbeispiel nutzen wir beim Beweis eine Kombination aus vollständiger Induktion und dem Schubfachprinzip.

Definition 4.18.

(a) Ein *Dreieck* in einem ungerichteten Graphen $G = (V, E)$ ist eine Menge $M = \{v_1, v_2, v_3\} \subseteq V$ mit $|M| = 3$, so dass die die Knoten in M alle miteinander benachbart sind, d.h. $\{v_i, v_j\} \in E$ für alle $i, j \in [3]$ mit $i \neq j$.

(b) Ein ungerichteter Graph heißt *dreiecksfrei*, falls er kein Dreieck enthält.

Beispiel: Für jedes $n \in \mathbb{N}_{\geqslant 1}$ ist der vollständig bipartite Graph $K_{n,n}$ dreiecksfrei. Dieser Graph hat $2n$ Knoten und n^2 Kanten.

Frage: Wie viele Kanten kann kann ein dreiecksfreier Graph auf $2n$ Knoten maximal haben? *Zur Erinnerung:* Der vollständige Graph K_{2n} auf $2n$ Knoten hat $\frac{1}{2} \cdot 2n \cdot (2n-1) \;=\; n^2 + n \cdot (n-1)$ Kanten.

Antwort: n^2 — gemäß dem folgenden Satz 4.19.

Satz 4.19 (*Satz von Mantel*, 1907)**.**
Für jedes $n \in \mathbb{N}_{\geqslant 1}$ und jeden ungerichteten Graphen $G = (V, E)$ mit $|V| = 2n$ und $|E| > n^2$ gilt: G besitzt ein Dreieck.

Beweis. Wir führen den Beweis per Induktion nach n.

Induktionsanfang: $n = 1$.
Für jeden ungerichteten Graphen $G = (V, E)$ mit $|V| = 2$ gilt: $|E| \leqslant 1$.
D.h.: Für $n = 1$ gibt es keinen ungerichteten Graphen $G = (V, E)$ mit $|V| = 2n$ und $|E| > n^2$. Somit gilt für jeden (der nicht-existierenden) ungerichteten Graphen $G = (V, E)$ mit $|V| = 2n = 2$ und $|E| > n^2 = 1$, dass G ein Dreieck besitzt.

Induktionsschritt: $n \mapsto n+1$.
Sei $n \in \mathbb{N}_{\geqslant 1}$ beliebig.

Induktionsannahme: Für jeden ungerichteten Graphen $G' = (V', E')$ mit $|V'| = 2n$ und $|E'| > n^2$ gilt: G' besitzt ein Dreieck.

Behauptung: Für jeden ungerichteten Graphen $G = (V, E)$ mit $|V| = 2(n+1)$ und $|E| > (n+1)^2$ gilt: G besitzt ein Dreieck.

Beweis: Sei $G = (V, E)$ ein beliebiger ungerichteter Graph mit $|V| = 2(n+1)$ und $|E| > (n+1)^2$, d.h. $|E| \geqslant (n+1)^2 + 1$.
Wir müssen zeigen, dass G ein Dreieck besitzt.

Wähle zwei Knoten $x, y \in V$, die durch eine Kante verbunden sind, d.h.: $\{x, y\} \in E$. Sei $G' := (V', E')$ der Graph, der aus G durch Löschen der Knoten x und y entsteht. D.h.: $V' = V \setminus \{x, y\}$ und $E' := \{e \in E \,:\, e \cap \{x, y\} = \emptyset\}$.

Fall 1: $|E'| > n^2$.
Dann ist G' ein Graph mit $2n$ Knoten und mehr als n^2 Kanten. Gemäß Induktionsannahme besitzt G' ein Dreieck $M = \{v_1, v_2, v_3\}$. Da G' ein Teilgraph von G ist, ist M auch ein Dreieck von G.

Fall 2: $|E'| \leqslant n^2$. Sei F die Menge aller Kanten von G, die genau einen der beiden Knoten x, y als Endpunkt haben. Dann gilt:

$$E \;\;=\;\; E' \;\dot\cup\; F \;\dot\cup\; \big\{\, \{x, y\} \,\big\} \,.$$

Also ist $|F| = |E| - |E'| - 1$.
Wegen $|E'| \leqslant n^2$ ist daher $|F| \geqslant |E| - n^2 - 1$.
Wegen $|E| \geqslant (n+1)^2 + 1$ ist also

$$|F| \quad \geqslant \quad (n+1)^2 - n^2 \quad = \quad n^2 + 2n + 1 - n^2 \quad = \quad 2n + 1 \; .$$

Wir wissen: $|V'| = 2n$ und $V = V' \dot\cup \{x, y\}$. Sei $v_1, \ldots, v_{2n}$ eine Auflistung aller Knoten in V'. Es gilt:

$$F \quad \subseteq \quad \big\{ \{x, v_i\} \,:\, i \in [2n] \big\} \;\cup\; \big\{ \{y, v_i\} \,:\, i \in [2n] \big\} \qquad \text{und} \qquad |F| \geqslant 2n+1 \; .$$

Gemäß Schubfachprinzip[8] muss es daher ein $i \in [2n]$ geben, so dass $\{x, v_i\} \in F$ und $\{y, v_i\} \in F$.
Somit gilt: $\{x, v_i\} \in E$ und $\{y, v_i\} \in E$ und $\{x, y\} \in E$. Also bilden die Knoten x, y, v_i ein Dreieck in G. □

4.6 Der Satz von Ramsey

Folie 258

Die *Ramsey-Theorie* ist ein Zweig der Kombinatorik, der von Frank P. Ramsey (1903–1930) gegründet wurde. Er beschäftigt sich mit Kanten-Färbungen von Graphen und Verallgemeinerungen hiervon.

Einen beliebigen ungerichteten Graphen $G = (V, E)$ mit $n := |V|$ Knoten stellen wir uns hierbei als Kanten-gefärbte Version des vollständigen Graphen K_n vor: Für jedes $e \in E$ erhält die Kante e in K_n die Farbe *rot*. Für jedes $e \in \mathcal{P}_2(V)$ mit $e \notin E$ erhält die Kante e in K_n die Farbe *blau*.

Wir behandeln hier nur die einfachste Version der Aussage von Rameys Theorem. Dazu benötigen wir die folgenden Begriffe.

Folie 259

Definition 4.20. Sei $k \in \mathbb{N}_{\geqslant 1}$ und sei $G = (V, E)$ ein ungerichteter Graph.

(a) Eine *Clique* der Größe k in G ist eine Menge C von k Knoten von G, die paarweise benachbart zu einander sind. D.h.: $C \subseteq V$ mit $|C| = k$ und es gilt $\{v, w\} \in E$ für alle $v, w \in C$ mit $v \neq w$.

Unter Verwendung von den in Kapitel 3 eingeführten Notationen lässt sich dies kurz schreiben als $G|_C \cong K_k$.[9]

[8] Wir nutzen $N := 2n$ Schubfächer namens $1, \ldots, N$. Die Dinge, die in diese Schubfächer verteilt werden, sind die Elemente in F. Jede Kante $e \in F$ landet in Schubfach $i \in [N]$, falls der Knoten v_i ein Endpunkt der Kante e ist. Da $|F| \geqslant N+1$ ist, müssen 2 Kanten im gleichen Schubfach landen. D.h. es gibt ein $i \in [N]$ und zwei Kanten $e, e' \in F$ mit $e \neq e'$, die beide den Knoten v_i als Endpunkt haben. Der andere Endpunkt der Kanten e, e' kann jeweils nur der Knoten x oder der Knoten y sein.

[9] D.h. der durch C induzierte Teilgraph von G ist ein vollständiger Graph auf k Knoten.

(b) Eine *unabhängige Menge* der Größe k in G ist eine Menge U von k Knoten von G, die paarweise nicht miteinander benachbart sind. D.h.: $U \subseteq V$ mit $|U| = k$ und es gilt $\{v, w\} \notin E$ für alle $v, w \in U$ mit $v \neq w$.

Unter Verwendung von den in Kapitel 3 eingeführten Notationen lässt sich dies kurz schreiben als $G|_U \cong (U, \emptyset)$.[10]

Folie 260

Der Satz von Ramsey besagt Folgendes für beliebige Zahlen $k, \ell \in \mathbb{N}_{\geqslant 1}$:

In jeder hinreichend großen Gruppe von Personen gibt es eine Gruppe von k Personen, die sich alle untereinander kennen (d.h. eine Clique der Größe k) oder eine Gruppe von ℓ Personen, die sich alle gegenseitig unbekannt sind (d.h. eine unabhängige Menge der Größe ℓ).

Diese Aussage wird durch den folgenden Satz formalisiert, der auch angibt, was genau mit „hinreichend groß“ gemeint ist.

Satz 4.21 (Satz von Ramsey)**.** *Für alle $k, \ell \in \mathbb{N}_{\geqslant 1}$ gibt es eine Zahl*[11] *$R(k, \ell) \in \mathbb{N}$, so dass für jeden ungerichteten Graphen $G = (V, E)$ mit $|V| \geqslant R(k, \ell)$ mindestens eine der beiden folgenden Aussagen erfüllt ist:*

(A) G besitzt eine Clique der Größe k.

(B) G besitzt eine unabhängige Menge der Größe ℓ.

Außerdem gilt: $R(k, \ell) \leqslant \binom{k+\ell-2}{k-1}$.

Beweis. Per Induktion nach $k+\ell$.

Induktionsanfang: Betrachte beliebige $k, \ell \in \mathbb{N}_{\geqslant 1}$ mit $k = 1$ oder $\ell = 1$. In jedem ungerichteten Graphen $G = (V, E)$ mit $|V| \geqslant 1$ können wir einfach einen beliebigen Knoten $v \in V$ wählen und $M := \{v\}$ setzen. M ist sowohl eine Clique der Größe 1 als auch eine unabhängige Menge der Größe 1. Insbesondere ist also im Fall $k = 1$ die Aussage (A) und im Fall $\ell = 1$ die Aussage (B) erfüllt.

Wir müssen nur noch nachrechnen, dass $\binom{k+\ell-2}{k-1} \geqslant 1$ ist.

Wir nutzen die Gleichung $\binom{N}{K} = \binom{N}{N-K}$ (Satz 4.8(a)) für $N := k+\ell-2$ und $K := k-1$ und beachten, dass dann $N-K = \ell-1$ ist. Laut Voraussetzung

[10] D.h. der durch U induzierte Teilgraph von G besitzt keine Kante(n).

[11] Die kleinstmögliche Zahl, die man als $R(k, \ell)$ wählen kann, wird „die zu k und ℓ gehörige *Ramsey-Zahl*“ genannt.

ist $k = 1$ oder $\ell = 1$. Also gilt: $\binom{k+\ell-2}{k-1} = \binom{k+\ell-2}{\ell-1} = \binom{k+\ell-2}{0} = 1$ (gemäß Beobachtung 4.4(a)).

INDUKTIONSSCHRITT: Betrachte beliebige $k, \ell \in \mathbb{N}_{\geqslant 1}$ mit $k \geqslant 2$ und $\ell \geqslant 2$.
Induktionsannahme: Für alle $k', \ell' \in \mathbb{N}_{\geqslant 1}$ mit $k'+\ell' < k+\ell$ gilt: Es gibt eine Zahl $R(k', \ell') \in \mathbb{N}$ mit $R(k', \ell') \leqslant \binom{k'+\ell'-2}{k'-1}$, so dass für jeden ungerichteten Graphen $G' = (V', E')$ mit $|V'| \geqslant R(k', \ell')$ gilt:

(A) G' besitzt eine Clique der Größe k' oder
(B) G' besitzt eine unabhängige Menge der Größe ℓ'.

Sei $G = (V, E)$ ein beliebiger ungerichteter Graph mit $|V| \geqslant \binom{k+\ell-2}{k-1}$.
Behauptung: G besitzt eine Clique der Größe k oder eine unabhängige Menge der Größe ℓ.

Beweis: Wir wählen einen beliebigen Knoten $v \in V$. Sei V_1 die Menge aller Nachbarn von v in G, und sei V_2 die Menge aller Knoten $\neq v$ in V, die keine Nachbarn von v in G sind. Dann gilt: $V = \{v\} \dot\cup V_1 \dot\cup V_2$.
Sei $G_1 := G|_{V_1}$ und $G_2 := G|_{V_2}$.
Sei $k_1 := k-1$ und $\ell_1 := \ell$. Sei $k_2 := k$ und $\ell_2 := \ell-1$. Dann gilt: $k_1+\ell_1 = k_2+\ell_2 = k+\ell-1$. Somit können wir die Induktionsannahme sowohl auf die Zahlen k_1, ℓ_1 als auch auf die Zahlen k_2, ℓ_2 anwenden.

Fall 1: $|V_1| \geqslant R(k_1, \ell_1)$.
Dann liefert die Induktionsannahme, dass für die Zahlen k_1, ℓ_1 und den Graphen G_1 gilt:

(A) G_1 besitzt eine Clique C_1 der Größe k_1 oder
(B) G_1 besitzt eine unabhängige Menge U_1 der Größe ℓ_1.

Wenn (B) gilt, dann ist U_1 eine unabhängige Menge der Größe $\ell_1 = \ell$ in G.
Wenn (B) nicht gilt, muss (A) gelten. Dann ist $C := C_1 \cup \{v\}$ eine Clique der Größe k in G, denn: $|C| = k_1+1 = k$, und v ist adjazent zu jedem Knoten in V_1, also insbes. auch zu jedem Knoten in C_1.
D.h. in Fall 1 ist die Behauptung bewiesen.

Fall 2: $|V_2| \geqslant R(k_2, \ell_2)$.
Dann liefert die Induktionsannahme, dass für die Zahlen k_2, ℓ_2 und den Graphen G_2 gilt:

(A) G_2 besitzt eine Clique C_2 der Größe k_2 oder
(B) G_2 besitzt eine unabhängige Menge U_2 der Größe ℓ_2.

Wenn (A) gilt, so ist C_2 eine Clique der Größe $k_2 = k$ in G.
Wenn (A) nicht gilt, muss (B) gelten. Dann ist $U := U_2 \cup \{v\}$ eine unabhängige Menge der Größe ℓ in G, denn: $|U| = \ell_2{+}1 = \ell$, und v ist zu keinem Knoten aus V_2 adjazent, also insbes. auch zu keinem Knoten in U_2. D.h. in Fall 2 ist die Behauptung bewiesen.

Wir schließen den Beweis ab, indem wir zeigen, dass einer der beiden Fälle 1 bzw. 2 eintreten muss. Wir führen einen indirekten Beweis. Angenommen, $|V_1| < R(k_1, \ell_1)$ und $|V_2| < R(k_2, \ell_2)$. Dann gilt:

$$\begin{aligned} |V| &= 1 + |V_1| + |V_2| \\ &\leqslant 1 + R(k_1, \ell_1) - 1 + R(k_2, \ell_2) - 1 \\ &\leqslant 1 + \tbinom{k_1+\ell_1-2}{k_1-1} - 1 + \tbinom{k_2+\ell_2-2}{k_2-1} - 1 \\ &< \tbinom{k_1+\ell_1-2}{k_1-1} + \tbinom{k_2+\ell_2-2}{k_2-1} . \end{aligned}$$

Beachte, dass $k_1{+}\ell_1{-}2 = k_2{+}\ell_2{-}2 = k{+}\ell{-}3$ und $k_1{-}1 = k{-}2$ und $k_2{-}1 = k{-}1$. Wir nutzen die Gleichung $\binom{N+1}{K} = \binom{N}{K-1} + \binom{N}{K}$ (Pascal'scher Rekurrenzsatz, Satz 4.5) für $N := k{+}\ell{-}3$ und $K := k{-}1$ und erhalten dadurch Folgendes:

$$\begin{aligned} |V| &< \tbinom{k_1+\ell_1-2}{k_1-1} + \tbinom{k_2+\ell_2-2}{k_2-1} \\ &= \tbinom{k+\ell-3}{k-2} + \tbinom{k+\ell-3}{k-1} \\ &= \tbinom{k+\ell-2}{k-1} . \end{aligned}$$

Dies ist ein Widerspruch zu unserer Wahl von G, da ja $|V| \geqslant \binom{k+\ell-2}{k-1}$ ist. Dies beendet den Beweis von Satz 4.21. □

4.7 Literaturhinweise

Als vertiefende Lektüre seien Kapitel 1 von [Ste07] und Kapitel 3 von [Juk08] sowie das Lehrbuch [Cam94] empfohlen.

Quellennachweis: Teile der Abschnitte 4.1–4.5 basieren auf Teilen von Kapitel 1 von [Ste07] und Kapitel 3 von [Juk08].

4.8 Übungsaufgaben

Aufgabe 4.1. Für ein $n \in \mathbb{N}$ seien 2^n Münzen gegeben, die wir im Folgenden mit $M_1, \ldots, M_{2^n}$ bezeichnen. Alle Münzen bis auf eine sind gleich schwer; diese eine Münze ist etwas schwerer als jede einzelne andere Münze. Diese Münze lässt sich mithilfe einer Balkenwaage wie folgt finden:

1. Falls $n = 0$, ist die gesuchte Münze die einzige, die vorhanden ist.

2. Ansonsten vergleiche das Gesamtgewicht der Münzen aus der Menge $A := \{M_1, \ldots, M_{2^{n-1}}\}$ mit dem Gesamtgewicht der Münzen aus der Menge $B := \{M_{2^{n-1}+1}, \ldots, M_{2^n}\}$. Ist das Gesamtgewicht von A größer als das von B, muss sich die gesuchte Münze in A befinden und das beschriebene Verfahren wird rekursiv auf die Menge A angewendet, andernfalls wird es rekursiv auf die Menge B angewendet.

(a) Beschreiben Sie das Verfahren für $n = 2$ durch einen Entscheidungsbaum. Wählen Sie hierfür geeignete Kanten- und Knotenbeschriftungen.

(b) Ist der von Ihnen in Teilaufgabe (a) aufgestellte Entscheidungsbaum ein Binärbaum? Ist er ein vollständiger Binärbaum?

(c) Welchen Situationen im Entscheidungsprozess entsprechen die inneren Knoten des Baumes? Welcher Situation entspricht ein Blatt?

(d) Wie viele Wiegevorgänge müssen für 2^n Münzen mindestens durchgeführt werden? Wie viele Wiegevorgänge sind im schlimmsten Fall, also höchstens, nötig?

(e) Gegeben seien jetzt 9 Münzen; 8 davon sind gleichschwer und eine ist etwas schwerer als jede der 8 anderen Münzen. Überlegen Sie sich ein Verfahren, mit dem Sie mit Hilfe der Balkenwaage und so wenigen Wiegevorgängen wie möglich die schwerere Münze finden können.

Aufgabe 4.2. Seien $n, k \in \mathbb{N}$ mit $n \geqslant 2$ und $k \leqslant n$ und sei $G_{n\times n}$ ein $(n \times n)$-Schachbrett, welches wir durch das $(n \times n)$ Gitter repräsentieren (siehe Aufgabe 3.3). Wir haben eine große Anzahl von schwarzen Spielsteinen zur Verfügung, die alle gleich aussehen. Und wir haben eine große Anzahl von weißen Spielsteinen zur Verfügung, die alle gleich aussehen.

(a) Wie viele Möglichkeiten gibt es, n schwarze Steine auf einem $(n \times n)$-Schachbrett zu platzieren, sodass in jeder Zeile und in jeder Spalte genau ein Stein liegt?

(b) Wie viele Möglichkeiten gibt es, $n-k$ schwarze und k weiße Steine so auf ein $(n \times n)$-Schachbrett zu stellen, dass keine zwei Steine in der gleichen Zeile oder Spalte stehen?

Begründen Sie jeweils, warum Ihre Antwort korrekt ist.

Aufgabe 4.3.

(a) Wir sagen, dass eine endliche Menge gerade bzw. ungerade ist, falls sie eine gerade bzw. ungerade Anzahl an Elementen enthält. Beweisen Sie, dass jede endliche, nicht-leere Menge genau so viele gerade wie ungerade Teilmengen enthalten muss.

(b) Sei $n \in \mathbb{N}$ beliebig. Wie viele Wörter der Länge n können über dem Alphabet $\Sigma = \{a, b\}$ gebildet werden, die ungerade viele a's enthalten?

(c) Bestimmen Sie die Anzahl der durch 6, 8 oder 20 teilbaren natürlichen Zahlen kleiner gleich 200.

Aufgabe 4.4. Seien A, B endliche, nicht-leere Mengen; sei $m := |A|$ und $\ell := |B|$.

(a) Wie viele injektive Funktionen von A nach B gibt es?

(b)* Wie viele surjektive Funktionen von A nach B gibt es?

Hinweis: Betrachten Sie für jedes $b \in B$ die Menge $M_b := \{f : A \to B \,:\, \text{f.a. } a \in A : f(a) \neq b\}$ und wenden Sie die Siebformel an.
Falls das nicht weiterhilft, führen Sie eine Literaturrecherche zum Stichwort *Stirling-Zahlen* durch.

Begründen Sie jeweils Ihre Antwort.

Aufgabe 4.5.

(a) Betrachten Sie den Beweis von Satz 4.7 und arbeiten Sie die dort fehlenden Details aus. D.h. beweisen Sie, dass

$$| \{f \in \text{Abb}([k],[k]) \,:\, f \text{ ist bijektiv}\} | \;=\; k!$$

und dass $h : \mathcal{P}_k([n]) \times B \to A$ bijektiv ist, wobei

$$h(X, f) := t_{X,f}.$$

(b) Beweisen Sie Satz 4.9 per Induktion.

Aufgabe 4.6.

(a) Sei $n \in \mathbb{N}_{\geqslant 1}$ mit $n \geqslant 2$ und $S \subseteq \{1, \ldots, 2n\}$ mit $|S| = n + 1$. Beweisen Sie die folgenden Aussagen:

(i) Es gibt zwei Zahlen $a, b \in S$, sodass $b = a + 1$ gilt.

(ii) Es gibt zwei Zahlen $a, b \in S$, sodass $a + b = 2n + 1$ gilt.

(iii) Es gibt zwei ungleiche Zahlen $a, b \in S$, sodass a ein Teiler von b ist.

(b) Seien $k, n \in \mathbb{N}_{\geqslant 1}$. Beweisen Sie, dass $\prod_{i=n}^{n+k-1} i$ durch k teilbar ist.

Aufgabe 4.7.

(a) Bestimmen Sie die zu $k = 3$ und $\ell = 3$ gehörige Ramsey-Zahl $R(3, 3)$, d.h. die kleinste natürliche Zahl n, sodass für jeden ungerichteten Graphen $G = (V, E)$ mit $|V| \geqslant n$ gilt: G besitzt eine Clique der Größe 3 oder eine unabhängige Menge der Größe 3.

Um zu beweisen, dass die von Ihnen gefundene Zahl n kleinstmöglich ist, geben Sie einen konkreten Graphen mit $n-1$ Knoten an, in dem es weder ein Dreieck gibt, noch eine unabhängige Menge der Größe 3.

(b) Betrachten Sie den vollständigen Graphen K_6. *Sim* ist das folgendermaßen auf K_6 definierte Spiel:

Es spielen zwei Spieler:innen, *Ruth*, welche einen roten Buntstift verwendet, und *Bob*, welcher mit einem blauen Buntstift ausgestattet ist. Die beiden markieren nun abwechselnd mit ihrem Buntstift eine Kante in K_6, wobei Ruth beginnt. Eine Kante darf höchstens einmal markiert werden. Das Spiel endet, sobald eine:r der beiden ein einfarbiges Dreieck einzeichnet, das heißt, sobald drei rote oder drei blaue Kanten in K_6 einen Kreis bilden. Diese Person verliert das Spiel.

Ziel ist es demnach, Kanten einzufärben, ohne jemals ein einfarbiges Dreieck zu zeichnen. Die Anzahl der Züge des Spiels ist offensichtlich durch $\binom{6}{2} = \frac{6 \cdot 5}{2} = 15$ beschränkt, da K_6 nur so viele Kanten besitzt.

Beweisen Sie, dass keine Partie des Spiels mit einem „Unentschieden“ enden kann.

Kapitel 5

Stochastik

5.1 Ereignisse und ihre Wahrscheinlichkeiten

Folie 261

Definition 5.1 (Wahrscheinlichkeitsraum)**.**
Ein *endlicher Wahrscheinlichkeitsraum* (Ω, P) besteht aus einer endlichen, nicht-leeren Menge Ω von *Ergebnissen* bzw. *Elementarereignissen*, denen *Wahrscheinlichkeiten* $\mathrm{P}(\omega) = p_\omega \in \mathbb{R}$ für jedes $\omega \in \Omega$ zugeordnet sind, so dass gilt:

$$0 \leqslant p_\omega \leqslant 1, \quad \text{für jedes } \omega \in \Omega, \qquad \text{und} \qquad \sum_{\omega \in \Omega} p_\omega = 1.$$

Die Menge Ω fassen wir hierbei als die Menge aller möglichen Ergebnisse eines Zufallsexperiments auf. Für jedes $\omega \in \Omega$ gibt $\mathrm{P}(\omega)$ die Wahrscheinlichkeit an, dass eine einmalige Durchführung des Zufallsexperiments das Ergebnis ω liefert.

Folie 262

Beispiel 5.2 (2-maliger Münzwurf)**.**
Wir werfen zwei mal hintereinander eine „faire“ Münze, d.h. eine Münze, die jeweils mit Wahrscheinlichkeit $\frac{1}{2}$ auf „Kopf“ bzw. auf „Zahl“ landet.[1] Als Wahrscheinlichkeitsraum betrachten wir dazu die Menge

$$\Omega = \{KK,\ KZ,\ ZK,\ ZZ\},$$

wobei z.B. KK für das Elementarergeignis steht, dass die Münze bei beiden Würfen auf „Kopf“ landet, und ZK für das Elementarereignis steht, dass

[1] Wir gehen davon aus, dass das Landen auf „Kopf“ bzw. „Zahl“ die einzigen möglichen Ergebnisse sind — d.h. es kann nie passieren, dass die Münze „auf dem Rand stehenbleibt“.

die Münze beim ersten Wurf auf „Zahl“ und beim zweiten Wurf auf „Kopf“ landet. Jedes der 4 möglichen Elementarereignisse hat hier dieselbe Wahrscheinlichkeit, d.h. für jedes $\omega \in \Omega$ ist hier $\mathrm{P}(\omega) = \frac{1}{4}$.

Folie 263

Definition 5.3 (Ereignisse)**.**
Ein *Ereignis* ist eine Menge von Ergebnissen, d.h. eine Teilmenge von Ω.
Die *Wahrscheinlichkeit* eines Ereignisses $A \subseteq \Omega$ ist definiert als

$$\mathrm{P}(A) \;:=\; \sum_{\omega \in A} \mathrm{P}(\omega)\,.$$

Wir schreiben $\bar{A}$ um das *Komplement* von A zu bezeichnen, d.h. $\bar{A} := \Omega \setminus A$.

Anschaulich bedeutet die Aussage „Ereignis A tritt ein“, dass wir als Ergebnis eines Zufallsexperiments ein Elementarereignis $\omega \in A$ erhalten. Dies geschieht mit Wahrscheinlichkeit $\mathrm{P}(A)$.

Die Aussage „Ereignis A tritt nicht ein“ entspricht gerade der Situation, in der wir als Ergebnis eines Zufallsexperiments ein Elementarereignis $\omega \in \bar{A}$ erhalten.

Folie 264

Beispiel 5.4. Für den in Beispiel 5.2 betrachteten Wahrscheinlichkeitsraum Ω ist z.B.

$$A \;:=\; \{KK,\ KZ,\ ZK\}$$

das Ereignis, bei dem bei mindestens einem der beiden Münzwürfe die Münze auf „Kopf“ landet. Die Wahrscheinlichkeit, dass dieses Ereignis eintritt, ist $\mathrm{P}(A) = \frac{3}{4}$.
Entsprechend ist $\bar{A} = \{ZZ\}$ das Ereignis, bei dem bei keinem der beiden Münzwürfe die Münze auf „Kopf“ landet. Dieses Ereignis tritt mit Wahrscheinlichkeit $\mathrm{P}(\bar{A}) = \frac{1}{4}$ ein.

Folie 265

Bemerkung 5.5 (Regeln zum Rechnen mit Wahrscheinlichkeiten)**.**
Man kann sich leicht davon überzeugen, dass für jeden endlichen Wahrscheinlichkeitsraum (Ω, P) und alle Ereignisse A und B gilt:

$$\mathrm{P}(\bar{A}) \;=\; 1 \;-\; \mathrm{P}(A)\,, \tag{5.1}$$

$$\mathrm{P}(A \cup B) \;=\; \mathrm{P}(A) \;+\; \mathrm{P}(B) \;-\; \mathrm{P}(A \cap B)\,. \tag{5.2}$$

Für $s \in \mathbb{N}_{\geqslant 1}$ und für beliebige Ereignisse $A_1, \ldots, A_s \subseteq \Omega$ gilt:

$$\mathrm{P}(A_1 \cup \cdots \cup A_s) \quad \leqslant \quad \sum_{i=1}^{s} \mathrm{P}(A_i)\,. \tag{5.3}$$

Hier ist $\mathrm{P}(A_1 \cup \cdots \cup A_s)$ gerade die Wahrscheinlichkeit dafür, dass mindestens eins der Ereignisse $A_1, \ldots, A_s$ eintritt, d.h. die Wahrscheinlichkeit dafür, dass wir als Ergebnis des Zufallsexperiments ein Elementarereignis $\omega \in A_1 \cup \cdots \cup A_s$ erhalten.Die Abschätzung (5.3) ist auch unter der Bezeichnung *Union Bound* bekannt.

Sind die Ereignisse $A_1, \ldots, A_s$ paarweise disjunkt, d.h. ist $A_i \cap A_j = \emptyset$ für alle $i, j \in \{1, \ldots, s\}$ mit $i \neq j$, so gilt sogar

$$\mathrm{P}(A_1 \cup \cdots \cup A_s) \quad = \quad \sum_{i=1}^{s} \mathrm{P}(A_i)\,. \tag{5.4}$$

Beweis. Da (Ω, P) ein endlicher Wahrscheinlichkeitsraum ist, gilt insbes.

$$\sum_{\omega \in \Omega} \mathrm{P}(\omega) \quad = \quad 1.$$

Beweis von (5.1): Für ein beliebiges $A \subseteq \Omega$ gilt: $A \cap \bar{A} = \emptyset$ und $A \cup \bar{A} = \Omega$. Somit gilt:

$$1 \;=\; \sum_{\omega \in \Omega} \mathrm{P}(\omega) \;=\; \sum_{\omega \in A} \mathrm{P}(\omega) + \sum_{\omega \in \bar{A}} \mathrm{P}(\omega) \;=\; \mathrm{P}(A) + \mathrm{P}(\bar{A}).$$

Somit ist $\mathrm{P}(\bar{A}) = 1 - \mathrm{P}(A)$.

Beweis von (5.2): Betrachte nun beliebige $A, B \subseteq \Omega$. Es gilt: $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$, und die drei Mengen $(A \setminus B)$, $(B \setminus A)$ und $(A \cap B)$ sind paarweise disjunkt. Außerdem gilt: $A = (A \setminus B) \,\dot\cup\, (A \cap B)$ und $B = (B \setminus A) \,\dot\cup\, (A \cap B)$. Somit gilt:

$$\begin{aligned}
\mathrm{P}(A) + \mathrm{P}(B) \;&=\; \sum_{\omega \in A} \mathrm{P}(\omega) \;+\; \sum_{\omega \in B} \mathrm{P}(\omega) \\
&=\; \sum_{\omega \in A \setminus B} \mathrm{P}(\omega) \;+\; \sum_{\omega \in A \cap B} \mathrm{P}(\omega) \;+\; \sum_{\omega \in B \setminus A} \mathrm{P}(\omega) \;+\; \sum_{\omega \in A \cap B} \mathrm{P}(\omega) \\
&=\; \sum_{\omega \in A \cup B} \mathrm{P}(\omega) \;+\; \sum_{\omega \in A \cap B} \mathrm{P}(\omega) \\
&=\; \mathrm{P}(A \cup B) + \mathrm{P}(A \cap B).
\end{aligned}$$

Somit gilt also: $\mathrm{P}(A \cup B) = \mathrm{P}(A) + \mathrm{P}(B) - \mathrm{P}(A \cap B)$.

Beweis von (5.3)*:* Sei nun $s \in \mathbb{N}_{\geqslant 1}$ und seien $A_1, \ldots, A_s \subseteq \Omega$ und sei $V = A_1 \cup \cdots \cup A_s$. Für jedes $\omega \in V$ gibt es mindestens ein $i \in [s]$, so dass $\omega \in A_i$ ist — aber es könnte auch mehrere verschiedene $i_1, i_2, \ldots$ geben, so dass $\omega \in A_{i_1}$ und $\omega \in A_{i_2}$ etc. ist. Auf jeden Fall gilt:

$$\sum_{i=1}^{s} \mathrm{P}(A_i) \;=\; \sum_{i=1}^{s} \sum_{\omega \in A_i} \mathrm{P}(\omega) \;\geqslant\; \sum_{\omega \in V} \mathrm{P}(\omega) \;=\; \mathrm{P}(V)\,.$$

Somit gilt also: $\mathrm{P}(A_1 \cup \cdots \cup A_s) \leqslant \sum_{i=1}^{s} \mathrm{P}(A_i)$.

Beweis von (5.4)*:* Seien nun $A_1, \ldots, A_s \subseteq \Omega$ paarweise disjunkt und sei $V := A_1 \cup \cdots \cup A_s$. Dann gilt für jedes $\omega \in V$: Es gibt genau ein $i \in [s]$ so dass $\omega \in A_i$ ist. Daher gilt:

$$\mathrm{P}(V) \;=\; \sum_{\omega \in V} \mathrm{P}(\omega) \;=\; \sum_{i=1}^{s} \sum_{\omega \in A_i} \mathrm{P}(\omega) \;=\; \sum_{i=1}^{s} \mathrm{P}(A_i)\,.$$

Somit gilt für paarweise disjunkte Mengen $A_1, \ldots, A_s \subseteq \Omega$:

$$\mathrm{P}(A_1 \cup \cdots \cup A_s) \;=\; \mathrm{P}(A_1) + \cdots + \mathrm{P}(A_s)\,.$$

□

Folie 266

Aus den in Bemerkung 5.5 bewiesenen Rechenregeln ergibt sich insbesondere, dass die Abbildung P eines endlichen Wahrscheinlichkeitsraums (Ω, P) eine *Wahrscheinlichkeitsverteilung* im Folgenden Sinne ergibt (wobei wir beachten, dass $\mathrm{P}(\{\omega\}) = \mathrm{P}(\omega)$ ist).

Definition 5.6. Sei Ω eine nicht-leere Menge. Eine *Wahrscheinlichkeitsverteilung* (auch: ein *Wahrscheinlichkeitsmaß*) für Ω ist eine Abbildung[2] $\mathrm{P} : \mathcal{P}(\Omega) \to [0, 1]$, die die folgenden Eigenschaften besitzt:

1. $\mathrm{P}(\Omega) = 1$.
2. Für alle $A \subseteq \Omega$ gilt: $\mathrm{P}(A) \geqslant 0$.
3. Für alle $A, B \subseteq \Omega$ mit $A \cap B = \emptyset$ gilt: $\mathrm{P}(A \cup B) = \mathrm{P}(A) + \mathrm{P}(B)$.

Gleichverteilung und Laplacescher Wahrscheinlichkeitsraum

Definition 5.7. Sei Ω eine endliche nicht-leere Menge.
Die *Gleichverteilung* auf Ω ist der endliche Wahrscheinlichkeitsraum (Ω, P), bei dem P wie folgt definiert ist: Für jedes $\omega \in \Omega$ ist $\mathrm{P}(\omega) = \frac{1}{|\Omega|}$.
D.h.: Jedes Elementarereignis tritt mit derselben Wahrscheinlichkeit auf.

Dieser Wahrscheinlichkeitsraum (Ω, P) wird auch *Laplacescher Wahrscheinlichkeitsraum* genannt.

Ist (Ω, P) der Laplacesche Wahrscheinlichkeitsraum, so gilt für jedes Ereignis $A \subseteq \Omega$: $\mathrm{P}(A) = \frac{|A|}{|\Omega|}$.

Beispiel: Der in Beispiel 5.2 betrachtete Wahrscheinlichkeitsraum ist ein Laplacescher Wahrscheinlichkeitsraum.

Vorsicht beim „intuitiven“ Argumentieren mit Wahrscheinlichkeiten

Bei der Analyse eines Zufallsexperiments sollte man sich nicht nur auf die eigene Intuition verlassen, sondern — um sicherzugehen, dass bei der Analyse kein Unsinn verzapft wird — auch die mathematische Definition der Wahrscheinlichkeiten benutzen. Oft ist die folgende *3-Schritt-Methode* hilfreich:

1. *Finde den richtigen Wahrscheinlichkeitsraum:*

   Bestimme alle möglichen Ergebnisse des Zufallsexperiments und deren Wahrscheinlichkeiten. D.h.: Bestimme die Menge Ω der Elementarereignisse und die Wahrscheinlichkeit $\mathrm{P}(\omega)$ für jedes $\omega \in \Omega$.

2. *Bestimme die relevanten Ereignisse:*

   Für welche konkreten Ereignisse $A \subseteq \Omega$ wollen wir wissen, mit welcher Wahrscheinlichkeit sie auftreten?

3. *Berechne die Wahrscheinlichkeiten der relevanten Ereignisse:*

   Für jedes Ereignis $A \subseteq \Omega$ gilt: $\mathrm{P}(A) = \sum_{\omega \in A} \mathrm{P}(\omega)$.

Beispiel: Diese Methode haben wir in Beispiel 5.4 angewendet um die Wahrscheinlichkeit dafür auszurechnen, dass bei zwei hintereinander ausgeführten Münzwürfen mindestens einmal die Münze auf „Kopf“ landet.

Folie 269

Beispiel 5.8. Wir nutzen einen „fairen“ Würfel, d.h. bei jedem Wurf des Würfels erhalten wir eine der Zahlen $1, 2, 3, 4, 5, 6$ als Ergebnis; und zwar jede dieser Zahlen mit der gleichen Wahrscheinlichkeit $\frac{1}{6}$.

Wir führen folgendes Zufallsexperiment aus: Wir würfeln zwei mal hintereinander.

Fragen:

(a) Wie groß ist die Wahrscheinlichkeit dafür, dass die Summe der in beiden Würfen erzielten Ergebnisse größer als 10 ist?

(b) Wie groß ist die Wahrscheinlichkeit dafür, dass die zweite gewürfelte Zahl größer als die erste ist?

Um diese beiden Fragen zu beantworten, nutzen wir die oben beschriebene 3-Schritt-Methode.

Folie 270

Schritt 1: Finde den richtigen Wahrscheinlichkeitsraum:

Jedes Tupel $(i, j) \in [6] \times [6]$ repräsentiert einen Ausgang des Zufallsexperiments — nämlich dass der erste Wurf die Zahl i und der zweite Wurf die Zahl j ergeben hat. Daher wählen wir die folgende Menge Ω von Elementarereignissen: $\Omega := [6] \times [6] = \{\, (i, j) \,:\, i \in [6],\ j \in [6] \,\}$.

Da jedes dieser Elementarereignisse mit derselben Wahrscheinlichkeit $\frac{1}{36}$ auftritt, wählen wir $\mathrm{P}(\omega) = \frac{1}{36}$ für jedes $\omega \in \Omega$. Somit haben wir einen Laplaceschen Wahrscheinlichkeitsraum, d.h. eine Gleichverteilung auf Ω, mit $|\Omega| = 36$.

Folie 271

Schritt 2: Bestimme die relevanten Ereignisse:

Bei Frage (a) wollen wir wissen: Wie groß ist die Wahrscheinlichkeit dafür, dass die Summe der in beiden Würfen erzielten Ergebnisse größer als 10 ist?

D.h. wir interessieren uns für das Ereignis A, das aus allen Elementarereignissen $(i, j) \in \Omega$ besteht, für die gilt: $i + j > 10$.
Sei also $A := \{\, (i, j) \in \Omega \,:\, i + j > 10 \,\}$. Offensichtlicherweise gilt:
$A = \{\, (5, 6),\ (6, 5),\ (6, 6) \,\}$.

Bei Frage (b) wollen wir wissen: Wie groß ist die Wahrscheinlichkeit dafür, dass die zweite gewürfelte Zahl größer als die erste ist?

[2] Wir schreiben $[0, 1]$ um die Menge aller reellen Zahlen r mit $0 \leqslant r \leqslant 1$ zu bezeichnen.

D.h. wir interessieren uns für das Ereignis B, das aus allen Elementarereignissen $(i,j) \in \Omega$ besteht, für die gilt: $i < j$.
Sei also $B := \{\, (i,j) \in \Omega \,:\, i < j \,\}$.

Folie 272

Schritt 3: Berechne die Wahrscheinlichkeiten der Ereignisse A und B:

Da (Ω, P) ein Laplacescher Wahrscheinlichkeitsraum mit $|\Omega| = 36$ ist, gilt für jedes Ereignis $C \subseteq \Omega$: $\mathrm{P}(C) = \frac{|C|}{36}$.

Insbesondere gilt für $A = \{\, (5,6),\ (6,5),\ (6,6) \,\}$, dass $|A| = 3$ ist. Somit ist $\mathrm{P}(A) = \frac{3}{36} = \frac{1}{12}$. Die Antwort auf Frage (a) lautet also: „Die Wahrscheinlichkeit dafür, dass die Summe der in beiden Würfen erzielten Augenzahlen größer als 10 ist, ist genau $\frac{1}{12}$.“

Folie 273

Für $B = \{\, (i,j) \in \Omega \,:\, i < j \,\}$ gilt: $\mathrm{P}(B) = \frac{|B|}{36}$. Aber wie können wir $|B|$ ausrechnen, ohne langwierig alle Tupel in B hinschreiben zu müssen? Durch geschicktes Abzählen!

Für jedes $i \in [6]$ sei X_i die Menge aller $j \in [6]$ mit $j > i$, d.h. $j \geqslant i{+}1$. Offensichtlicherweise ist $|X_i| = 6{-}i$ (von den 6 Elementen in $[6]$ gehören die ersten i nicht zu X_i, während die restlichen $6{-}i$ Elemente zu X_i dazugehören).
B ist dann die Vereinigung der Mengen $B_i := \{i\} \times X_i$ für jedes $i \in [6]$. Da diese Mengen paarweise disjunkt sind gilt:[3]

$$|B| = \sum_{i=1}^{6} |\{i\}{\times}X_i| = \sum_{i=1}^{6} |X_i| = \sum_{i=1}^{6} (6{-}i) = \sum_{k=0}^{5} k = \tfrac{5\cdot(5+1)}{2} = \tfrac{30}{2} = 15\,.$$

Somit ist $\mathrm{P}(B) = \frac{|B|}{36} = \frac{15}{36} = \frac{5}{12}$. Die Antwort auf Frage (b) lautet also: „Die Wahrscheinlichkeit dafür, dass die zweite gewürfelte Zahl größer als die erste ist, ist genau $\frac{5}{12}$.“

Folie 274

Das Geburtstagsproblem

Beispiel 5.9. Beim *Geburtstagsproblem* (auch bekannt unter dem Begriff *Geburtstagsparadoxon*) geht es um die folgende Situation.

In einem Raum befinden sich k Personen.

[3] Wir wenden hier die Gaußsche Summenformel an: $\sum_{k=0}^{n} = \frac{n(n+1)}{2}$, siehe Satz 2.44.

Frage: Wie groß ist die Wahrscheinlichkeit dafür, dass es darunter zwei Personen gibt, die am gleichen Tag Geburtstag[4] haben?

Verblüffende Antwort: Schon bei nur $k = 25$ Personen ist die Wahrscheinlichkeit, dass zwei davon am gleichen Tag Geburtstag haben, größer als $\frac{1}{2}$. Und bei $k = 50$ Personen ist sie größer als 0,96.

Dies lässt sich wie folgt errechnen. Wir wenden die 3-Schritt-Methode an.

Erfahrungsbericht: Am 23.01.2023 wurde dieses Zufallsexperiment unter den Teilnehmer:innen der Veranstaltung „Diskrete Strukturen“ durchgeführt. Am Experiment nahmen insgesamt 58 Personen teil. *Ergebnis:* Es gab einen Tag, an dem 3 Personen Geburtstag haben und zwei weitere Tage, an denen je 2 Personen Geburtstag haben.

Folie 275

Schritt 1: Finde den richtigen Wahrscheinlichkeitsraum

Wir machen die folgenden vereinfachenden Annahmen (die nicht unbedingt exakt der Realität entsprechen):

- Niemand ist in einem Schaltjahr geboren; somit gibt es genau 365 Möglichkeiten dafür, an welchem Tag jemand Geburtstag hat.
- Geburtstage sind über die 365 Tage des Jahres gleichverteilt.

Wir nummerieren die k Personen durch mit den Zahlen $1, \ldots, k$, und wir nummerieren die 365 denkbaren Geburtstage durch mit den Zahlen $1, \ldots, 365$. Als Wahrscheinlichkeitsraum wählen wir

$$\Omega \;:=\; \{\, (a_1, \ldots, a_k) \,:\, a_1, \ldots, a_k \in \{1, \ldots, 365\} \,\} \;=\; \{1, \ldots, 365\}^k$$

Hierbei steht „a_i“ dafür, dass Person i am Tag a_i Geburtstag hat.

Entsprechend der oben beschriebenen Annahmen gehen wir davon aus, dass wir eine Gleichverteilung auf Ω haben,d.h. jedes Elementarereignis $\omega \in \Omega$ hat die Wahrscheinlichkeit

$$\mathrm{P}(\omega) \;=\; \frac{1}{|\Omega|} \;=\; \frac{1}{365^k}\,.$$

Schritt 2: Finde die relevanten Ereignisse

Wir interessieren uns für das Ereignis, bei dem mindestens zwei der k Personen am gleichen Tag Geburtstag haben, d.h., für das Ereignis

$$A \;:=\; \{\, (a_1, \ldots, a_k) \in \Omega \;:\; \text{es gibt } i, j \in [k] \text{ mit } i \neq j \text{ und } a_i = a_j \,\}$$

Schritt 3: Berechne die Wahrscheinlichkeit des Ereignisses A

Wir wissen: $\mathrm{P}(A) = \frac{|A|}{|\Omega|} = \frac{|A|}{365^k}$

Aber wie können wir $|A|$ ausrechnen?
Idee: Wir berechnen stattdessen $\mathrm{P}(\bar{A})$ und nutzen die Gleichung $\mathrm{P}(A) = 1 - \mathrm{P}(\bar{A})$.

Es gilt:

$$\begin{aligned}
\bar{A} &= \Omega \setminus A \\
&= \{(a_1, \ldots, a_k) \in \Omega \quad : a_1, \ldots, a_k \text{ sind paarweise verschieden}\} \\
&= \{(a_1, \ldots, a_k) \in [n]^k \;: a_1, \ldots, a_k \text{ sind paarweise verschieden}\}
\end{aligned}$$

für $n := 365$. Aus Kapitel 4, Gleichung (4.2) wissen wir, dass Folgendes gilt:

$$\left|\bar{A}\right| \;=\; (n)_k \;=\; n \cdot (n{-}1) \cdot (n{-}2) \cdots (n{-}k{+}1)$$

Also gilt:

$$\mathrm{P}(\bar{A}) \;=\; \frac{\left|\bar{A}\right|}{|\Omega|} \;=\; \frac{(n)_k}{n^k} \;=\; \prod_{i=0}^{k-1} \frac{n-i}{n} \;=\; \prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right)$$

Um dies zu vereinfachen, nutzen wir die Abschätzung (4.8), die besagt:

$$\text{Für alle } x \in \mathbb{R} \text{ ist } \; 1 + x \leqslant e^x \,.$$

Für $x := -\frac{i}{n}$ liefert dies: $(1 - \frac{i}{n}) \leqslant e^{-\frac{i}{n}}$. Somit ist

$$\mathrm{P}(\bar{A}) \;\leqslant\; \prod_{i=1}^{k-1} e^{-\frac{i}{n}} \;=\; e^{\sum_{i=1}^{k-1} -\frac{i}{n}} \,.$$

[4] ohne Berücksichtigung des Geburtsjahrs

Unter Verwendung der Gaußschen Summenformel erhalten wir:

$$\sum_{i=1}^{k-1} -\frac{i}{n} \;=\; -\frac{1}{n} \cdot \sum_{i=1}^{k-1} i \;=\; -\frac{1}{n} \cdot \frac{(k-1)\cdot k}{2} \;=\; -\frac{(k-1)\cdot k}{2n}\,.$$

Also ist

$$\mathrm{P}(\bar{A}) \;\leqslant\; e^{-\frac{(k-1)\cdot k}{2n}} \qquad \text{und} \qquad \mathrm{P}(A) \;=\; 1 - \mathrm{P}(\bar{A}) \;\geqslant\; 1 - e^{-\frac{(k-1)\cdot k}{2n}}\,. \quad (5.5)$$

Durch Einsetzen von $n = 365$ erhalten wir:

$$\mathrm{P}(A) \;\geqslant\; 1 - e^{-\frac{(k-1)\cdot k}{730}}\,.$$

Ausrechnen mit dem Taschenrechner liefert für $k = 25$ Personen:

$$\mathrm{P}(A) \;\geqslant\; 1 - e^{\frac{-600}{730}} \;\geqslant\; 1 - 0{,}43958 \;\geqslant\; 0{,}56\,.$$

Für $n = 30$ erhalten wir:

$$\mathrm{P}(A) \;\geqslant\; 1 - e^{\frac{-870}{730}} \;\geqslant\; 1 - 0{,}30368 \;\geqslant\; 0{,}7\,.$$

Und für $n = 50$ erhalten wir:

$$\mathrm{P}(A) \;\geqslant\; 1 - e^{\frac{-2450}{730}} \;\geqslant\; 1 - 0{,}03486 \;\geqslant\; 0{,}96\,.$$

Folie 277

Bezug zur Informatik: Kollisionen beim Hashing

Um schnellen Zugriff auf einzelne Daten zu haben, verwendet man beim Programmieren gerne *Hashtabellen* bzw. *Hashfunktionen*.
Dabei werden einzelne Datensätze, die aus einer großen Menge D stammen können, auf „Schlüssel“ aus einer (i.d.R. kleineren) Menge $S = \{1, \ldots, n\}$ (mit $n \in \mathbb{N}_{\geqslant 1}$) abgebildet.
Eine Hashfunktion ist eine Funktion $h : D \to S$, so dass man bei Eingabe eines Datenelements $d \in D$ den „Hashwert“ $h(d)$ schnell berechnen kann.
Informationen über die verfügbaren Datenwerte werden in einem Array $A[1 \ldots n]$ abgespeichert — und zwar für den Datenwert d im Array-Eintrag $A(h(d))$.
Wenn man auf die für d gespeicherten Informationen zugreifen will, berechnet man einfach schnell den Hashwert $i := h(d)$ und schaut dann im Array-Eintrag $A(i)$ nach. Problematisch dabei sind *Kollisionen* — also wenn mehrere verschiedene Datenwerte auf denselben Hashwert i abgebildet werden. Dann speichert man im Array-Eintrag i.d.R. eine Liste

aller entsprechenden Datenwerte ab, die man dann wieder mühsam durchsuchen muss.
Das „Geburtstagsproblem“ zeigt, dass Kollisionen mit recht großer Wahrscheinlichkeit auftreten können. Für die Situation, in der wir n Schlüssel zur Verfügung haben und insgesamt k Datenwerte gespeichert werden, gibt uns Gleichung (5.5) die Wahrscheinlichkeit dafür an, dass es Kollisionen gibt.
Beachte: Schon bei $k \approx \sqrt{n}$ ist diese Wahrscheinlichkeit recht groß.

5.2 Zufallsvariablen

Folie 278

Definition 5.10 (Zufallsvariable)**.**
Sei (Ω, P) ein endlicher Wahrscheinlichkeitsraum.
Eine *Zufallsvariable* ist eine Funktion

$$X : \Omega \to \mathbb{R}\,.$$

Für jede Zahl $r \in \mathbb{R}$ definieren wir die Wahrscheinlichkeit dafür, dass die Zufallsvariable X den Wert r annimmt, durch

$$\mathrm{P}(X = r) \;:=\; \mathrm{P}(A) \quad \text{für das Ereignis} \quad A := \{\omega \in \Omega \,:\, X(\omega) = r\}.$$

Folie 279

Beispiel 5.11 (Münzwürfe und Zufallsvariablen)**.**
Für eine beliebige, feste Zahl $p \in [0, 1]$ haben wir eine Münze zur Verfügung, die mit Wahrscheinlichkeit p auf „Kopf“ und mit Wahrscheinlichkeit $1 - p$ auf „Zahl“ fällt. Für eine feste Zahl $s \in \mathbb{N}_{\geqslant 1}$ werfen wir s-mal hintereinander die Münze.

Formal gesehen, betrachten also den Wahrscheinlichkeitsraum (Ω, P), dessen Elementarereignisse Worte der Länge s über dem Alphabet $\{K, Z\}$ sind, d.h. $\Omega = \{K, Z\}^s$.
Jedes Elementarereignis $\omega = \omega_1 \cdots \omega_s \in \Omega$ tritt mit Wahrscheinlichkeit $\mathrm{P}(\omega) := p^k(1-p)^{s-k}$ ein, wobei k die Anzahl der Vorkommen des Buchstabens K im Wort ω ist.

Folie 280

Für jeden Münzwurf $i \in \{1, \ldots, s\}$ betrachten wir die Zufallsvariable X_i, der wir den Wert 1 zuordnen, falls die Münze im i-ten Wurf auf „Kopf“ gelandet ist, und der wir den Wert 0 zuordnen, falls die Münze im i-ten Wurf auf „Zahl“ gelandet ist. Wir schreiben dafür kurz

$$X_i \;:=\; \begin{cases} 1 & \text{falls die Münze im } i\text{-ten Wurf auf „Kopf“ landet} \\ 0 & \text{sonst} \end{cases}$$

und meinen damit die Zufallsvariable $X_i : \Omega \to \mathbb{R}$, bei der für jedes Elementarereignis $\omega \in \Omega$ gilt:

$$X_i(\omega) \;=\; \begin{cases} 1 & \text{falls an der } i\text{-ten Position des Worts } \omega \\ & \text{der Buchstabe } K \text{ steht} \\ 0 & \text{sonst.} \end{cases}$$

Offensichtlicherweise gilt für jedes $i \in \{1, \ldots, s\}$, dass

$$\mathrm{P}(X_i = 1) \;=\; p \qquad \text{und} \qquad \mathrm{P}(X_i = 0) \;=\; 1 - p\,.$$

Folie 281

Zusätzlich zu den Zufallsvariablen $X_1, \ldots, X_s$ betrachten wir noch eine weitere Zufallsvariable X, die angeben soll, bei wie vielen der s Münzwürfe die Münze auf „Kopf“ gelandet ist. Wir schreiben dazu kurz

$$X \;:=\; \sum_{i=1}^{s} X_i$$

und meinen damit die Zufallsvariable $X : \Omega \to \mathbb{R}$, bei der für jedes Elementarereignis $\omega \in \Omega$ gilt:[5]

$$X(\omega) \;=\; \sum_{i=1}^{s} X_i(\omega).$$

Man kann sich leicht davon überzeugen, dass für jedes $k \in \{0, \ldots, s\}$ gilt:

$$\mathrm{P}(X = k) \;=\; \binom{s}{k}\, p^k\, (1-p)^{s-k}.$$

Dieser Wert gibt die Wahrscheinlichkeit dafür an, dass bei den s Münzwürfen die Münze insgesamt genau k-mal auf „Kopf“ landet.

5.3 Erwartungswert

Sei (Ω, P) ein endlicher Wahrscheinlichkeitsraum und sei $X : \Omega \to \mathbb{R}$ eine Zufallsvariable. Da Ω endlich ist, ist auch das *Bild* von Ω unter X, d.h. die Menge $\mathrm{Bild}(X) := \{X(\omega) : \omega \in \Omega\}$ endlich.

Definition 5.12 (Erwartungswert einer Zufallsvariablen)**.**
Sei (Ω, P) ein endlicher Wahrscheinlichkeitsraum und sei $X : \Omega \to \mathbb{R}$ eine Zufallsvariable. Der *Erwartungswert* der Zufallsvariablen X ist definiert als

$$\mathrm{E}(X) \quad := \quad \sum_{r \in \mathrm{Bild}(X)} r \cdot \mathrm{P}(X = r).$$

Anschaulich ist der Erwartungswert der „zu erwartende“ Wert, den wir erhalten, wenn wir das Zufallsexperiment sehr oft wiederholen und den Durchschnitt der dabei für X erhaltenen Werte berechnen.

Man kann sich leicht davon überzeugen, dass Folgendes gilt:

$$\mathrm{E}(X) \quad = \quad \sum_{\omega \in \Omega} X(\omega) \cdot \mathrm{P}(\omega)\,. \tag{5.6}$$

Beweis. Es gilt:

$$\begin{aligned}
\mathrm{E}(X) &= \sum_{r \in \mathrm{Bild}(X)} r \cdot \mathrm{P}(X = r) \\
&= \sum_{r \in \mathrm{Bild}(X)} r \cdot \mathrm{P}(\{\omega \in \Omega : X(\omega) = r\}) \\
&= \sum_{r \in \mathrm{Bild}(X)} r \cdot \left(\sum_{\substack{\omega \in \Omega: \\ X(\omega) = r}} \mathrm{P}(\omega) \right) \\
&= \sum_{r \in \mathrm{Bild}(X)} \sum_{\substack{\omega \in \Omega: \\ X(\omega) = r}} X(\omega) \cdot \mathrm{P}(\omega) \\
&= \sum_{\omega \in \Omega} X(\omega) \cdot \mathrm{P}(\omega)\,.
\end{aligned}$$

□

Folie 283

Beispiel 5.13 (Erwartungswert beim Würfeln)**.**
Wir werfen einen herkömmlichen Würfel, d.h. einen Würfel, der 6 Seiten besitzt, die mit den Augenzahlen 1 bis 6 durchnummeriert sind, und bei dem jede Augenzahl mit der selben Wahrscheinlichkeit gewürfelt wird. Sei X die Zufallsvariable, die die gewürfelte Augenzahl beschreibt. Der Erwartungswert von X ist

$$\mathrm{E}(X) \quad = \quad \sum_{i=1}^{6} i \cdot \mathrm{P}(X=i) \quad = \quad \sum_{i=1}^{6} i \cdot \tfrac{1}{6} \quad = \quad \tfrac{1}{6} \cdot \tfrac{6 \cdot 7}{2} \quad = \quad \tfrac{7}{2} \quad = \quad 3{,}5\,.$$

Folie 284

Man beachte, dass die Zufallsvariable X^2 das Quadrat der gewürfelten Augenzahl beschreibt. Der Erwartungswert von X^2 ist

$$\mathrm{E}(X^2) = \sum_{i=1}^{6} i^2 \cdot \mathrm{P}(X^2 = i^2) = \sum_{i=1}^{6} i^2 \cdot \mathrm{P}(X=i) = \tfrac{1}{6} \cdot \sum_{i=1}^{6} i^2 = \tfrac{91}{6} = 15{,}1666\cdots\,.$$

Insbesondere ist hier

$$\mathrm{E}(X^2) \quad \neq \quad \mathrm{E}(X)^2,$$

da $\mathrm{E}(X)^2 = (3{,}5)^2 = 12{,}25$ ist.

Folie 285

Linearität des Erwartungswerts

Bemerkung 5.14 (*Linearität des Erwartungswerts*)**.**
Man kann sich leicht davon überzeugen, dass für jeden endlichen Wahrscheinlichkeitsraum (Ω, P), für alle Zufallsvariablen X und Y und für alle Zahlen $a \in \mathbb{R}$ gilt:

$$\mathrm{E}(aX) \quad = \quad a \cdot \mathrm{E}(X) \qquad \text{und} \qquad \mathrm{E}(X+Y) \quad = \quad \mathrm{E}(X) + \mathrm{E}(Y)\,.$$

Daraus folgt, dass für alle $s \in \mathbb{N}_{\geqslant 1}$, alle Zufallsvariablen $X_1, \ldots, X_s$ und alle Zahlen $a_1, \ldots, a_s \in \mathbb{R}$ gilt:

$$\mathrm{E}\left(\sum_{i=1}^{s} a_i X_i \right) \quad = \quad \sum_{i=1}^{s} a_i \cdot \mathrm{E}(X_i)\,.$$

[5] *Zur Erinnerung:* Der Binomialkoeffizient $\binom{n}{k}$ gibt an, wie viele verschiedene k-elementige Teilmengen eine n-elementige Menge besitzt. Es gilt: $\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$.

Beweis. Wir nutzen (5.6). Daraus folgt:

$$\begin{aligned} a \cdot \mathrm{E}(X) &= a \cdot \sum_{\omega\in\Omega} X(\omega) \cdot \mathrm{P}(\omega) \\ &= \sum_{\omega\in\Omega} a \cdot X(\omega) \cdot \mathrm{P}(\omega) \\ &= \sum_{\omega\in\Omega} (aX)(\omega) \cdot \mathrm{P}(\omega) \\ &= \mathrm{E}(aX)\,. \end{aligned}$$

Des Weiteren gilt:

$$\begin{aligned} \mathrm{E}(X) + \mathrm{E}(Y) &= \left(\sum_{\omega\in\Omega} X(\omega) \cdot \mathrm{P}(\omega)\right) + \left(\sum_{\omega\in\Omega} Y(\omega) \cdot \mathrm{P}(\omega)\right) \\ &= \sum_{\omega\in\Omega} \big(X(\omega) + Y(\omega)\big) \cdot \mathrm{P}(\omega) \\ &= \sum_{\omega\in\Omega} (X+Y)(\omega) \cdot \mathrm{P}(\omega) \\ &= \mathrm{E}(X+Y)\,. \end{aligned}$$

Es folgt:

$$\mathrm{E}\left(\sum_{i=1}^{s} a_i X_i\right) \;=\; \sum_{i=1}^{s} \mathrm{E}(a_i X_i) \;=\; \sum_{i=1}^{s} a_i\, \mathrm{E}(X_i)\,.$$

□

Folie 286

Beispiel 5.15 (Erwartungswert bei Münzwürfen)**.**
Wir betrachten wieder das Szenario aus Beispiel 5.11, bei dem für jedes $i \in \{1, \ldots, s\}$ die Zufallsvariable X_i angibt, ob die Münze beim i-ten Münzwurf auf „Kopf“ gelandet ist, und bei dem die Zufallsvariable $X := \sum_{i=1}^{s} X_i$ angibt, bei wie vielen der s Münzwürfe die Münze auf „Kopf“ gelandet ist. Für jedes $i \in \{1, \ldots, s\}$ hat X_i den Erwartungswert

$$\mathrm{E}(X_i) \;=\; 0 \cdot \mathrm{P}(X_i = 0) \;+\; 1 \cdot \mathrm{P}(X_i = 1) \;=\; \mathrm{P}(X_i = 1) \;=\; p.$$

Gemäß der Linearität des Erwartungswerts ist der Erwartungswert der Zufallsvariablen $X := \sum_{i=1}^{s} X_i$ daher der Wert

$$\mathrm{E}(X) \;=\; \sum_{i=1}^{s} \mathrm{E}(X_i) \;=\; p \cdot s.$$

Folie 287

Bemerkung 5.16. Die in Bemerkung 5.14 formulierte Linearität des Erwartungswerts besagt, dass Summen und konstante Vielfache aus der Bildung des Erwartungswerts herausgezogen werden können, so dass

$$\mathrm{E}\left(\sum_{i=1}^{s} a_i X_i\right) \quad = \quad \sum_{i=1}^{s} a_i \cdot \mathrm{E}(X_i).$$

Im Gegensatz dazu dürfen wir Produkte i.d.R. nicht einfach aus der Bildung des Erwartungswerts herausziehen. Beispielsweise haben wir in Beispiel 5.13 eine Situation kennen gelernt, in der gilt:

$$\mathrm{E}(X \cdot X) \quad \neq \quad \mathrm{E}(X) \cdot \mathrm{E}(X)\,.$$

5.4 Varianz

Folie 288

Die *Varianz* ist ein Maß dafür, wie weit die tatsächlichen Werte einer Zufallsvariablen X vom Erwartungswert $\mathrm{E}(X)$ abweichen.

Definition 5.17 (Varianz einer Zufallsvariablen)**.**
Sei (Ω, P) ein endlicher Wahrscheinlichkeitsraum und sei $X : \Omega \to \mathbb{R}$ eine Zufallsvariable. Die *Varianz* der Zufallsvariablen X ist definiert als

$$\mathrm{Var}(X) \quad := \quad \mathrm{E}\Big(\big(X - \mathrm{E}(X)\big)^2\Big).$$

Somit ist die Varianz einer Zufallsvariablen X definiert als der Erwartungswert des Quadrats der Abweichung von X zum Erwartungswert von X. Anschaulich ist die Varianz von X also der „zu erwartende“ Wert, den wir erhalten, wenn wir das Zufallsexperiment sehr oft wiederholen, jeweils die Abweichung des für X erzielten Werts vom Erwartungswert $\mathrm{E}(X)$ berechnen, und den Durchschnitt der Quadrate dieser Abweichungen berechnen.

Folie 289

Regeln zum Rechnen mit Varianzen

Bemerkung 5.18 (Regeln zum Rechnen mit Varianzen)**.**
Für jede Zufallsvariable X über einem endlichen Wahrscheinlichkeitsraum (Ω, P) und für alle Zahlen $a, b \in \mathbb{R}$ gilt:

$$\mathrm{Var}(X) \quad = \quad \mathrm{E}(X^2) - \mathrm{E}(X)^2 \qquad \text{und} \qquad \mathrm{Var}(aX + b) \quad = \quad a^2 \cdot \mathrm{Var}(X).$$

Beweis. Es gilt:

$$\begin{aligned}
\mathrm{Var}(X) &\overset{\text{Def.}}{=} \mathrm{E}\Big((X-\mathrm{E}(X))^2\Big) \\
&= \mathrm{E}\Big(X^2 - 2\cdot\mathrm{E}(X)\cdot X + \mathrm{E}(X)^2\Big) \\
&\overset{\text{Linearität}}{=} \mathrm{E}(X^2) - 2\,\mathrm{E}(X)\cdot\mathrm{E}(X) + \mathrm{E}(X)^2\cdot\mathrm{E}(1) \\
&\overset{\mathrm{E}(1)=1}{=} \mathrm{E}(X^2) - \mathrm{E}(X)^2.
\end{aligned}$$

Unter Verwendung dieser Gleichung erhalten wir:

$$\begin{aligned}
\mathrm{Var}(aX) &= \mathrm{E}((aX)^2) - \mathrm{E}(aX)^2 \\
&\overset{\text{Linearität}}{=} \mathrm{E}(a^2\cdot X^2) - \big(a\cdot\mathrm{E}(X)\big)^2 \\
&\overset{\text{Linearität}}{=} a^2\cdot\mathrm{E}(X^2) - a^2\cdot\mathrm{E}(X)^2 \\
&= a^2\cdot\Big(\mathrm{E}(X^2) - \mathrm{E}(X)^2\Big) \\
&= a^2\cdot\mathrm{Var}(X).
\end{aligned}$$

Außerdem gilt für jede Zufallsvariable Y:

$$\begin{aligned}
\mathrm{Var}(Y+b) &= \mathrm{E}\Big(\big(Y+b-\underbrace{\mathrm{E}(Y+b)}_{\overset{\text{Linearität}}{=}\,\mathrm{E}(Y)+b}\big)^2\Big) \\
&= \mathrm{E}\Big(\big(Y-\mathrm{E}(Y)\big)^2\Big) \\
&= \mathrm{Var}(Y).
\end{aligned}$$

Insgesamt erhalten wir daher für die Zufallsvariable $Y := aX$, dass

$$\mathrm{Var}(aX+b) \;=\; \mathrm{Var}(aX) \;=\; a^2\cdot\mathrm{Var}(X).$$

□

Folie 290

Beispiel 5.19 (Varianz beim Würfeln)**.**
Wir betrachten das Szenario aus Beispiel 5.13, bei dem die Zufallsvariable X die beim 1-maligen Werfen eines 6-seitigen Würfels erzielte Augenzahl angibt. Wir wissen bereits, dass der Erwartungswert $\mathrm{E}(X) = 3{,}5 = \frac{7}{2}$ ist, und dass der Erwartungswert $\mathrm{E}(X^2) = \frac{91}{6}$ ist.
Die Varianz von X ist der Wert

$$\mathrm{Var}(X) = \mathrm{E}(X^2) - \mathrm{E}(X)^2 = \tfrac{91}{6} - \big(\tfrac{7}{2}\big)^2 = \tfrac{91}{6} - \tfrac{49}{4}$$

$$= \tfrac{182-147}{12} \qquad = \tfrac{35}{12} \qquad = 2{,}916666\cdots .$$

Folie 291

Bemerkung 5.20 (Nicht-Linearität der Varianz)**.**
Anhand der Regel

$$\mathrm{Var}(aX + b) \quad = \quad a^2 \cdot \mathrm{Var}(X)$$

lässt sich leicht sehen, dass *die Varianz i.d.R. nicht linear ist*:
Beispielsweise erhalten wir für $a = 2$ und $b = 0$, dass

$$\mathrm{Var}(X + X) \quad = \quad 4 \cdot \mathrm{Var}(X) \quad \neq \quad \mathrm{Var}(X) + \mathrm{Var}(X),$$

falls $\mathrm{Var}(X) \neq 0$.

5.5 Schranken

Folie 292

In diesem Abschnitt stellen wir zwei Werkzeuge bereit, mit deren Hilfe wir abschätzen können, mit welcher Wahrscheinlichkeit, der Wert einer Zufallsvariablen X „weit“ vom Erwartungswert $\mathrm{E}(X)$ abweicht.

Folie 293

Die Markov-Ungleichung

Satz 5.21 (Markov[6]-Ungleichung)**.**
Sei (Ω, P) *ein endlicher Wahrscheinlichkeitsraum und sei* $X : \Omega \to \mathbb{R}_{\geqslant 0}$ *eine Zufallsvariable, die nur Werte* $\geqslant 0$ *annehmen kann. Für jede reelle Zahl* $a > 0$ *gilt:*

$$\mathrm{P}(X \geqslant a) \quad \leqslant \quad \frac{\mathrm{E}(X)}{a}.$$

Beweis. Es gilt:

$$\begin{aligned} \mathrm{E}(X) &= \sum_{x \in \mathrm{Bild}(X)} x \cdot \mathrm{P}(X = x) \\ &\geqslant \sum_{\substack{x \in \mathrm{Bild}(X) \\ \text{mit} x \geqslant a}} a \cdot \mathrm{P}(X = x) \;=\; a \cdot \mathrm{P}(X \geqslant a). \end{aligned}$$

□

[6] In der Literatur werden unterschiedliche Schreibweisen verwendet, darunter Markov, Markow, Markoff.

Bemerkung 5.22. Aus der Markov-Ungleichung folgt direkt, dass

$$\mathrm{P}(X \geqslant c \cdot \mathrm{E}(X)) \quad \leqslant \quad \tfrac{1}{c}$$

für jede Zahl $c > 0$ gilt und für jede Zufallsvariable $X : \Omega \to \mathbb{R}_{\geqslant 0}$, die nur Werte $\geqslant 0$ annehmen kann und deren Erwartungswert > 0 ist.

Folie 294

Ein Beispiel zur Anwendung der Markov-Ungleichung

Bemerkung 5.23. *Randomisiertes Quicksort* ist die Variante des Sortieralgorithmus *Quicksort*, bei der in jedem einzelnen Schritt das Pivotelement *zufällig* und gleichverteilt aus den prinzipiell denkbaren Pivotelementen gezogen wird.

Eine detaillierte Laufzeitanalyse zeigt, dass die *erwartete Laufzeit* von randomisiertem Quicksort bei Eingabe einer zu sortierenden Liste der Länge n von der Form $c \cdot n \cdot \log_2(n)$ ist, für eine geeignete Konstante c.

Aus der Markov-Ungleichung folgt, dass die Wahrscheinlichkeit, das Pech zu haben, bei einem konkreten Lauf von randomisiertem Quicksort eine Laufzeit von $\geqslant 10 \cdot c \cdot n \cdot \log_2(n)$ (also dem 10-fachen der erwarteten Laufzeit) zu erwischen, höchstens $\frac{1}{10}$ ist.

Folie 295

Die Tschebyscheff-Ungleichung

Satz 5.24 (Tschebyscheff[7]-Ungleichung)**.**
Für jeden endlichen Wahrscheinlichkeitsraum (Ω, P)*, für jede Zufallsvariable* $X : \Omega \to \mathbb{R}$ *und für jede reelle Zahl* $a > 0$ *gilt:*

$$\mathrm{P}\Big(|X - \mathrm{E}(X)| \;\geqslant\; a\Big) \quad \leqslant \quad \frac{\mathrm{Var}(X)}{a^2}.$$

[7] In der Literatur werden unterschiedliche Schreibweisen verwendet, darunter Tschebyscheff, Tschebycheff, Tschebyschew, Chebychev und Tschebyschow.

Beweis. Wir betrachten die Zufallsvariable $Y := |X - \mathrm{E}(X)|$ und wenden die Markov-Ungleichung auf die Zufallsvariable Y^2 an. Wir erhalten:

$$\mathrm{P}(|X - \mathrm{E}(X)| \geqslant a) \quad = \quad \mathrm{P}(Y \geqslant a) \quad = \quad \mathrm{P}(Y^2 \geqslant a^2) \quad \overset{\text{Markov}}{\leqslant} \quad \frac{\mathrm{E}(Y^2)}{a^2}.$$

Hierbei gilt:

$$\mathrm{E}(Y^2) \quad = \quad \mathrm{E}((X - \mathrm{E}(X))^2) \quad \overset{\text{Def.}}{=} \quad \mathrm{Var}(X).$$

□

Ein Beispiel zur Anwendung der Tschebyscheff-Ungleichung behandeln wir in Abschnitt 5.7.

5.6 Paarweise Unabhängigkeit

Folie 296

Definition 5.25. Sei (Ω, P) ein endlicher Wahrscheinlichkeitsraum.

(a) Zwei Ereignisse A und B heißen (stochastisch) *unabhängig*, wenn gilt:

$$\mathrm{P}(A \cap B) \quad = \quad \mathrm{P}(A) \cdot \mathrm{P}(B).$$

Für jede Zahl $s \in \mathbb{N}_{\geqslant 1}$ heißen die Ereignisse $A_1, \ldots, A_s$ *paarweise unabhängig*, wenn für alle $i, j \in \{1, \ldots, s\}$ mit $i \neq j$ die Ereignisse A_i und A_j unabhängig voneinander sind.

(b) Zwei Zufallsvariablen X und Y heißen *unabhängig*, wenn für alle Werte $r, s \in \mathbb{R}$ gilt:

$$\mathrm{P}(X = r \text{ und } Y = s) \quad = \quad \mathrm{P}(X = r) \cdot \mathrm{P}(Y = s).$$

Für jede Zahl $s \in \mathbb{N}_{\geqslant 1}$ heißen die Zufallsvariablen $X_1, \ldots, X_s$ *paarweise unabhängig* (kurz: *pw. unabh.*), wenn für alle $i, j \in \{1, \ldots, s\}$ mit $i \neq j$ die Zufallsvariablen X_i und X_j unabhängig voneinander sind.

Folie 297

Vorsicht beim Begriff der (stochastischen) Unabhängigkeit

Bemerkung 5.26. Per Definition sind 2 Ereignisse A und B genau dann (stochastisch) unabhängig, wenn gilt: $\mathrm{P}(A \cap B) = \mathrm{P}(A) \cdot \mathrm{P}(B)$.

Falls (Ω, P) ein Laplacescher Wahrscheinlichkeitsraum ist, so wissen wir, dass Folgendes für alle Ereignisse A und B gilt:

- $\mathrm{P}(A \cap B) = \frac{|A \cap B|}{|\Omega|}$
- $\mathrm{P}(A) = \frac{|A|}{|\Omega|}$
- $\mathrm{P}(B) = \frac{|B|}{|\Omega|}$

Also sind die Ereignisse A und B genau dann (stochastisch) unabhängig, wenn gilt:

$$|A \cap B| \quad = \quad \frac{|A| \cdot |B|}{|\Omega|} \, .$$

Stochastische Unabhängigkeit hat *nichts* damit zu tun, ob die Ereignisse disjunkt sind oder nicht.
Beispiel: Ist $\mathrm{P}(A) > 0$ und $\mathrm{P}(B) > 0$ und $A \cap B = \emptyset$, so ist $\mathrm{P}(A \cap B) = 0 \neq \mathrm{P}(A) \cdot \mathrm{P}(B)$. Somit sind die Ereignisse A, B *nicht* unabhängig!

Folie 298

Beispiel 5.27.

(a) Wir betrachten das Szenario aus Beispiel 5.2, bei dem eine faire Münze zwei mal hintereinander geworfen wird.

Sei A_1 das Ereignis, dass die Münze beim ersten Wurf auf „Zahl“ landet, sei A_2 das Ereignis, dass die Münze beim zweiten Wurf auf „Kopf“ landet, und sei A_3 das Ereignis, dass die Münze bei beiden Münzwürfen auf der gleichen Seite landet. Also ist

$$A_1 = \{ZK,\ ZZ\} \ , \quad A_2 = \{KK,\ ZK\} \ , \quad A_3 = \{KK,\ ZZ\} \ ,$$

und es gilt

$$\mathrm{P}(A_1) = \tfrac{1}{2} \ , \qquad \mathrm{P}(A_2) = \tfrac{1}{2} \ , \qquad \mathrm{P}(A_3) = \tfrac{1}{2} \ .$$

Außerdem gilt

$$\begin{aligned} \mathrm{P}(A_1 \cap A_2) &= \mathrm{P}(\{ZK\}) = \tfrac{1}{4} = \mathrm{P}(A_1) \cdot \mathrm{P}(A_2). \\ \mathrm{P}(A_1 \cap A_3) &= \mathrm{P}(\{ZZ\}) = \tfrac{1}{4} = \mathrm{P}(A_1) \cdot \mathrm{P}(A_3). \\ \mathrm{P}(A_2 \cap A_3) &= \mathrm{P}(\{KK\}) = \tfrac{1}{4} = \mathrm{P}(A_2) \cdot \mathrm{P}(A_3). \end{aligned}$$

Daher sind die drei Ereignisse A_1, A_2, A_3 paarweise unabhängig.

Man beachte, dass trotz der paarweisen Unabhängigkeit die Ereignisse hier *nicht* paarweise disjunkt sind. Außerdem gilt hier

$$\mathrm{P}(A_1 \cap A_2 \cap A_3) \quad \neq \quad \mathrm{P}(A_1) \cdot \mathrm{P}(A_2) \cdot \mathrm{P}(A_3),$$

denn $A_1 \cap A_2 \cap A_3 = \emptyset$, d.h. die drei Ereignisse können nicht alle gleichermaßen eintreten, und daher ist $\mathrm{P}(A_1 \cap A_2 \cap A_3) = 0$, wohingegen $\mathrm{P}(A_1) \cdot \mathrm{P}(A_2) \cdot \mathrm{P}(A_3) = \frac{1}{8}$ ist.

(b) Entsprechend dem in Teil (a) betrachteten Szenario definieren wir die Zufallsvariablen Y_1, Y_2, Y_3 wie folgt:

$$Y_1 := \begin{cases} 1 & \text{falls die Münze beim 1. Wurf auf „Zahl“ landet} \\ 0 & \text{sonst} \end{cases}$$

$$Y_2 := \begin{cases} 1 & \text{falls die Münze beim 2. Wurf auf „Kopf“ landet} \\ 0 & \text{sonst} \end{cases}$$

$$Y_3 := \begin{cases} 1 & \text{falls die Münze bei beiden Würfen} \\ & \text{auf der gleichen Seite landet} \\ 0 & \text{sonst} \end{cases}$$

Somit gilt für jedes $i \in \{1, 2, 3\}$

$$\mathrm{P}(Y_i = 1) \;=\; \mathrm{P}(A_i) \;=\; \tfrac{1}{2} \qquad \text{und} \qquad \mathrm{P}(Y_i = 0) \;=\; \tfrac{1}{2}.$$

Man kann sich leicht davon überzeugen, dass die drei Zufallsvariablen Y_1, Y_2, Y_3 paarweise unabhängig sind.

Man beachte, dass trotz der paarweisen Unabhängigkeit die drei Zufallsvariablen nicht „vollständig unabhängig“ voneinander sind. Beispielsweise gilt

$$\mathrm{P}(Y_1 = 1 \text{ und } Y_2 = 1 \text{ und } Y_3 = 0) \;\neq\; \mathrm{P}(Y_1 = 1) \cdot \mathrm{P}(Y_2 = 1) \cdot \mathrm{P}(Y_3 = 0),$$

da $\mathrm{P}(Y_1 = 1 \text{ und } Y_2 = 1 \text{ und } Y_3 = 0) = \mathrm{P}(\{ZK\}) = \frac{1}{4}$ ist, wohingegen $\mathrm{P}(Y_1 = 1) \cdot \mathrm{P}(Y_2 = 1) \cdot \mathrm{P}(Y_3 = 0) = \frac{1}{8}$ ist.

Für *paarweise unabhängige* Zufallsvariablen gelten für Erwartungswert und Varianz noch die folgenden sehr nützlichen Regeln.

Satz 5.28 (Erwartungswert & Varianz von pw. unabh. Zufallsvariablen)**.** *Sei* (Ω, P) *ein endlicher Wahrscheinlichkeitsraum, sei* $s \in \mathbb{N}_{\geqslant 1}$ *und seien* $X_1, \ldots, X_s$ *paarweise unabhängige Zufallsvariablen. Dann gilt:*

$$\mathrm{E}(X_i \cdot X_j) \quad = \quad \mathrm{E}(X_i) \cdot \mathrm{E}(X_j)$$

für alle $i, j \in \{1, \ldots, s\}$ *mit* $i \neq j$*, und es gilt*

$$\mathrm{Var}\left(\sum_{i=1}^{s} X_i\right) \quad = \quad \sum_{i=1}^{s} \mathrm{Var}(X_i).$$

Beweis. Seien $i, j \in \{1, \ldots, s\}$ mit $i \neq j$. Wir setzen $Y := X_i$ und $Z := X_j$. Es gilt:

$$\begin{aligned} \mathrm{E}(Y) \cdot \mathrm{E}(Z) &= \left(\sum_{y \in \mathrm{Bild}(Y)} y \cdot \mathrm{P}(Y = y)\right) \cdot \left(\sum_{z \in \mathrm{Bild}(Z)} z \cdot \mathrm{P}(Z = z)\right) \\ &= \sum_{\substack{y \in \mathrm{Bild}(Y),\\ z \in \mathrm{Bild}(Z)}} y \cdot z \cdot \mathrm{P}(Y = y) \cdot \mathrm{P}(Z = z) \end{aligned}$$

Laut Voraussetzung sind Y und Z unabhängig, d.h. es gilt für alle Werte $y, z \in \mathbb{R}$, dass

$$\mathrm{P}(Y = y \text{ und } Z = z) \quad = \quad \mathrm{P}(Y = y) \cdot \mathrm{P}(Z = z).$$

Somit ist

$$\begin{aligned} \mathrm{E}(Y) \cdot \mathrm{E}(Z) &= \sum_{\substack{y \in \mathrm{Bild}(Y),\\ z \in \mathrm{Bild}(Z)}} y \cdot z \cdot \mathrm{P}(Y = y \text{ und } Z = z) \\ &= \sum_{x \in \mathrm{Bild}(YZ)} x \cdot \Big(\sum_{\substack{y \in \mathrm{Bild}(Y),\\ z \in \mathrm{Bild}(Z)\\ \text{mit } yz = x}} \mathrm{P}(Y = y \text{ und } Z = z) \Big) \\ &= \sum_{x \in \mathrm{Bild}(YZ)} x \cdot \mathrm{P}(YZ = x) \\ &= \mathrm{E}(YZ). \end{aligned}$$

Wir haben also gezeigt, dass für alle $i, j \in \{1, \ldots, s\}$ mit $i \neq j$ gilt:

$$\mathrm{E}(X_i \cdot X_j) \quad = \quad \mathrm{E}(X_i) \cdot \mathrm{E}(X_j).$$

Um zu zeigen, dass

$$\mathrm{Var}\left(\sum_{i=1}^{s} X_i\right) \quad = \quad \sum_{i=1}^{s} \mathrm{Var}(X_i)$$

ist, beachten wir, dass $\mathrm{Var}(Z) = \mathrm{E}(Z^2) - \mathrm{E}(Z)^2$ für jede Zufallsvariable Z gilt. Speziell für

$$Z \quad := \quad \sum_{i=1}^{s} X_i$$

ist

$$Z^2 \quad = \quad \sum_{i,j=1}^{s} X_i \cdot X_j \quad = \quad \sum_{i=1}^{s} (X_i)^2 \quad + \quad \sum_{\substack{i,j \in \{1,\ldots,s\} \\ \text{mit } i \neq j}} X_i \cdot X_j.$$

Auf Grund der Linearität des Erwartungswerts gilt daher:

$$\mathrm{E}(Z^2) \quad = \quad \sum_{i=1}^{s} \mathrm{E}({X_i}^2) \quad + \quad \sum_{\substack{i,j \in \{1,\ldots,s\} \\ \text{mit } i \neq j}} \mathrm{E}(X_i \cdot X_j). \tag{5.7}$$

Andererseits gilt auf Grund der Linearität des Erwartungswerts auch, dass $\mathrm{E}(Z) = \sum_{i=1}^{s} \mathrm{E}(X_i)$. Somit ist

$$\begin{aligned} \mathrm{E}(Z)^2 &= \sum_{i,j=1}^{s} \mathrm{E}(X_i) \cdot \mathrm{E}(X_j) \\ &= \sum_{i=1}^{s} \mathrm{E}(X_i)^2 \quad + \quad \sum_{\substack{i,j \in \{1,\ldots,s\} \\ \text{mit } i \neq j}} \mathrm{E}(X_i) \cdot \mathrm{E}(X_j). \end{aligned}$$

Die paarweise Unabhängigkeit der Zufallsvariablen $X_1, \ldots, X_s$ liefert uns, dass $\mathrm{E}(X_i \cdot X_j) = \mathrm{E}(X_i) \cdot \mathrm{E}(X_j)$ für alle $i, j \in \{1, \ldots, s\}$ mit $i \neq j$ gilt. Somit ist

$$\mathrm{E}(Z)^2 \quad = \quad \sum_{i=1}^{s} \mathrm{E}(X_i)^2 \quad + \quad \sum_{\substack{i,j \in \{1,\ldots,s\} \\ \text{mit } i \neq j}} \mathrm{E}(X_i \cdot X_j) \tag{5.8}$$

Aus den Gleichungen (5.7) und (5.8) erhalten wir, dass

$$\begin{aligned}
\mathrm{Var}(Z) &= \mathrm{E}(Z^2) - \mathrm{E}(Z)^2 \\
&= \sum_{i=1}^{s} \mathrm{E}({X_i}^2) \quad - \quad \sum_{i=1}^{s} \mathrm{E}(X_i)^2 \\
&= \sum_{i=1}^{s} \Big(\mathrm{E}({X_i}^2) - \mathrm{E}(X_i)^2 \Big) \\
&= \sum_{i=1}^{s} \mathrm{Var}(X_i).
\end{aligned}$$

□

5.7 Ein Beispiel zur Verwendung der Tschebyscheff-Ungleichung

Folie 300

Der Zufallssurfer

Suchmaschinen im Internet beruhen u.a. darauf, die von ihnen gefundene Liste der Ergebnisse auf eine eingegebene Suchanfrage möglichst gut nach ihrer „Relevanz“ zu sortieren, so dass die am besten geeigneten Treffer möglichst weit oben in der Liste der Suchergebnisse angezeigt werden.

Eine Grundlage des von Suchmaschinen verwendeten Verfahrens beruht auf dem Modell des *Zufallssurfers* (engl.: *Random Surfer*). Hierbei stellt man sich vor, dass die einzelnen Webseiten Knoten eines gerichteten Graphen sind, und dass ein Link, der von einer Webseite auf eine andere Webseite führt, einer gerichteten Kante entspricht.

Ein „zufällig vorgehender“ Web-Surfer beginnt auf einer beliebigen Webseite und klickt sich nach und nach durchs Internet, indem er jeweils einem zufällig ausgewählten Link folgt. Dies entspricht dem in der Stochastik seit vielen Jahrzehnten untersuchten Konzept der *Markov-Ketten*.

Als Maß für das „Renommee“ einer einzelnen Webseite nimmt man dann die Wahrscheinlichkeit, mit der der Zufallssurfer nach langem hin- und her-klicken auf dieser Webseite landet. Und dieses „Renommee“ ist einer der Bestandteile, die in die Sortierung der Suchergebnisse eingehen, um möglichst relevante Treffer möglichst weit oben in der Liste der Suchergebnisse anzuzeigen.

Die Analyse der Bewegungen des Zufallssurfers ist für die Veranstaltung „Diskrete Strukturen“ zu anspruchsvoll. Im folgenden Beispiel betrachten wir ein ähnliches, aber deutlich einfacheres Szenario.

Beispiel 5.29 (Der Frosch)**.**
In einem Teich befinden sich Steine in einer langen Reihe. Die Steine sind durchnummeriert mit $\ldots, -2, -1, 0, 1, 2, \ldots$
Ein Frosch sitzt anfänglich auf Stein 0. Dann beginnt er mit gleicher Wahrscheinlichkeit $\frac{1}{2}$ immer wieder entweder nach rechts oder nach links zu springen.

Frage: Mit welcher Wahrscheinlichkeit wird der Frosch nach n Sprüngen vom Anfangsstein 0 mindestens a Steine weit entfernt sein (für eine gegebene Zahl a)?

Für jedes $i \in [n]$ sei $X_i = +1$, falls der Frosch im i-ten Schritt nach rechts springt, und $X_i = -1$, falls er im i-ten Schritt nach links springt.
Sei $X := \sum_{i=1}^{n} X_i$. D.h. X gibt an, auf welchem Stein er sich nach n Sprüngen befindet.

Für jedes $i \in [n]$ gilt: $\mathrm{E}(X_i) = (-1) \cdot \frac{1}{2} + (+1) \cdot \frac{1}{2} = 0$.
Also gilt:

$$\mathrm{E}(X) \;=\; \mathrm{E}\left(\sum_{i=1}^{n} X_i\right) \;=\; \sum_{i=1}^{n} \mathrm{E}(X_i) \;=\; \sum_{i=1}^{n} 0 \;=\; 0\,.$$

D.h.: Nach n Sprüngen sitzt der Frosch „im Erwartungswert“ wieder auf seinem ursprünglichen Ausgangspunkt.

Aber mit welcher Wahrscheinlichkeit hat er dennoch eine Entfernung $\geqslant a$ vom Startpunkt (für eine gegebene Zahl a)?

Die Zufallsvariable $|X - 0| = |X|$ gibt die Entfernung vom Startpunkt nach n Sprüngen an. Die Tschebyscheff-Ungleichung liefert (beachte dazu, dass $\mathrm{E}(X) = 0$ ist):

$$\mathrm{P}(|X| \geqslant a) \;=\; \mathrm{P}(|X - \mathrm{E}(X)| \geqslant a) \;\leqslant\; \frac{\mathrm{Var}(X)}{a^2}\,. \qquad (5.9)$$

Wir nutzen Satz 5.28, um die Varianz $\mathrm{Var}(X)$ auszurechnen: Die Zufallsvariablen $X_1, \ldots, X_n$ sind paarweise unabhängig voneinander. Daher gilt:

$$\mathrm{Var}(X) \;=\; \mathrm{Var}\left(\sum_{i=1}^{n} X_i\right) \;=\; \sum_{i=1}^{n} \mathrm{Var}(X_i)\,.$$

Für jedes einzelne $i \in [n]$ gilt: $\mathrm{E}((X_i)^2) = (-1)^2 \cdot \frac{1}{2} + (+1)^2 \cdot \frac{1}{2} = 1$.

Also ist

$$\mathrm{Var}(X_i) \quad = \quad \mathrm{E}((X_i)^2) - \mathrm{E}(X_i) \quad = \quad 1 - 0 \quad = \quad 1\,.$$

Somit gilt:

$$\mathrm{Var}(X) \quad = \quad \sum_{i=1}^{n} \mathrm{Var}(X_i) \quad = \quad n\,.$$

Wir setzen dies in (5.9) ein und erhalten:

$$\mathrm{P}(|X| \geqslant a) \quad \leqslant \quad \frac{\mathrm{Var}(X)}{a^2} \quad = \quad \frac{n}{a^2}\,.$$

Somit gilt für jedes $a > 0$: Die Wahrscheinlichkeit, dass der Frosch nach n Sprüngen einen Abstand $\geqslant a$ vom Startpunkt hat, ist $\leqslant \frac{n}{a^2}$.
Insbes. gilt z.B. bei $n = 100$ Sprüngen: Die Wahrscheinlichkeit, dass er am Ende einen Abstand von $\geqslant 20$ vom Startpunkt hat, ist $\leqslant \frac{100}{20^2} = \frac{100}{400} = \frac{1}{4}$.

5.8 Bedingte Wahrscheinlichkeiten

Folie 302

Definition 5.30. Sei (Ω, P) ein endlicher Wahrscheinlichkeitsraum. Seien A, B zwei Ereignisse.
Die *bedingte Wahrscheinlichkeit* $\mathrm{P}(A|B)$ für das Ereignis A unter der Bedingung B ist definiert durch

$$\mathrm{P}(A|B) \quad := \quad \frac{\mathrm{P}(A \cap B)}{\mathrm{P}(B)}\,.$$

Die Wahrscheinlichkeit $\mathrm{P}(A|B)$ bezeichnet man auch als *a-posteriori-Wahrscheinlichkeit* von A bzgl. B.

Interpretation: Wir stellen uns vor, dass wir ein Zufallsexperiment durchgeführt haben und bereits wissen, dass Ereignis B eingetreten ist. Der Wert $\mathrm{P}(A|B)$ gibt an, mit welcher Wahrscheinlichkeit hierbei auch das Ereignis A eingetreten ist.

Folie 303

Beispiel 5.31. Wir führen unabhängig voneinander drei Würfe mit einer fairen Münze durch. Der Wahrscheinlichkeitsraum ist also (Ω, P) mit $\Omega = \{K, Z\}^3$ und $\mathrm{P}(\omega) = \frac{1}{|\Omega|} = \frac{1}{8}$ für jedes $\omega \in \Omega$.
Sei A das Ereignis, dass mind. 2 der 3 Münzwürfe das Ergebnis „K“ liefern. Dann ist $\mathrm{P}(A) = \frac{4}{8} = \frac{1}{2}$.

Nehmen wir mal an, dass wir den ersten Münzwurf gesehen haben und wissen, dass dessen Ergebnis „Z“ war. Nun wollen wir wissen, mit welcher Wahrscheinlichkeit unter den insgesamt 3 Münzwürfen dennoch das Ereignis A eingetreten ist.

Sei B das Ereignis, dass beim ersten Münzwurf das Ergebnis „Z“ eingetreten ist. Dann ist $\mathrm{P}(B) = \frac{1}{2}$.

Außerdem ist $\mathrm{P}(A \cap B) = \frac{1}{8}$, denn $A \cap B = \{ZKK\}$.

Somit ist

$$\mathrm{P}(A|B) \;=\; \frac{\mathrm{P}(A \cap B)}{\mathrm{P}(B)} \;=\; \tfrac{1}{8} \cdot \tfrac{2}{1} \;=\; \tfrac{1}{4}\,.$$

Folie 304

Bemerkung 5.32. Zwei Ereignisse A, B sind genau dann (stochastisch) unabhängig voneinander, wenn gilt: $\mathrm{P}(A \cap B) = \mathrm{P}(A) \cdot \mathrm{P}(B)$.
Somit gilt für beliebige Ereignisse A, B:

$$\mathrm{P}(A|B) = \mathrm{P}(A) \quad\Longleftrightarrow\quad A \text{ und } B \text{ sind (stochastisch) unabhängig.}$$

Folie 305

Rechenregeln

Bemerkung 5.33. Für jeden Wahrscheinlichkeitsraum (Ω, P) und alle Ereignisse A und B gilt:

(a) *Multiplikationssatz für Wahrscheinlichkeiten*:
$\mathrm{P}(A \cap B) \;=\; \mathrm{P}(B) \cdot \mathrm{P}(A|B)$

(b) *Satz von Bayes*: Ist $\mathrm{P}(A) \neq 0$ und $\mathrm{P}(B) \neq 0$, so gilt:

$$\mathrm{P}(A|B) \;=\; \frac{\mathrm{P}(A)}{\mathrm{P}(B)} \;\cdot\; \mathrm{P}(B|A)\,.$$

(c) *Satz der totalen Wahrscheinlichkeit*: Sei $\ell \in \mathbb{N}_{\geqslant 1}$ und seien $B_1, \ldots, B_\ell \subseteq \Omega$, so dass gilt: $\Omega = \bigcup_{i \in [\ell]} B_i$ und die Mengen $B_1, \ldots, B_\ell$ sind paarweise disjunkt. Dann gilt:

$$\mathrm{P}(A) \;=\; \sum_{i=1}^{\ell} \mathrm{P}(A \cap B_i) \;=\; \sum_{i=1}^{\ell} \mathrm{P}(B_i) \cdot \mathrm{P}(A|B_i)\,.$$

Beweis. (a): Dies folgt direkt aus Definition 5.30.

(b): Gemäß Definition 5.30 gilt:

$$\mathrm{P}(A|B) = \frac{\mathrm{P}(A \cap B)}{\mathrm{P}(B)} \qquad \text{und} \qquad \mathrm{P}(B|A) = \frac{\mathrm{P}(A \cap B)}{\mathrm{P}(A)}.$$

Somit gilt:

$$\mathrm{P}(A \cap B) = \mathrm{P}(A|B) \cdot \mathrm{P}(B) \qquad \text{und} \qquad \mathrm{P}(A \cap B) = \mathrm{P}(B|A) \cdot \mathrm{P}(A).$$

Also gilt:

$$\mathrm{P}(A|B) \cdot \mathrm{P}(B) = \mathrm{P}(B|A) \cdot \mathrm{P}(A).$$

Teilen durch $\mathrm{P}(B)$ liefert:

$$\mathrm{P}(A|B) = \frac{\mathrm{P}(A)}{\mathrm{P}(B)} \cdot \mathrm{P}(B|A).$$

(c): Es gilt: $A = \bigcup_{i=1}^{\ell} (A \cap B_i)$, und die Ereignisse $(A \cap B_i)$ für $i \in \{1, \ldots, \ell\}$ sind paarweise disjunkt. Gemäß (5.4) gilt daher:

$$\mathrm{P}(A) \quad = \quad \sum_{i=1}^{\ell} \mathrm{P}(A \cap B_i)\,.$$

Außerdem gilt gemäß Definition 5.30 für jedes $i \in [\ell]$:

$$\mathrm{P}(A|B_i) \quad = \quad \frac{\mathrm{P}(A \cap B_i)}{\mathrm{P}(B_i)}\,,$$

d.h.: $\mathrm{P}(A \cap B) = \mathrm{P}(B_i) \cdot \mathrm{P}(A|B_i)$. Also gilt:

$$\mathrm{P}(A) \quad = \quad \sum_{i=1}^{\ell} \mathrm{P}(A \cap B_i) \quad = \quad \sum_{i=1}^{\ell} \mathrm{P}(B_i) \cdot \mathrm{P}(A|B_i)\,.$$

□

Folie 306

Beispiel 5.34. Eine Studie[8] zur Zuverlässigkeit von Antigen-Schnelltests auf SARS-CoV-2 kam zu folgendem Ergebnis innerhalb einer Gruppe von Personen, die Symptome einer COVID-19-Erkrankung hatten und einen Antigen-Schnelltest durchführten:

[8] https://www.cochrane.de/news/aktueller-cochrane-review-wie-zuverlaessig-sind-corona-schnelltests

(a) 5% der Personen war tatsächlich an COVID-19 erkrankt;
95% der Personen war gesund;

(b) 4,5% der Personen hatte ein positives Testergebnis;
95,5% der Personen hatte ein negatives Testergebnis;

(c) 99,47% der gesunden Personen hatte ein negatives Testergebnis;
0,53% der gesunden Personen hatte ein positives Testergebnis (d.h. der Test war „falsch positiv“).

(d) 80% der kranken Personen hatte ein positives Testergebnis;
20% der kranken Personen hatte ein negatives Testergebnis (d.h. der Test war „falsch negativ“);

Folie 307

Wir wollen nun die beiden folgenden Fragen beantworten:

1. Wenn ich ein negatives Testergebnis habe: Wie groß ist die Wahrscheinlichkeit, dass ich tatsächlich gesund bin?
2. Wenn ich ein positives Testergebnis habe: Wie groß ist die Wahrscheinlichkeit, dass ich tatsächlich krank bin?

Um diese Fragen zu beantworten, betrachten wir die folgenden Ereignisse:

- N: „das Testergebnis ist negativ“ (dann ist $\overline{N}$ das Ereignis „das Testergebnis ist positiv“)
- G: „die getestete Person ist gesund“ (dann ist $\overline{G}$ das Ereignis „die getestete Person ist krank“)

Wir sehen das Testergebnis und wissen daher, welches der beiden Ereignisse N bzw. $\overline{N}$ eingetreten ist.
Bei Frage 1 wollen wir wissen, wie groß die Wahrscheinlichkeit $\mathrm{P}(G|N)$ ist.
Bei Frage 2 wollen wir wissen, wie groß die Wahrscheinlichkeit $\mathrm{P}(\overline{G}|\overline{N})$ ist.

Folie 308

Wir wissen:

- Gemäß (a) ist $\mathrm{P}(G) = 0{,}95$ und $\mathrm{P}(\overline{G}) = 0{,}05$.
- Gemäß (b) ist $\mathrm{P}(N) = 0{,}955$ und $\mathrm{P}(\overline{N}) = 0{,}045$.
- Gemäß (c) ist $\mathrm{P}(N|G) = 0{,}9947$ und $\mathrm{P}(\overline{N}|G) = 0{,}0053$.

- Gemäß (d) ist $\mathrm{P}(\overline{N}|\overline{G}) = 0{,}8$ und $\mathrm{P}(N|\overline{G}) = 0{,}2$.

Um die Fragen 1 und 2 zu beantworten, können wir den Satz von Bayes benutzen. Für Frage 1 erhalten wir:

$$\mathrm{P}(G|N) \quad = \quad \frac{\mathrm{P}(G)}{\mathrm{P}(N)} \cdot \mathrm{P}(N|G) \quad = \quad \frac{0{,}95}{0{,}955} \cdot 0{,}9947 \quad = \quad 0{,}98949\cdots \,.$$

D.h.: Wenn ich ein negatives Testergebnis habe, ist (gemäß der zitierten Studie) die Wahrscheinlichkeit, dass ich tatsächlich gesund bin, etwa 98,95%.

Für Frage 2 erhalten wir:

$$\mathrm{P}(\overline{G}|\overline{N}) \quad = \quad \frac{\mathrm{P}(\overline{G})}{\mathrm{P}(\overline{N})} \cdot \mathrm{P}(\overline{N}|\overline{G}) \quad = \quad \frac{0{,}05}{0{,}045} \cdot 0{,}8 \quad = \quad 0{,}\overline{8}\,.$$

D.h.: Wenn ich ein positives Testergebnis habe, ist (gemäß der zitierten Studie) die Wahrscheinlichkeit, dass ich tatsächlich krank bin, $88{,}\overline{8}\%$. Es besteht also immerhin noch eine Wahrscheinlichkeit von $11{,}\overline{1}\%$ dass ich gesund bin.

5.9 Einige wichtige Wahrscheinlichkeitsräume

Folie 309

Einfache Urnenmodelle

Beispiel 5.35. In einer Urne befinden sich n Kugeln, die mit den Zahlen $1, \ldots, n$ durchnummeriert sind. Wir ziehen zufällig nacheinander k Kugeln. Wir nutzen im Folgenden unsere Erkenntnisse aus Abschnitt 4.2.

Variante 1: *Mit Zurücklegen und mit Berücksichtigung der Reihenfolge*

Dies entspricht dem Wahrscheinlichkeitsraum $(\Omega_{\mathrm{mm}}, \mathrm{P}_{\mathrm{mm}})$ mit

$$\Omega_{\mathrm{mm}} \;:=\; \{\, (a_1, \ldots, a_k) \;:\; a_1, \ldots, a_k \in [n] \,\}$$

mit $|\Omega_{\mathrm{mm}}| = n^k$ und $\mathrm{P}_{\mathrm{mm}}(\omega) = \frac{1}{|\Omega_{\mathrm{mm}}|}$ für alle $\omega \in \Omega_{\mathrm{mm}}$.

Variante 2: *Ohne Zurücklegen und mit Berücksichtigung der Reihenfolge*

Dies entspricht dem Wahrscheinlichkeitsraum $(\Omega_{\mathrm{om}}, \mathrm{P}_{\mathrm{om}})$ mit

$$\Omega_{\mathrm{om}} \;:=\; \{\, (a_1, \ldots, a_k) \in [n]^k \;:\; a_1, \ldots, a_k \text{ sind paarweise verschieden} \,\}$$

mit $|\Omega_{\mathrm{om}}| = (n)_k$ und $\mathrm{P}_{\mathrm{om}}(\omega) = \frac{1}{|\Omega_{\mathrm{om}}|}$ für alle $\omega \in \Omega_{\mathrm{om}}$.

Variante 3: *Ohne Zurücklegen und ohne Berücksichtigung der Reihenfolge*

Dies entspricht dem Wahrscheinlichkeitsraum $(\Omega_{\text{oo}}, \mathrm{P}_{\text{oo}})$ mit

$$\Omega_{\text{oo}} \;:=\; \{X \subseteq [n] \,:\, |X| = k\}$$

mit $|\Omega_{\text{oo}}| = \binom{n}{k}$ und $\mathrm{P}_{\text{oo}}(\omega) = \frac{1}{|\Omega_{\text{oo}}|}$ für alle $\omega \in \Omega_{\text{oo}}$.

Variante 4: *Mit Zurücklegen und ohne Berücksichtigung der Reihenfolge*

Dies entspricht dem Wahrscheinlichkeitsraum $(\Omega_{\text{mo}}, \mathrm{P}_{\text{mo}})$ mit

$$\Omega_{\text{mo}} \;:=\; \{f : [n] \to \mathbb{N} \,:\, \sum_{x=1}^{n} f(x) = k\}$$

mit $|\Omega_{\text{mo}}| = \binom{k+n-1}{n-1}$ und $\mathrm{P}_{\text{mo}}(\omega) = \frac{1}{|\Omega_{\text{mo}}|}$ für alle $\omega \in \Omega_{\text{mo}}$.

Produktexperimente

Wir stellen uns vor, dass wir nacheinander n Zufallsexperimente unabhängig voneinander durchführen und deren Ergebnisse in einem n-Tupel zusammenfassen. Beispielsweise könnten wir dreimal hintereinander eine Münze werfen, danach zweimal würfeln und dann noch ohne Zurücklegen und ohne Berücksichtigung der Reihenfolge vier Kugeln aus einer Urne mit insgesamt 15 Kugeln ziehen.

Definition 5.36. Sei $n \in \mathbb{N}_{\geqslant 1}$, und für jedes $i \in [n]$ sei (Ω_i, P_i) ein endlicher Wahrscheinlichkeitsraum.
Das *Produkt der Wahrscheinlichkeitsräume* (Ω_i, P_i) für $i \in [n]$ ist (Ω, P) mit

$$\Omega \;:=\; \Omega_1 \times \cdots \times \Omega_n$$

und, für jedes $\omega = (\omega_1, \ldots, \omega_n) \in \Omega$,

$$\mathrm{P}(\omega) \;:=\; \prod_{i=1}^{n} \mathrm{P}_i(\omega_i)\,.$$

Man kann sich leicht davon überzeugen, dass (Ω, P) ein endlicher Wahrscheinlichkeitsraum ist (Details: Übungsaufgabe).

Die Bernoulli-Verteilung

Ein *Bernoulli-Experiment* ist ein Zufallsexperiment, bei dem es nur 2 verschiedene Ausgänge gibt. Das Paradebeispiel dafür ist der Wurf einer Münze. Wir sprechen von einem „Erfolg“, wenn die Münze auf „Kopf“ landet, und von einem „Misserfolg“, wenn sie auf „Zahl“ landet.
Es sei p (mit $0 \leqslant p \leqslant 1$) die „Erfolgswahrscheinlichkeit“, d.h. die Wahrscheinlichkeit, dass die Münze auf „Kopf“ landet.
Als Wahrscheinlichkeitsraum nutzen wir (Ω, P) mit $\Omega = \{K, Z\}$ und $\mathrm{P}(K) = p$ und $\mathrm{P}(Z) = 1-p$. Die Verteilung P wird auch die *Bernoulli-Verteilung* genannt.
Die Zufallsvariable X mit $X(K) = 1$ und $X(Z) = 0$ wird auch *Indikatorvariable* genannt. Sie hat Erwartungswert

$$\mathrm{E}(X) \quad = \quad 1 \cdot \mathrm{P}(X = 1) \; + \; 0 \cdot \mathrm{P}(X = 0) \quad = \quad p$$

und Varianz

$$\mathrm{Var}(X) \quad = \quad \mathrm{E}(X^2) - \mathrm{E}(X)^2 \quad = \quad p - p^2 \quad = \quad p \cdot (1-p)\,.$$

Die *Binomialverteilung* $B(n, p)$

Wir führen unabhängig voneinander n Bernoulli-Experimente durch, bei denen jedes dieselbe Erfolgswahrscheinlichkeit p besitzt.
Für jedes $i \in [n]$ sei X_i die Indikatorvariable, die angibt, ob das i-te Experiment erfolgreich war oder nicht. D.h.: $\mathrm{P}(X_i = 1) = p$, $\mathrm{P}(X_i = 0) = 1 - p$, $\mathrm{E}(X_i) = p$ und $\mathrm{Var}(X_i) = p \cdot (1-p)$.
Wir betrachten die Zufallsvariable $S := \sum_{i=1}^{n} X_i$. D.h. S gibt an, wie viele der n Experimente erfolgreich waren.
Für jedes $k \in \{0, \ldots, n\}$ gilt:

$$\mathrm{P}(S = k) \quad = \quad \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k}\,.$$

Es gilt gemäß der Linearität des Erwartungswerts:

$$\mathrm{E}(S) \quad = \quad \sum_{i=1}^{n} \mathrm{E}(X_i) \quad = \quad n \cdot p\,.$$

Da die Zufallsvariablen $X_1, \ldots, X_n$ paarweise unabhängig sind, gilt gemäß Satz 5.28:

$$\mathrm{Var}(S) \quad = \quad \sum_{i=1}^{n} \mathrm{Var}(X_i) \quad = \quad n \cdot p \cdot (1-p)\,.$$

Folie 314

Die *geometrische Verteilung*

Wir führen wieder unabhängig voneinander n Bernoulli-Experimente durch, bei denen jedes dieselbe Erfolgswahrscheinlichkeit p besitzt. Es sei $0 < p < 1$.
Für jedes $i \in [n]$ sei X_i die Indikatorvariable, die angibt, ob das i-te Experiment erfolgreich war oder nicht.
Wir betrachten die Zufallsvariable $Y := \min\{i \in [n] \,:\, X_i = 1\}$, d.h.: $Y = k$ bedeutet, dass die ersten $k-1$ Durchführungen des Zufallsexperiments zu einem Misserfolg führten und die k-te Durchführung erfolgreich war. Es gilt:

$$\mathrm{P}(Y = k) \quad = \quad (1-p)^{k-1} \cdot p\,.$$

Wenn wir jetzt kein festes n mehr vorgeben, sondern einfach das Bernoulli-Experiment immer weiter hintereinander durchführen, bis wir den ersten „Erfolg“ erzielt haben, betrachten wir den *diskreten Wahrscheinlichkeitsraum* (Ω, P) mit $\Omega = \mathbb{N}_{\geqslant 1}$ und $\mathrm{P}(k) = (1-p)^{k-1} \cdot p$ für alle $k \in \Omega$.
Man kann nachrechnen (hier ohne Beweis), dass P eine Wahrscheinlichkeitsverteilung auf Ω ist und dass die Zufallsvariable Y den Erwartungswert $\mathrm{E}(Y) = \frac{1}{p}$ und die Varianz $\mathrm{Var}(Y) = \frac{1-p}{p^2}$ hat.

5.10 Ein weiteres Beispiel: Das Monty Hall Problem

Folie 315

Beispiel 5.37 (Das Monty Hall Problem)**.** In der TV-Spielshow „Geh aufs Ganze!“ stehen drei „Tore“ namens „Tor 1“, „Tor 2“, „Tor 3“ zur Verfügung. Hinter einem davon verbirgt sich der Hauptpreis, hinter einem weiteren ein Trostpreis, und hinter dem verbliebenen eine Niete, die „der Zonk“ genannt wird.

Das Spiel läuft zwischen dem Showmaster und einem Kandidaten ab, und zwar wie folgt:

1. Der Kandidat sucht sich eins der drei Tore aus.
2. Der Showmaster öffnet eines der beiden verbliebenen Tore — und zwar eins, hinter dem sich entweder der Zonk oder der Trostpreis befinden.
3. Der Kandidat kann entscheiden, ob er bei seinem in Punkt 1 gewählten Tor bleibt, oder ob er zu dem anderen noch geschlossenen Tor wechselt.

Danach ist das Spiel beendet und der Kandidat gewinnt das, was sich hinter dem Tor verbirgt, für das er sich in Punkt 3 entschieden hat.

Frage: Was sollte der Kandidat in Schritt 3 tun, um seine Chancen auf den Hauptgewinn zu maximieren?

Dieses Problem ist auch unter den Begriffen *Monty Hall Problem* bzw. *Ziegenproblem* bekannt.

Folie 316

Zur Beantwortung der Frage wenden wir wieder die 3-Schritt-Methode an.

Schritt 1: Finde den richtigen Wahrscheinlichkeitsraum

Wir wählen $\Omega := \{ (i,j) : i,j \in \{1,2,3\} \}$. Hierbei steht $\omega = (i,j)$ für das Elementarereignis, bei dem der Hauptgewinn sich hinter „Tor i“ verbirgt und der Kandidat in Punkt 1 „Tor j“ wählt.

Wir gehen davon aus, dass der Showmaster die Preise bzw. Nieten zufällig auf die 3 Tore verteilt hat und dass der Kandidat in Punkt 1 zufällig eins der drei Tore wählt (jedes mit derselben Wahrscheinlichkeit). Somit gilt für jedes $\omega \in \Omega$, dass $\mathrm{P}(\omega) = \frac{1}{|\Omega|} = \frac{1}{9}$ ist.

Folie 317

Schritt 2: Finde die relevanten Ereignisse

Wir untersuchen 2 verschiedene Strategien, die der Kandidat verfolgen könnte.

Strategie 1: Er bleibt bei dem in Punkt 1 gewählten Tor.

Strategie 2: Er wechselt in Punkt 3 zu dem (einzigen noch verbliebenen) anderen Tor.

Dass er bei Strategie 1 den Hauptgewinn bekommt, entspricht dem Ereignis $A := \{ (i,i) : i \in [3] \}$.

Dass er bei Strategie 2 den Hauptgewinnn bekommt, entspricht dem Ereignis $B := \{ (i,j) : i,j \in [3],\ i \neq j \} = \bar{A}$.

Schritt 3: Berechne die Wahrscheinlichkeiten der Ereignisse A und B

$\mathrm{P}(A) = \frac{|A|}{|\Omega|} = \frac{3}{9} = \frac{1}{3}$.

$\mathrm{P}(B) = \mathrm{P}(\bar{A}) = 1 - \mathrm{P}(A) = 1 - \frac{1}{3} = \frac{2}{3}$.

D.h.: Um eine möglichst große Gewinnwahrscheinlichkeit zu haben, sollte der Kandidat in Punkt 3 das Tor wechseln. Dann wird er mit Wahrscheinlichkeit $\frac{2}{3}$ den Hauptgewinn erhalten.

Intuitive Erläuterung: Wenn der Showmaster in Schritt 2 nicht ein Tor öffnen, sondern einfach fragen würde, ob der Kandidat lieber darauf wetten will, dass der Hauptgewinn sich hinter einem der beiden anderen (nicht von ihm in Schritt 1 gewählten) Tore befindet, könnte man leicht einsehen, dass „Wechseln“ eine Erfolgswahrscheinlichkeit von $\frac{2}{3}$ hat.

5.11 Literaturhinweise

Als vertiefende Lektüre seien die Kapitel 11 und 12 von [Juk08] sowie das Lehrbuch [Kre91] empfohlen.

Quellennachweis: Teile dieses Kapitels basieren auf Teilen der Kapitel 11 und 12 von [Juk08].

5.12 Übungsaufgaben

Aufgabe 5.1. Sei Ω ein endlicher Wahrscheinlichkeitsraum und seien $A, B \subseteq \Omega$ Ereignisse mit $\mathrm{P}(A) = 0{,}7$; $\mathrm{P}(B) = 0{,}6$ und $\mathrm{P}(A \cap B) = 0{,}5$. Berechnen Sie:

(a) $\mathrm{P}(A \cup B)$

(b) $\mathrm{P}(\overline{A} \cup \overline{B})$

(c) $\mathrm{P}(\overline{A} \cap \overline{B})$

(d) $\mathrm{P}(A \cap \overline{B})$

(e) $\mathrm{P}(\overline{A} \cap B)$

(f) $\mathrm{P}\Big((A \cap \overline{B}) \cup (\overline{A} \cap B)\Big)$

Begründen Sie jeweils Ihre Antwort.

Aufgabe 5.2. Wenden Sie zur Lösung der folgenden Aufgaben jeweils die 3-Schritt-Methode an.

(a) Gegeben seien drei verschiedene positive ganze Zahlen a_1, a_2, a_3 und drei verschiedene negative ganze Zahlen b_1, b_2, b_3. Aus diesen sechs Zahlen ziehen wir, ohne Zurücklegen, zufällig zwei Zahlen und wetten darauf, ob deren Produkt positiv oder negativ ist. Auf welches Ergebnis sollten Sie wetten, um Ihre Gewinnchancen zu maximieren?

(b) Gegeben sei eine faire Münze, deren Wurf mit gleicher Wahrscheinlichkeit Kopf oder Zahl ergibt, und eine unfaire Münze, deren Wurf immer Kopf ergibt. Wir wählen eine der beiden Münzen zufällig aus und werfen sie zweimal. Angenommen, beide Würfe ergeben Kopf. Wie groß ist dann die Wahrscheinlichkeit, dass die unfaire Münze ausgewählt wurde?

Aufgabe 5.3.

(a) Harald Töpfer steht vor dem finalen Rätsel auf seiner epischen Reise – der Suche nach dem sagenumwobenen Stein der Greise. Das Rätsel selbst ist (insbesondere nach dem dreiköpfigen Riesenhund und dem menschlichen Schachspiel) erstaunlich harmlos: Harald muss lediglich den korrekten Schlüssel aus den unzähligen herumschwirrenden geflügelten Schlüsseln finden. Da sich die Schlüssel nicht unterscheiden lassen, bleibt Harald nur stumpfes, zufälliges Ausprobieren.

Angenommen, es flattern n Schlüssel durch den Raum. Berechnen Sie den Erwartungswert $\mathrm{E}(X)$ der Zufallsvariable X, die die Anzahl ausprobierter Schlüssel bezeichnet, wenn Harald die Schlüssel nach dem Ausprobieren *nicht* wieder fliegen lässt, das heißt, er wird bereits getestete Schlüssel nicht noch einmal fangen und testen.

(b) Wir betrachten m Bälle und n Körbe. Jeden Ball werfen wir zufällig und unabhängig voneinander in die Körbe. Jeder Ball kann also mit gleicher Wahrscheinlichkeit $\frac{1}{n}$ in jedem Korb landen. Bestimmen Sie den Erwartungswert der folgenden Zufallsvariablen:

(i) X sei die Anzahl aller Bälle im *ersten* Korb.

(ii) Y sei die Anzahl aller Körbe mit *genau einem* Ball darin.

(c) In einem Wahlbüro zählen Hans und Franz die Stimmen aus. Dabei ist ihnen folgendes aufgefallen: Mit einer Wahrscheinlichkeit von $\frac{2}{3}$ ist der Stimmzettel einwandfrei und kann gewertet werden. Umgekehrt gibt es jedoch mit einer Wahrscheinlichkeit von $\frac{1}{3}$ irgendeine Art von Formfehler und die Stimme ist ungültig. Hans und Franz wissen, dass die Wahl (erneut) wiederholt werden muss, wenn es am Ende nicht mindestens 100 gültige Stimmen *mehr* gibt als ungültige.

Geben Sie mittels der Tschebyscheff-Ungleichung eine Schätzung der Wahrscheinlichkeit darüber ab, ob die Wahl erneut wiederholt werden muss, wenn noch 500 Stimmen ausgezählt werden müssen und die gültigen Stimmen momentan gleichauf sind mit den ungültigen.

Begründen Sie jeweils Ihre Antwort.

Aufgabe 5.4. Für $i \in [n]$ mit $n \in \mathbb{N}_{\geqslant 1}$ seien endliche Wahrscheinlichkeitsräume (Ω_i, P_i) gegeben. Beweisen Sie, dass das Produkt der Wahrscheinlichkeitsräume (Ω, P), definiert durch

$$\begin{aligned} \Omega &:= \Omega_1 \times \cdots \times \Omega_n, \\ \mathrm{P}(\omega) &:= \prod_{i=1}^{n} \mathrm{P}_i(\omega_i), \end{aligned}$$

ebenfalls ein endlicher Wahrscheinlichkeitsraum ist.

Aufgabe 5.5. Ein Sortiment aus 20 Teilen gilt als „gut“, wenn es höchstens zwei defekte Teile enthält und als „schlecht“, wenn es mindestens vier defekte Teile enthält. Weder Käufer, noch Verkäufer wissen, ob das gegebene Sortiment gut oder schlecht ist. Deshalb beschließen Sie, vier zufällig herausgegriffene Teile zu testen. Nur wenn alle vier in Ordnung sind, findet der Kauf (des ganzen Sortiments) statt. Der Verkäufer trägt bei diesem Verfahren das Risiko, ein gutes Sortiment nicht zu verkaufen, der Käufer das Risiko, ein schlechtes Sortiment zu kaufen. Wer trägt das größere Risiko?

Aufgabe 5.6. Die folgende Frage hat der französische Edelmann De Méré an seinen Freund Pascal im 17. Jahrhundert gestellt: Wir würfeln dreimal und betrachten die Ereignisse A, dass die Summe der Augenzahlen 11 ist, und B, dass die Summe der Augenzahlen 12 ist. Sind diese beiden Ereignisse gleich wahrscheinlich?
Wenden Sie die 3-Schritt-Methode an, um die Wahrscheinlichkeiten $\mathrm{P}(A)$ und $\mathrm{P}(B)$ zu bestimmen und De Mérés Frage zu beantworten.

Kapitel 6

Algebraische Strukturen

6.1 Modulare Arithmetik

Teilbarkeit und Division mit Rest

Folie 318

Definition 6.1. Sei $x \in \mathbb{R}$.

(a) Der *Betrag* von x ist definiert als

$$|x| := \begin{cases} x & \text{falls } x \geqslant 0 \\ (-1) \cdot x & \text{falls } x < 0. \end{cases}$$

(b) Wir schreiben $\lfloor x \rfloor$ für die größte Zahl $z \in \mathbb{Z}$ mit $z \leqslant x$.

(c) Wir schreiben $\lceil x \rceil$ für die kleinste Zahl $z \in \mathbb{Z}$ mit $z \geqslant x$.

Beispiel: Für $x := 3{,}7$ ist $|x| = 3{,}7$ und $\lfloor x \rfloor = 3$ und $\lceil x \rceil = 4$.
Für $x := -7$ ist $|x| = 7$ und $\lfloor x \rfloor = -7$ und $\lceil x \rceil = -7$.

Folie 319

Definition 6.2. Sei $b \in \mathbb{Z}$.
Ein (ganzzahliger) *Teiler* von b ist eine Zahl $a \in \mathbb{Z}$ mit $a \neq 0$, so dass es ein $c \in \mathbb{Z}$ mit $a \cdot c = b$ gibt.
Wir sagen dann auch: b ist ein (ganzzahliges) *Vielfaches* von a.
Wir schreiben $a \,|\, b$ um auszudrücken, dass a ein Teiler von b ist.

Definition 6.3. Eine *Primzahl* ist eine eine Zahl $p \in \mathbb{N}$ mit $p \geqslant 2$, deren einzige Teiler die Zahlen 1 und p sind.

Folie 320

Teilbarkeitsregeln

Bemerkung 6.4. Für alle $a, b, c \in \mathbb{Z}$ gilt:

(a) Aus $a \mid b$ folgt für alle $d \in \mathbb{Z}$, dass $a \mid bd$.

(b) *Transitivität:* Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$.

(c) Aus $a \mid b$ und $a \mid c$ folgt für alle $s, t \in \mathbb{Z}$, dass $a \mid (sb + tc)$.

(d) Aus $a \mid (b + c)$ und $a \mid b$ folgt $a \mid c$.

(e) Ist $c \neq 0$, so gilt: $a \mid b \iff ac \mid bc$.

(f) Aus $a \mid b$ und $b \mid a$ folgt: $a = b$ oder $a = (-1) \cdot b$.

Beweis. Dies folgt ganz leicht aus Definition 6.2. Details: Übungsaufgabe. □

Folie 321

Division mit Rest

Satz 6.5. *Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$.*
Dann gibt es $q, r \in \mathbb{Z}$ mit $0 \leqslant r < |b|$, so dass $a = qb + r$.
Diese Zahlen q, r sind eindeutig bestimmt.

Die Zahl r wird der Rest von a modulo b genannt;
die Zahl q wird Ganzzahlquotient von a bzgl. b genannt.

Beweis. Sei $S := \{a - qb : q \in \mathbb{Z}, \text{ so dass } (a - qb) \in \mathbb{N} \text{ ist }\}$.
Wegen $b \neq 0$ ist $S \neq \emptyset$. Sei r das *kleinste* Element in S (bzgl. der linearen Ordnung $\leqslant$ der natürlichen Zahlen).
Wegen $r \in S$ gilt: Es gibt ein $q \in \mathbb{Z}$ mit $r = a - qb$. Somit ist $a = qb + r$.

Behauptung 1: $0 \leqslant r < |b|$

Beweis: Wegen $r \in \mathbb{N}$ ist $r \geqslant 0$.
Wir führen einen Beweis durch Widerspruch und nehmen an, r wäre $\geqslant |b|$.
Dann ist $0 \leqslant r - |b| = a - qb - |b|$.
Falls $b > 0$ ist, setzen wir $\tilde{q} := q+1$ und erhalten $r - |b| = a - \tilde{q}b \in S$.
Falls $b < 0$ ist, setzen wir $\tilde{q} := q-1$ und erhalten $r - |b| = a - \tilde{q}b \in S$.

In beiden Fällen ist $\tilde{r} := r - |b| \in S$ und $\tilde{r} < r$ — was ein Widerspruch zur Minimalität von r ist. $\square_{Beh.1}$

Somit haben wir Zahlen $q, r \in \mathbb{Z}$ mit $0 \leqslant r < |b|$ gefunden, so dass $a = qb + r$ ist.

Behauptung 2: Für alle $r', q' \in \mathbb{Z}$ mit $0 \leqslant r' < |b|$ und $a = q'b + r'$ gilt: $q' = q$ und $r' = r$.

Beweis: Es gilt: $0 = a - a = qb + r - q'b - r'$. Also ist $r - r' = q'b - qb = (q'-q)b$.
Somit ist b ein Teiler von $(r-r')$.
Außerdem gilt wegen $0 \leqslant r < |b|$ und $0 \leqslant r' < |b|$, dass $|r-r'| < |b|$. Wegen $b \,|\, (r-r')$ muss daher gelten: $r - r' = 0$.
D.h.: $r = r'$ und $qb = q'b$. Da $b \neq 0$ ist, können wir durch b teilen und erhalten: $q = q'$. $\square_{Beh.2}$

Dies beendet den Beweis von Satz 6.5. $\square$

Folie 322

Kongruenz modulo n

Definition 6.6. Sei $n \in \mathbb{N}_{\geqslant 1}$.
Zwei Zahlen $a, b \in \mathbb{Z}$ heißen *kongruent modulo* n, kurz:

$$a \equiv b \mod n$$

falls der Rest von a modulo n und der Rest von b modulo n identisch sind.

Bemerkung 6.7. Für alle $n \in \mathbb{N}_{\geqslant 1}$ und alle $a, b \in \mathbb{Z}$ gilt:

$$a \equiv b \mod n \quad \Longleftrightarrow \quad n \,|\, (a - b)\,.$$

Beweis. Seien $q, r, q', r' \in \mathbb{Z}$ mit $0 \leqslant r < n$ und $0 \leqslant r' < n$ gemäß Satz 6.5 gewählt, so dass $a = qn + r$ und $b = q'n + r'$. Es gilt:

$$\begin{aligned} a \equiv b \mod n \quad &\Longleftrightarrow \quad r = r' \quad \Longleftrightarrow \quad a-b \;=\; qn - q'n \;=\; (q-q')n \\ &\Longleftrightarrow \quad n \,|\, (a-b)\,. \end{aligned}$$

$\square$

Folie 323

Regeln zum Rechnen mit Kongruenzen

Lemma 6.8. *Sei $n \in \mathbb{N}_{\geqslant 1}$. Seien $a, b, x, y \in \mathbb{Z}$, so dass gilt:*

$$x \equiv y \mod n \qquad \text{und} \qquad a \equiv b \mod n\,.$$

Dann gilt:

(a) $x + a \equiv y + b \mod n$.

(b) $x - a \equiv y - b \mod n$.

(c) $xa \equiv yb \mod n$.

(d) Für jedes $d \in \mathbb{N}$ gilt: $x^d \equiv y^d \mod n$.

Beweis. Dies folgt leicht aus Definition 6.6 und Bemerkung 6.7. Details: Übungsaufgabe. □

Teilerfremde Zahlen und der ggT

Folie 324

Definition 6.9. Seien $a, b \in \mathbb{Z} \setminus \{0\}$.

(a) Der *größte gemeinsame Teiler* $\mathrm{ggT}(a, b)$ der Zahlen a und b ist die größte Zahl $t \in \mathbb{N}_{\geqslant 1}$, für die gilt: $t \mid a$ und $t \mid b$.

Beispiel: $\mathrm{ggT}(8, 12) = 4$, $\mathrm{ggT}(-21, 7) = 7$, $\mathrm{ggT}(8, 9) = 1$.

(b) Die Zahlen a und b heißen *teilerfremd* (oder: *relativ prim*), falls gilt: $\mathrm{ggT}(a, b) = 1$.

Folie 325

Linearkombinationen

Definition 6.10. Eine (ganzzahlige) *Linearkombination* zweier Zahlen $a, b \in \mathbb{Z}$ ist eine Zahl der Form $xa + yb$ mit $x, y \in \mathbb{Z}$.
Eine Linearkombination ist *positiv* falls sie > 0 ist.

Satz 6.11 (*Vielfachsummendarstellung des ggT, Lemma von Bézout*)**.**
Seien $a, b \in \mathbb{Z} \setminus \{0\}$.
$\mathrm{ggT}(a,b)$ *ist die kleinste positive Linearkombination von* a *und* b.
Insbesondere gibt es Zahlen $x, y \in \mathbb{Z}$*, so dass* $ax + by = \mathrm{ggT}(a,b)$.

Beweis. Sei $t := \mathrm{ggT}(a,b)$.
Sei $S := \{ax + by \,:\, x, y \in \mathbb{Z},\ ax + by > 0\}$. Wegen $a, b \neq 0$ ist $S \neq \emptyset$. Sei k das kleinste Element von S und seien $x, y \in \mathbb{Z}$,so dass $k = ax + by$.
Wegen $t \mid a$ und $t \mid b$ gilt: $t \mid k$.
Unser Ziel ist, zu zeigen, dass $k = t$ ist.
Wegen $t \mid k$ und $t, k \geqslant 0$ genügt es zu zeigen, dass $k \mid t$; dann folgt gemäß Bemerkung 6.4(f) nämlich, dass $t = k$ ist.

Behauptung 1: $k \mid a$.

Beweis: Seien $q, r \in \mathbb{Z}$ mit $a = qk + r$ und $0 \leqslant r < k$. Es gilt:

$$r \;=\; a - qk \;=\; a - q(ax + by) \;=\; a(1 - qx) + b(-qy)\,.$$

Wegen $(1 - qx) \in \mathbb{Z}$ und $-qy \in \mathbb{Z}$ ist also r eine Linearkombination von a und b.
Falls $r > 0$, so ist $r \in S$. Da k das kleinste Element in S ist, ist $r \geqslant k$.
Widerspruch zu $r < k$.
Somit ist also $r = 0$. D.h.: $a = qk$. Somit gilt: $k \mid a$. $\square_{\text{Beh.1}}$

Auf die gleiche Weise lässt sich Folgendes beweisen:

Behauptung 2: $k \mid b$.

Wegen $k \mid a$ und $k \mid b$ und $t = \mathrm{ggT}(a,b)$ gilt: $k \mid t$. $\square$

Folie 326

Satz 6.12 (Euklid'scher Hilfssatz)**.** *Seien* $a, b \in \mathbb{Z} \setminus \{0\}$ *und sei* $n \in \mathbb{N}_{\geqslant 1}$.
Wenn $n \mid ab$ *und* $\mathrm{ggT}(a,n) = 1$*, dann gilt:* $n \mid b$.

Insbes. gilt für jede Primzahl p*: Falls* $p \mid ab$*, so gilt:* $p \mid a$ *oder* $p \mid b$.

Beweis. Gemäß Voraussetzung gilt: $n \mid ab$ und $\mathrm{ggT}(a,n) = 1$.
Gemäß der Vielfachsummendarstellung des ggT gibt es $x, y \in \mathbb{Z}$, so dass $xa + yn = \mathrm{ggT}(a,n) = 1$.
Multiplizieren mit b liefert: $bxa + byn = b$.
Wegen $n \mid bxa$ (da $n \mid ab$) und $n \mid byn$ gilt: $n \mid bxa + byn = b$.

Sei nun p eine Primzahl mit $p \mid ab$. Falls[1] $p \nmid a$, so gilt: $\text{ggT}(a,p) = 1$ (da p eine Primzahl ist). Gemäß dem eben Gezeigten folgt für $n := p$, dass $p \mid b$. □

Einfache Folgerungen

Satz 6.13.

(a) Für $n \in \mathbb{N}_{\geqslant 1}$ und $a, b \in \mathbb{Z} \setminus \{0\}$ mit $\text{ggT}(n,a) = \text{ggT}(n,b) = 1$ gilt: $\text{ggT}(n, ab) = 1$.

(b) Sei p eine Primzahl und sei $k \in \mathbb{N}$ mit $1 \leqslant k < p$. Es gilt: $p \mid \binom{p}{k}$.

(c) Für jede Primzahl p gilt: $\sqrt{p}$ ist irrational, d.h. $\sqrt{p} \notin \mathbb{Q}$.

Beweis. (a): Sei $t := \text{ggT}(n, ab)$. Angenommen, $t \geqslant 2$. Laut Voraussetzung ist $\text{ggT}(n,a) = \text{ggT}(n,b) = 1$. Somit ist auch $\text{ggT}(t,a) = 1$. Aus $t \mid ab$ und $\text{ggT}(t,a) = 1$ folgt gemäß dem Euklid'schen Hilfssatz, dass $t \mid b$.
Widerspruch zu $\text{ggT}(n,b) = 1$.

(b): Setze $a := \binom{p}{k}$, $b := k!$ und $x := (p)_k$. Es gilt: $a = \frac{x}{b}$, d.h. $ab = x$.
Wegen $p \mid x$ (da $x = (p)_k = p \cdot (p-1) \cdots (p-k+1)$) gilt $p \mid ab$ und da p eine Primzahl ist, folgt aus dem Euklid'schen Hilfssatz: $p \mid a$ oder $p \mid b$.
Gemäß Voraussetzung ist $k < p$, und daher ist auch jeder einzelne Faktor von $b = k! = k \cdot (k-1) \cdots 1$ kleiner als p. Somit gilt: $p \nmid b$. Also gilt: $p \mid a = \binom{p}{k}$.

(c): Gemäß Voraussetzung ist p eine Primzahl. Angenommen, $\sqrt{p} \in \mathbb{Q}$. Dann können wir $\sqrt{p}$ als „gekürzten Bruch" schreiben, d.h. es gibt Zahlen $a, b \in \mathbb{Z} \setminus \{0\}$ und $\text{ggT}(a,b) = 1$, so dass $\sqrt{p} = \frac{a}{b}$.
Es gilt: $p = \frac{a^2}{b^2}$, d.h. $b^2 p = a^2$.
Also gilt: $p \mid a^2$. Aus dem Euklid'schen Hilfssatz folgt: $p \mid a$. Somit gibt es ein $x \in \mathbb{Z}$, so dass $a = px$.

Aus $a^2 = b^2 p$ und $a = px$ folgt: $p^2 x^2 = b^2 p$.
Teilen durch p liefert: $px^2 = b^2$. Somit gilt: $p \mid b^2$. Aus dem Euklid'schen Hilfssatz folgt: $p \mid b$.

Wir haben gezeigt: $p \mid a$ und $p \mid b$. Somit gilt: $\text{ggT}(a,b) \geqslant p$. *Widerspruch* zu $\text{ggT}(a,b) = 1$. □

Bemerkung 6.14 (Kürzungsregel).
Sei $n \in \mathbb{N}_{\geqslant 1}$ und sei $a \in \mathbb{Z} \setminus \{0\}$, so dass $\text{ggT}(n, a) = 1$.
Für alle $x, y \in \mathbb{Z}$ mit $ax \equiv ay \mod n$ gilt: $x \equiv y \mod n$.

Beweis. Wegen $ax \equiv ay \mod n$ gilt: $n \,|\, (ax - ay) = a(x-y)$.
Wegen $\text{ggT}(n, a) = 1$ folgt aus dem Euklid'schen Hilfssatz: $n \,|\, x-y$. Somit gilt: $x \equiv y \mod n$. □

Repräsentantenmengen modulo n

Sei $n \in \mathbb{N}_{\geqslant 1}$. Für jedes $i \in \mathbb{N}$ setze

$$n\mathbb{Z} + i \quad := \quad \{nz + i \,:\, z \in \mathbb{Z}\}\,.$$

Die Menge $n\mathbb{Z} + i$ wird auch *Restklasse modulo n* genannt.
An Stelle von $n\mathbb{Z} + 0$ schreiben wir auch kurz $n\mathbb{Z}$.

Aus Satz 6.5 folgt:

$$\mathbb{Z} \quad = \quad \bigcup_{\substack{r \in \mathbb{N} \text{ mit} \\ 0 \leqslant r < n}} n\mathbb{Z} + r$$

und die Mengen $n\mathbb{Z} + r$ für $0 \leqslant r < n$ sind paarweise disjunkt.
Wir sagen auch: $(n\mathbb{Z} + r)_{0 \leqslant r < n}$ ist eine *Zerlegung* der Menge $\mathbb{Z}$.

Eine *Repräsentantenmenge modulo n* ist eine Menge $R \subseteq \mathbb{Z}$ mit $|R| = n$, so dass es für jedes $r \in \mathbb{N}$ mit $0 \leqslant r < n$ genau ein Element $x_r \in R$ gibt mit $x_r \equiv r \mod n$.

Beispiel: Für $n = 5$ sind $R := \{0, 1, 2, 3, 4\}$ und $R' := \{0, 1, -1, 2, -2\}$ Repräsentantenmengen modulo 5.

Für jedes $n \in \mathbb{N}_{\geqslant 1}$ gilt: Die Menge

$$\mathbb{Z}_n \quad := \quad \{r \in \mathbb{N} \,:\, 0 \leqslant r < n\}$$

ist eine Repräsentantenmenge modulo n.

Lemma 6.15. *Sei $n \in \mathbb{N}_{\geqslant 1}$, sei R eine Repräsentantenmenge modulo n und sei $a \in \mathbb{Z} \setminus \{0\}$ mit $\mathrm{ggT}(a, n) = 1$. Dann ist auch $aR := \{ar : r \in R\}$ eine Repräsentantenmenge modulo n.*

Beweis. Wegen $|R| = n$ und $a \neq 0$ ist $|aR| = n$.

Behauptung: Für alle $X, Y \in aR$ mit $X \neq Y$ gilt: $X \not\equiv Y \mod n$.

Beweis: Wegen $X, Y \in aR$ gibt es $x, y \in R$, so dass $X = ax$ und $Y = ay$ und $x \neq y$. Da R eine Repräsentantenmenge modulo n ist, gilt: $x \not\equiv y \mod n$.
Angenommen, es würde gelten: $X \equiv Y \mod n$, also $ax \equiv ay \mod n$. Dann folgt aus der Kürzungsregel, dass $x \equiv y \mod n$. *Widerspruch.* $\square_{\text{Beh.}}$

Aus der Behauptung sowie der Tatsache, dass $|aR| = n$ ist, folgt, dass aR eine Repräsentantenmenge modulo n ist. $\square$

Folgerung 6.16. *Für jede Primzahl p und jedes $a \in \mathbb{Z} \setminus \{0\}$ ist die folgende Abbildung $f : a\mathbb{Z}_p \to \mathbb{Z}_p$ bijektiv:*

$$f(x) := r \quad \textit{wobei } r \textit{ der Rest von } x \textit{ modulo } p \textit{ ist,}$$

für alle $x \in a\mathbb{Z}_p$; und $a\mathbb{Z}_p$ ist eine Repräsentantenmenge modulo p.

Beispiel: Für $n := 5$ ist $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.
Für $a := 3$ ist $3\mathbb{Z}_5 = \{0, 3, 6, 9, 12\}$ eine Repräsentantenmenge modulo 5. Es gilt:

$$\begin{aligned} 0 &\equiv 0 \mod 5\,, \\ 3 &\equiv 3 \mod 5\,, \\ 6 &\equiv 1 \mod 5\,, \\ 9 &\equiv 4 \mod 5\,, \\ 12 &\equiv 2 \mod 5\,. \end{aligned}$$

Lösen einer Gleichung modulo n

Satz 6.17. *Sei $n \in \mathbb{N}_{\geqslant 1}$ und sei $a \in \mathbb{Z} \setminus \{0\}$.*

[1] Wir schreiben $a \nmid b$ um auszudrücken, dass a *kein* Teiler von b ist, d.h. dass *nicht* gilt: $a \mid b$.

(a) Wenn $\mathrm{ggT}(a,n) = 1$ *ist, dann gilt für jedes* $b \in \mathbb{Z}$*: Die Gleichung*

$$ax \equiv b \mod n$$

besitzt eine eindeutig bestimmte Lösung $x \in \mathbb{Z}_n$*.*

(b) Die Gleichung

$$ax \equiv 1 \mod n$$

besitzt genau dann eine Lösung $x \in \mathbb{Z}_n$*, wenn* $\mathrm{ggT}(a,n) = 1$ *ist.*

Falls $\mathrm{ggT}(a,n) = 1$ ist, so wird die (eindeutig bestimmte) Zahl $a' \in \mathbb{Z}_n$ mit $aa' \equiv 1 \mod n$ *multiplikatives Inverses von* a *modulo* n genannt und mit $a^{-1} \mod n$ bezeichnet.

Beweis. (a): Gemäß der Voraussetzung gilt: $\mathrm{ggT}(a,n) = 1$.
Gemäß Lemma 6.15 ist $a\mathbb{Z}_n$ eine Repräsentantenmenge modulo n. Somit gibt es ein $B \in a\mathbb{Z}_n$, so dass $B \equiv b \mod n$. Wegen $B \in a\mathbb{Z}_n$ gibt es ein $x \in \mathbb{Z}_n = \{0, \ldots, n-1\}$, so dass $B = ax$.
Somit ist $x \in \mathbb{Z}_n$ eine Lösung der Gleichung $ax \equiv b \mod n$.

Angenommen, diese Gleichung besitzt eine weitere Lösung $x' \in \mathbb{Z}_n$. Dann gilt: $ax \equiv ax' \mod n$. Gemäß der Kürzungsregel gilt dann: $x \equiv x' \mod n$. Wegen $x, x' \in \mathbb{Z}_n = \{0, \ldots, n-1\}$ ist dann $x = x'$. Somit ist die Lösung eindeutig.

(b): Falls $\mathrm{ggT}(a,n) = 1$ ist, so können wir (a) für $b := 1$ anwenden und erhalten, dass die Gleichung $ax \equiv 1 \mod n$ eine eindeutig bestimmte Lösung besitzt.

Betrachte nun den Fall, dass $\mathrm{ggT}(a,n) \neq 1$ *ist.* Dann ist $t := \mathrm{ggT}(a,n) \geqslant 2$.
Angenommen, es gäbe ein $x \in \mathbb{Z}_n$, so dass $ax \equiv 1 \mod n$. Dann gilt: $n \mid ax-1$. Und wegen $t \mid n$ gilt dann auch: $t \mid ax-1$.
Wegen $t \mid a$ folgt dann gemäß Bemerkung 6.4(d): $t \mid -1$. Aber dann muss gelten: $t = 1$. *Widerspruch.* □

Folie 332

Beispiel 6.18. Löse die Gleichung

$$2x \equiv 3 \mod 7\,.$$

Wir nutzen Satz 6.17 für $n = 7$ und $a = 2$.
Wegen $\mathrm{ggT}(n,a) = 1$ erhalten wir, dass die Gleichung eine eindeutige Lösung $x \in \mathbb{Z}_7$ besitzt.

Zum Finden der Lösung betrachten wir die folgende Tabelle:

$x \in \mathbb{Z}_7$	$2x$	Rest von $2x$ modulo 7
0	0	0
1	2	2
2	4	4
3	6	6
4	8	1
5	10	3
6	12	5

Somit löst $x := 5$ die Gleichung $2x \equiv 3 \mod 7$.

Euklidischer Algorithmus

Folie 333

Effizientes Berechnen von ggT(a, b)

Um bei gegebenen Zahlen $a, b \in \mathbb{N}_{\geqslant 1}$ den größten gemeinsamen Teiler $\mathrm{ggT}(a, b)$ zu berechnen, kann man das folgende Verfahren verwenden.

Euklidischer Algorithmus
Eingabe: $a, b \in \mathbb{N}$ mit $a > b \geqslant 1$.
Ausgabe: $\mathrm{ggT}(a, b)$

1. Sei $x := a$, sei $y := b$ und sei r der Rest von x modulo y.
2. Falls $r = 0$, so STOPP mit Ausgabe y.
3. Falls $r \neq 0$, so setze $x := y$, $y := r$ und sei r der Rest von x modulo y.
4. Mach weiter in Zeile 2.

Die Korrektheit des Algorithmus (also die Tatsache, dass die vom Algorithmus ausgegebene Zahl tatsächlich $\mathrm{ggT}(a, b)$ ist), folgt aus den beiden folgenden Fakten:

- Wenn $y \mid x$, so ist $\mathrm{ggT}(x, y) = y$.

- Wenn $x = qy + r$ für ein $q \in \mathbb{Z}$, so ist $\text{ggT}(x, y) = \text{ggT}(y, r)$.

  Beweis: Sei $t := \text{ggT}(x, y)$ und $t' := \text{ggT}(y, r)$.

  Wegen $t \mid x$ und $t \mid y$ und $x = qy + r$ folgt: $t \mid r$.

  Somit gilt: $t \mid y$ und $t \mid r$. Also: $t \mid \text{ggT}(y, r) = t'$.

  Andererseits gilt wegen $t' \mid y$ und $t' \mid r$ und $x = qy + r$ auch: $t' \mid x$.
  Somit gilt: $t' \mid x$ und $t' \mid y$. Also: $t' \mid \text{ggT}(x, y) = t$.

  Wir haben gezeigt: $t \mid t'$ und $t' \mid t$. Wegen $t, t' \geqslant 1$ folgt: $t = t'$. □

Folie 334

Beispiel 6.19. Wir wenden den Euklisischen Algorithmus an, um Folgendes zu berechnen:

(a) $\text{ggT}(348, 124)$.

$$\begin{array}{rcll} 348 & = & 2 \cdot 124 + 100 & \text{also: } x = 348,\ y = 124,\ r = 100 \\ 124 & = & 1 \cdot 100 + 24 & \text{also: } x = 124,\ y = 100,\ r = 24 \\ 100 & = & 4 \cdot 24 + 4 & \text{also: } x = 100,\ y = 24,\ r = 4 \\ 24 & = & 6 \cdot 4 + 0 & \text{also: } x = 24,\ y = 4,\ r = 0 \end{array}$$

Dies liefert die Ausgabe 4, d.h.: $\text{ggT}(348, 124) = 4$.

(b) $\text{ggT}(4864, 3458)$.

$$\begin{array}{rcll} 4864 & = & 1 \cdot 3458 + 1406 & \text{also: } x = 4864,\ y = 3458,\ r = 1406 \\ 3458 & = & 2 \cdot 1406 + 646 & \text{also: } x = 3458,\ y = 1406,\ r = 646 \\ 1406 & = & 2 \cdot 646 + 114 & \text{also: } x = 1406,\ y = 646,\ r = 114 \\ 646 & = & 5 \cdot 114 + 76 & \text{also: } x = 646,\ y = 114,\ r = 76 \\ 114 & = & 1 \cdot 76 + 38 & \text{also: } x = 114,\ y = 76,\ r = 38 \\ 76 & = & 2 \cdot 38 + 0 & \text{also: } x = 76,\ y = 38,\ r = 0 \end{array}$$

Dies liefert die Ausgabe 38, d.h.: $\text{ggT}(4864, 3458) = 38$.

Primzahlen

Satz 6.20 (*Fundamentalsatz der Arithmetik*)**.**
Für jede Zahl $n \in \mathbb{N}$ mit $n \geqslant 2$ gibt es eine eindeutige Primfaktorzerlegung, d.h. es gibt eindeutig bestimmte Zahlen $k \in \mathbb{N}_{\geqslant 1}$, Primzahlen $p_1 < \cdots < p_k$ und Zahlen $s_1, \ldots, s_k \in \mathbb{N}_{\geqslant 1}$, so dass

$$n \quad = \quad p_1^{s_1} \cdots p_k^{s_k} \, .$$

Beweis.

Schritt 1: Zunächst beweisen wir per Induktion nach n, dass jedes $n \in \mathbb{N}$ mit $n \geqslant 2$ eine Primfaktorzerlegung besitzt.

Induktionsanfang: $n = 2$.
Wir wählen $k = 1$, $p_1 = 2$ und $s_1 = 1$. Es gilt: $n = 2 = p_1^{s_1}$.

Induktionsschritt: $n \to n{+}1$. Sei $n \geqslant 2$ beliebig.

Induktionsannahme: Jedes $n' \in \mathbb{N}$ mit $2 \leqslant n' \leqslant n$ besitzt eine Primfaktorzerlegung.

Behauptung: $n{+}1$ besitzt eine Primfaktorzerlegung.

Beweis: Falls $n{+}1$ eine Primzahl ist, so wählen wir $k = 1$, $p_1 = n{+}1$ und $s_1 = 1$ und sind fertig, da $n{+}1 = p_1^{s_1}$ ist.
Falls $n{+}1$ keine Primzahl ist, so gibt es Zahlen $a, b \in \mathbb{N}$ mit $a, b \geqslant 2$, so dass $n{+}1 = ab$ ist. Insbesondere gilt dann: $a, b < n{+}1$.
Gemäß der Induktionsannahme besitzt jede der Zahlen a und b eine Primfaktorzerlegung. Daraus erhalten wir eine Primfaktorzerlegung des ab, also der Zahl $n{+}1$. $\square_{\text{Schritt 1}}$

Schritt 2: Sein nun $n \in \mathbb{N}$ mit $n \geqslant 2$ beliebig gewählt. Gemäß Schritt 1 besitzt n eine Primfaktorzerlegung, d.h. es gibt eine Zahl $k \in \mathbb{N}_{\geqslant 1}$, Primzahlen $p_1 < \cdots < p_k$ und Zahlen $s_1, \ldots, s_k \in \mathbb{N}_{\geqslant 1}$, so dass $n = p_1^{s_1} \cdots p_k^{s_k}$.
Angenommen es gäbe eine weitere Primfaktorzerlegung von n, d.h. eine Zahl $\ell \in \mathbb{N}_{\geqslant 1}$, Primzahlen $q_1 < \cdots < q_\ell$ und Zahlen $t_1, \ldots, t_\ell \in \mathbb{N}_{\geqslant 1}$, so dass $n = q_1^{t_1} \cdots q_\ell^{t_\ell}$ ist.
O.B.d.A. betrachten wir den Fall, dass $k \leqslant \ell$ ist.

Per Induktion nach j kann man für alle $j \in [k]$ zeigen, dass $p_j = q_j$ und $s_j = t_j$ gilt. *Details: Übungsaufgabe.*
Dann gilt also:

$$1 \quad = \quad \frac{n}{n} \quad = \quad \frac{q_1^{t_1} \cdots q_\ell^{t_\ell}}{p_1^{s_1} \cdots p_k^{s_k}} \quad = \quad \prod_{i=k+1}^{\ell} q_i^{t_i},$$

und daher muss gelten: $k = \ell$. Somit ist die Primfaktorzerlegung eindeutig. □

Satz 6.21 (*Kleiner Satz von Fermat*)**.**
Für jede Primzahl p und jedes $a \in \mathbb{N}$ gilt:

$$a^p \equiv a \mod p\,.$$

Falls $p \nmid a$, so gilt insbesondere:

$$a^{p-1} \equiv 1 \mod p\,.$$

Beweis. Wir führen den Beweis per Induktion nach a.

Induktionsanfang: $a = 0$.
Offensichtlicherweise gilt: $0^0 = 0 \equiv 0 \mod p$.

Induktionsschritt: $a \to a{+}1$.

Induktionsannahme: $a^p \equiv a \mod p$.
Behauptung: $(a{+}1)^p \equiv a{+}1 \mod p$.
Beweis: Wir nutzen die binomische Formel:

$$(a{+}1)^p \;=\; \sum_{k=0}^{p} \tbinom{p}{k} \cdot a^k \cdot 1^{p-k} \;=\; \tbinom{p}{0} \cdot a^0 \;+\; \tbinom{p}{p} \cdot a^p \;+\; \sum_{k=1}^{p-1} \tbinom{p}{k} \cdot a^k\,.$$

Gemäß Satz 6.13(b) gilt $p \mid \binom{p}{k}$ für alle k mit $1 \leqslant k < p$.
Somit gilt: $\sum_{k=1}^{p-1} \binom{p}{k} \cdot a^k \equiv 0 \mod p$.
Außerdem gilt: $\binom{p}{0} = 1 = \binom{p}{p}$ und $a^0 = 1$.
Somit gilt:

$$(a{+}1)^p \equiv 1 + a^p \mod p\,.$$

Gemäß der Induktionsannahme ist $a^p \equiv a \mod p$. Daher gilt:
$1 + a^p \equiv 1 + a \mod p$. Somit erhalten wir: $(a{+}1)^p \equiv a{+}1 \mod p$.
Dies beendet den Induktionsbeweis.

Für denn Fall, dass $p \nmid a$ gilt, müssen wir noch zeigen, dass $a^{p-1} \equiv 1 \mod p$ ist. Gemäß dem gerade bereits Gezeigten gilt: $a^p \equiv a \mod p$.
Wegen $p \nmid a$ und da p eine Primzahl ist, gilt: $\mathrm{ggT}(p, a) = 1$. Wir wenden die Kürzungsregel (Bemerkung 6.14) an für $x := a^{p-1}$ und $y := 1$. Wegen $a^p \equiv a \mod p$ gilt also: $ax \equiv ay \mod p$. Die Kürzungsregel liefert:
$x \equiv y \mod p$, d.h. $a^{p-1} \equiv 1 \mod p$. □

Der Chinesische Restsatz

Satz 6.22 (*Chinesischer Restsatz*)**.**
Sei $k \in \mathbb{N}_{\geqslant 1}$*, seien* $m_1, \ldots, m_k \in \mathbb{N}_{\geqslant 1}$ *mit* $\text{ggT}(m_i, m_j) = 1$ *für alle* $i, j \in [k]$ *mit* $i \neq j$*, und sei* $n := \prod_{i=1}^{k} m_i$*.*
Seien $a_1, \ldots, a_k \in \mathbb{Z}$ *beliebig. Es gibt ein eindeutig bestimmtes* $x \in \mathbb{Z}_n$*, so dass*

$$x \equiv a_i \mod m_i \quad \text{für alle } i \in [k].$$

Beweis. Für jedes $i \in [k]$ setze $n_i := \frac{n}{m_i}$; d.h.: $n = m_i \cdot n_i$.
Aus der Voraussetzung folgt: $\text{ggT}(m_i, n_i) = 1$. Wir wenden Satz 6.17(b) an (für $a := n_i$, $n := m_i$) und erhalten das *multiplikative Inverse* n_i^{-1} von n_i *modulo* m_i, d.h. es gilt: $n_i^{-1} \in \mathbb{Z}_{m_i}$ und $n_i \cdot n_i^{-1} \equiv 1 \mod m_i$.
Wir setzen

$$X := \sum_{i=1}^{k} a_i n_i n_i^{-1}.$$

Behauptung: Für alle $i \in [k]$ gilt: $X \equiv a_i \mod m_i$.

Beweis: Betrachte ein beliebiges $i \in [k]$.
Wegen $m_i \mid n_j$ für alle $j \in [k] \setminus \{i\}$ gilt: $X \equiv a_i n_i n_i^{-1} \mod m_i$.
Da n_i^{-1} das multiplikative Inverse von n_i modulo m_i ist, folgt:
$X \equiv a_i \mod m_i$. $\square_{\text{Beh.}}$

Wir wählen nun $x \in \mathbb{Z}_n$, so dass $x \equiv X \mod n$. Wegen $m_i \mid n$ folgt aus der obigen Behauptung, dass $x \equiv a_i \mod m_i$ gilt (für alle $i \in [k]$).

Wir müssen nur noch zeigen, dass dieses x eindeutig bestimmt ist.
Angenommen, es gibt ein weiteres $x' \in \mathbb{Z}_n$, so dass $x' \equiv a_i \mod m_i$ für alle $i \in [k]$ gilt.
Dann gilt für alle $i \in [k]$: $x - x' \equiv a_i - a_i \mod m_i$, d.h. $x - x' \equiv 0 \mod m_i$, also gilt: $m_i \mid (x - x')$.
Da die Zahlen $m_1, \ldots, m_k$ paarweise teilerfremd sind und $n = \prod_{i=1}^{k} m_i$ ist, folgt aus dem Fundamentalsatz der Arithmetik (Satz 6.20): $n \mid (x - x')$, d.h. $x \equiv x' \mod n$. Wegen $x, x' \in \mathbb{Z}_n = \{0, \ldots, n-1\}$ muss dann gelten:
$x = x'$. $\square$

Anwendung des Chinesischen Restsatzes

Der Chinesische Restsatz ermöglicht es, eine große Zahl durch mehrere kleinere Zahlen eindeutig zu repräsentieren.

Seien p_1 und p_2 zwei große Primzahlen mit $p_1 \neq p_2$. Sei $n := p_1 \cdot p_2$.
Eine Zahl $z \in \mathbb{N}$ mit $0 \leqslant z < n$ können wir durch das Tupel (a_1, a_2) repräsentieren, wobei a_i der Rest von z modulo p_i sei, für jedes $i \in [2]$.

Es gilt nämlich für $x := z$, dass $x \equiv a_i \mod p_i$ für jedes $i \in [2]$; und gemäß der Aussage des Chinesischen Restsatzes gibt es kein weiteres $x \neq z$ mit $x \in \mathbb{Z}_n$ und $x \equiv a_i \mod p_i$ für jedes $i \in [2]$.

Dieses Prinzip wird im folgenden Satz verallgemeinert:

Satz 6.23 (Fingerabdrucksatz)**.** *Sei $k \in \mathbb{N}_{\geqslant 1}$, seien $p_1 \ldots, p_k$ paarweise verschiedene Primzahlen und sei $n := \prod_{i=1}^{k} p_i$. Für alle $a, b \in \mathbb{Z}_n$ gilt:*

$$a \equiv b \mod p_i \quad \text{für alle } i \in [k] \qquad \Longleftrightarrow \qquad a = b\,.$$

Somit können wir $b \in \mathbb{Z}_n$ eindeutig aus seinem „Fingerabdruck“ $(b_1, \ldots, b_k)$ rekonstruieren, wobei b_i der Rest von b modulo p_i ist, für jedes $i \in [k]$.

Beweis. Die Richtung „$\Longleftarrow$“ ist offensichtlich.
Für die Richtung „$\Longrightarrow$“ nutzen wir den Chinesischen Restsatz für $a_i := b$ und $m_i := p_i$ für alle $i \in [k]$. Gemäß Aussage des Chinesischen Restsatzes gibt es ein eindeutig bestimmtes $x \in \mathbb{Z}_n$, so dass $x \equiv b \mod p_i$ für alle $i \in [k]$ gilt. Da sowohl $x = a$ also auch $x = b$ Lösungen für alle $i \in [k]$ sind, muss gelten: $a = b$. □

Anwendung in der Kryptographie: RSA-Verfahren

RSA-Verschlüsselung

Beim *RSA-Verfahren*[2] handelt es sich um ein asymmetrisches kryptographisches Verfahren, mit dem man Nachrichten sowohl verschlüsseln als auch digital signieren kann.
„Asymmetrisch“ bedeutet, dass es einen geheimen Schlüssel und einen öffentlichen Schlüssel gibt.

[2] benannt nach seinen Erfindern Rivest, Shamir, Adleman

Um für mich selbst solche Schlüssel zu erhalten, wähle ich zwei sehr große Primzahlen p_1 und p_2 mit $p_1 \neq p_2$ und setze $n := p_1 \cdot p_2$.
Die Zahl n *gebe ich öffentlich bekannt*; die beiden Primzahlen p_1, p_2 *halte ich geheim.*
Nachrichten, die man verschlüsselt an mich schicken kann, sind Zahlen in $\mathbb{Z}_n$.
Ich berechne die Zahl $m := (p_1-1) \cdot (p_2-1)$ (die ich geheim halte) und wähle eine kleine Zahl k, die teilerfremd ist zu m (d.h.: $\text{ggT}(k, m) = 1$). Diese Zahl k gebe ich als meinen *„öffentlichen Schlüssel"* (engl.: public key) bekannt.
Ich berechne *das multiplikative Inverse* $\ell := k^{-1}$ *von* k *modulo* m und halte dieses als meinen *„privaten Schlüssel" geheim.*

Wenn jemand mir eine verschlüsselte Nachricht x schicken will, berechnet er den Rest y von x^k modulo n und schickt mir die Zahl y zu.

Um y zu entschlüsseln, berechne ich den Rest r von y^ℓ modulo n.

Behauptung: $r = x$.

Beweis. Gemäß dem Fingerabdrucksatz (Satz 6.23) genügt es zu zeigen, dass $r \equiv x \mod p_i$ für jedes $i \in [2]$ gilt.
Wir betrachten p_1 (für p_2 folgt die Aussage analog).
Wegen $p_1 \mid n$ und $y \equiv x^k \mod n$ gilt: $y \equiv x^k \mod p_1$. Daher gilt auch: $y^\ell \equiv x^{k\ell} \mod p_1$, d.h. $r \equiv x^{k\ell} \mod p_1$.
Fall 1: $p_1 \mid x$.
Dann gilt auch: $p_1 \mid (x^{k\ell} - x)$, d.h. $x^{k\ell} \equiv x \mod p_1$. Somit gilt: $r \equiv x \mod p_1$.
Fall 2: $p_1 \nmid x$.
Dann folgt aus dem kleinen Satz von Fermat (Satz 6.21): $x^{p_1-1} \equiv 1 \mod p_1$.
Gemäß unserer Wahl von k und ℓ gilt: $k \cdot \ell \equiv 1 \mod m$. Somit gilt: $m \mid (k \cdot \ell - 1)$, d.h. es gibt ein $c \in \mathbb{Z}$, so dass $k \cdot \ell - 1 = c \cdot m = c \cdot (p_1-1) \cdot (p_2-1)$.
Somit gilt: $x^{k\ell-1} = x^{c \cdot m} = \left(x^{p_1-1}\right)^{c \cdot (p_2-1)}$.
Wegen $x^{p_1-1} \equiv 1 \mod p_1$ folgt also: $x^{k\ell-1} \equiv 1^{c \cdot (p_2-1)} \mod p_1$, d.h. $x^{k\ell-1} \equiv 1 \mod p_1$. Daher ist $x^{k\ell} \equiv x \mod p_1$, d.h. $r \equiv x \mod p_1$. □

Folie 340

RSA-Signierung

Falls ich jemandem eine Nachricht $x \in \mathbb{Z}_n$ schicken will, kann ich diese mit einer „Signatur" versehen, so dass der Empfänger sicher sein kann, dass die Nachricht tatsächlich von mir stammt. Dazu kann ich wie folgt vorgehen:

Ich berechne den Rest z von x^ℓ modulo n und schicke dem Empfänger die Zahlen x und z.
Der Empfänger berechnet den Rest r von z^k modulo n und überprüft, ob $r = x$ ist. Falls ja, kann er davon ausgehen, dass die Nachricht tatsächlich von mir an ihn geschickt worden ist.

Behauptung: $r = x$.

Beweis. Es gilt: $r \equiv z^k \mod n$ und $z \equiv x^\ell \mod n$. Also gilt: $r \equiv x^{k\ell} \mod n$.
Wir sind also genau in derselben Situation wie oben bei der RSA-Verschlüsselung. Dort haben wir bereits gezeigt, dass $r = x$ ist. □

6.2 Gruppen, Ringe und Körper

Gruppen

Folie 341

Verknüpfungen

Definition 6.24. Sei M eine Menge.

(a) Eine *Verknüpfung* auf M ist eine Abbildung $\circ : M \times M \to M$.

Für $a, b \in M$ schreiben wir statt $\circ(a, b)$ oft $a \circ b$. Insbesondere bedeutet $(a \circ b) \circ c$ dann: $\circ(\circ(a, b), c)$.

(b) Eine Verknüpfung $\circ$ auf M heißt *assoziativ*, wenn für alle $a, b, c \in M$ gilt: $(a \circ b) \circ c = a \circ (b \circ c)$.

(c) Eine Verknüfung $\circ$ auf M heißt *kommutativ*, wenn für alle $a, b \in M$ gilt: $a \circ b = b \circ a$.

Beispiel: Betrachte $M := \mathbb{Q}$ und die Verknüfung

- $+$ (Addition auf $\mathbb{Q}$): diese Verknüpfung ist assoziativ und kommutativ
- $-$ (Subtraktion auf $\mathbb{Q}$): diese Verknüpfung ist nicht assoziativ (denn: $(2-3)-4 = -1-4 = -5$, aber $2-(3-4) = 2-(-1) = 3$) und nicht kommutativ (denn: $2-3 = -1$, aber $3-2 = 1$)

- $\cdot$ (Multiplikation auf $\mathbb{Q}$): diese Verknüpfung ist assoziativ und kommutativ
- $:$ (Division auf $\mathbb{Q}$): diese Verknüpfung ist nicht assoziativ (denn: $(18 : 3) : 3 = 6 : 3 = 2$, aber $18 : (3 : 3) = 18 : 1 = 18$) und nicht kommutativ (denn: $2 : 1 = 2$, aber $1 : 2 = \frac{1}{2}$)

Folie 342

Halbgruppen, Monoide und neutrale Elemente

Definition 6.25. Sei M eine Menge und sei $\circ$ eine Verknüpfung auf M.

(a) $(M, \circ)$ ist eine *Halbgruppe*, falls $\circ$ assoziativ ist.

$(M, \circ)$ ist eine *kommutative Halbgruppe*, falls $\circ$ assoziativ und kommutativ ist.

(b) Ein *neutrales Element* für $(M, \circ)$ ist ein $e \in M$, so dass für alle $a \in M$ gilt: $a \circ e = e \circ a = a$.

(c) $(M, \circ)$ ist ein *Monoid*, falls $(M, \circ)$ eine Halbgruppe ist, die ein neutrales Element besitzt.

Ein *kommutatives Monoid* ist eine kommutative Halbgruppe, die ein neutrales Element besitzt.

Bemerkung 6.26. Sei M eine Menge und sei $\circ$ eine Verknüpfung auf M. Wenn $(M, \circ)$ ein neutrales Element besitzt, so ist dieses eindeutig bestimmt.

Beweis: Seien e und e' neutrale Elemente für $(M, \circ)$. Dann gilt für alle $a \in M$: $a \circ e = e \circ a = a = a \circ e' = e' \circ a$.
Indem wir $a := e'$ wählen, erhalten wir: $e' \circ e = e'$.
Indem wir $a := e$ wählen, erhalten wir: $e = e' \circ e$.
Somit gilt: $e = e'$. □

Folie 343

Beispiele 6.27.

(a) Sei Σ ein Alphabet (d.h. eine nicht-leere Menge).

Sei $\circ$ die *Konkatenation* auf Σ^*, d.h. für alle Worte $v, w \in \Sigma^*$ ist $v \circ w$ das Wort vw.

Dann ist $(\Sigma^*, \circ)$ ein Monoid, dessen neutrales Element e das leere Wort ε ist. Falls $|\Sigma| \geqslant 2$ ist, so ist diese Monoid *nicht* kommutativ.

(b) Betrachte $\mathbb{N}$ mit der Verknüpfung

- $+$ (Addition auf $\mathbb{N}$): Dann ist $(\mathbb{N}, +)$ ein kommutatives Monoid, dessen neutrales Element e die Zahl 0 ist.
- $\cdot$ (Multiplikation auf $\mathbb{N}$): Dann ist $(\mathbb{N}, \cdot)$ ein kommutatives Monoid, dessen neutrales Element e die Zahl 1 ist.

(c) Betrachte $\mathbb{N}_{\geqslant 1}$ mit der Verknüpfung $+$ (Addition): Dann ist $(\mathbb{N}_{\geqslant 1}, +)$ eine kommutative Halbgruppe, die kein neutrales Element besitzt.

Folie 344

Inverse Elemente und Gruppen

Definition 6.28. Sei $(M, \circ)$ ein Monoid und sei e dessen neutrales Element. Ein *Inverses* von $a \in M$ ist ein $a' \in M$, so dass gilt: $a \circ a' = e = a' \circ a$.

Bemerkung 6.29. Sei $(M, \circ)$ ein Monoid. Wenn ein $a \in M$ ein Inverses besitzt, so ist dieses eindeutig bestimmt.

Beweis: Sei e das neutrale Element des Monoids $(M, \circ)$. Seien $a', a'' \in M$ Inverse von a. Dann gilt: $a \circ a' = e = a' \circ a$ und $a \circ a'' = e = a'' \circ a$.
Somit gilt: $(a'' \circ a) \circ a' = e \circ a' = a'$. Und es gilt:
$(a'' \circ a) \circ a' = a'' \circ (a \circ a') = a'' \circ e = a''$. Somit gilt: $a' = a''$. □

Definition 6.30. Eine *Gruppe* ist ein Monoid $(M, \circ)$, bei dem jedes Element $a \in M$ ein Inverses besitzt.

D.h.: M ist eine Menge und $\circ$ ist eine Verknüpfung auf M, für die gilt:

(1) $\circ$ ist assoziativ, d.h. für alle $a, b, c \in M$ gilt: $(a \circ b) \circ c = a \circ (b \circ c)$,

(2) $(M, \circ)$ besitzt ein neutrales Element e, d.h.: $e \in M$ und für alle $a \in M$ gilt: $a \circ e = e \circ a = a$, und

(3) jedes $a \in M$ besitzt ein Inverses, d.h. es gibt ein $a' \in M$, so dass $a \circ a' = a' \circ a = e$.

Definition 6.31. Eine *kommutative Gruppe* bzw. *abelsche Gruppe* ist eine Gruppe $(M, \circ)$, deren Verknüpfung $\circ$ kommutativ ist.

Beispiele 6.32.

(a) $(\mathbb{N}, +)$ ist keine Gruppe, da kein $n \in \mathbb{N}$ mit $n \neq 0$ ein Inverses besitzt.

(b) $(\mathbb{Z}, +)$ ist eine abelsche Gruppe mit neutralem Element 0; für jedes $z \in \mathbb{Z}$ gilt: das Inverse von z ist die Zahl $(-1) \cdot z$.

(c) $(\mathbb{Z} \setminus \{0\}, \cdot)$ ist ein kommutatives Monoid mit neutralem Element 1; aber keine Gruppe, da z.B. die Zahl $2 \in \mathbb{Z}$ kein Inverses besitzt.

(d) $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1; für jedes $q \in \mathbb{Q}$ gilt: das Inverse von q ist die Zahl $\frac{1}{q}$.

(e) $(\mathbb{Q}, \cdot)$ ist keine Gruppe, da die Zahl 0 kein Inverses besitzt, denn es gibt kein $q \in \mathbb{Q}$, so dass $0 \cdot q = 1$.

Die *symmetrische Gruppe* S_n

Beispiel 6.33. Sei $n \in \mathbb{N}_{\geqslant 1}$ und betrachte die Menge $[n] = \{1, \ldots, n\}$.
Sei S_n die Menge aller Permutationen von $[n]$, d.h. die Menge aller bijektiven Abbildungen $f : [n] \to [n]$.
Für alle $f, g \in S_n$ sei $f \circ g$ die Abbildung $h : [n] \to [n]$ mit $h(i) := f(g(i))$ für alle $i \in [n]$. Da f und g bijektiv sind, ist auch h bijektiv.
Somit ist $\circ$ eine Verknüpfung auf S_n.

Behauptung: $(S_n, \circ)$ ist eine Gruppe.

Beweis: Man kann leicht nachrechnen, dass $\circ$ assoziativ ist, dass die Identitätsfunktion $\mathrm{id}_{[n]}$ das neutrale Element von $(S_n, \circ)$ ist, und dass für jedes $f \in S_n$ gilt: das Inverse von f ist die *Umkehrabbildung* f^{-1} mit $f^{-1}(j) = i$ für alle $j \in [n]$ und dasjenige $i \in [n]$ mit $f(i) = j$. Details: Übungsaufgabe. □

Die Gruppe $(S_n, \circ)$ wird die *symmetrische Gruppe* S_n genannt. Es gilt: $|S_n| = n!$. Für $n \geqslant 3$ ist die symmetrische Gruppe S_n ist nicht kommutativ, denn: Sei $f \in S_n$ mit $f(1) = 2$, $f(2) = 3$ und $f(3) = 1$ — wir schreiben dafür kurz: $f = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$. Sei $g = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$, d.h. $g(1) = 3$, $g(2) = 2$ und $g(3) = 1$. Dann ist $f \circ g \neq g \circ f$, denn $(f \circ g)(2) = f(g(2)) = f(2) = 3$ und $(g \circ f)(2) = g(f(2)) = g(3) = 1$, also $(f \circ g)(2) \neq (g \circ f)(2)$, also $f \circ g \neq g \circ f$.

Verknüpfungen auf $\mathbb{Z}_n$

Beispiele 6.34. Sei $n \in \mathbb{N}$ mit $n \geqslant 2$. Betrachte $\mathbb{Z}_n = \{0, \ldots, n-1\}$.

(a) Sei $+_n$ die „Addition modulo n“, d.h. für alle $a, b \in \mathbb{Z}_n$ sei $a +_n b$ der Rest der Zahl $(a+b)$ modulo n.

Dann ist $(\mathbb{Z}_n, +_n)$ eine abelsche Gruppe mit neutralem Element 0. Das Inverse von $a \in \mathbb{Z}_n \setminus \{0\}$ ist die Zahl $a' := n-a$, und das Inverse von 0 ist die Zahl 0.

(b) Sei $\cdot_n$ die „Multiplikation modulo n“, d.h. für alle $a, b \in \mathbb{Z}_n$ sei $a \cdot_n b$ der Rest der Zahl $(a \cdot b)$ modulo n.

Dann ist $(\mathbb{Z}_n, \cdot_n)$ ein kommutatives Monoid mit neutralem Element 1; aber es ist keine Gruppe, da $0 \in \mathbb{Z}_n$ kein Inverses besitzt.

(c) Sei $\mathbb{Z}_n^\times := \{a \in \mathbb{Z}_n \,:\, a \neq 0 \text{ und } \mathrm{ggT}(a, n) = 1\}$.

Dann ist $(\mathbb{Z}_n^\times, \cdot_n)$ eine abelsche Gruppe mit neutralem Element 1.

Beweis:

- $\cdot_n$ ist eine Verknüpfung auf $\mathbb{Z}_n^\times$, denn: Seien $a, b \in \mathbb{Z}_n^\times$ und sei $c := a \cdot_n b$. Zu zeigen: $c \in \mathbb{Z}_n^\times$, d.h. $\mathrm{ggT}(c, n) = 1$.
  Wegen $a, b \in \mathbb{Z}_n^\times$ gilt: $\mathrm{ggT}(a, n) = 1 = \mathrm{ggT}(b, n)$. Gemäß Satz 6.13(a) gilt: $\mathrm{ggT}(ab, n) = 1$.
  Wegen $c = a \cdot_n b$ gilt: $c \in \mathbb{Z}_n$ und $c \equiv a \cdot b \mod n$. Somit gibt es ein $k \in \mathbb{N}$, so dass $c + kn = ab$. Aus $\mathrm{ggT}(ab, n) = 1$ folgt dann: $\mathrm{ggT}(c, n) = 1$ (denn: angenommen $t := \mathrm{ggT}(c, n) \geqslant 2$, dann gilt: $t \mid c$ und $t \mid n$, also: $t \mid c+kn$, d.h. $t \mid ab$, also $t \mid \mathrm{ggT}(ab, n)$. Widerspruch zu $\mathrm{ggT}(ab, n) = 1$).
- Wir wissen bereits, dass $\cdot_n$ assoziativ und kommutativ ist, und dass 1 das neutrale Element ist. Es gilt: $1 \in \mathbb{Z}_n^\times$.
  Um zu zeigen, dass $(\mathbb{Z}_n^\times, \cdot_n)$ eine abelsche Gruppe ist, müssen wir nur noch zeigen, dass jedes $a \in \mathbb{Z}_n^\times$ ein Inverses besitzt, d.h. dass es ein $x \in \mathbb{Z}_n^\times$ gibt, so dass $a \cdot_n x = 1$ ist.
  Da $\mathrm{ggT}(a, n) = 1$ ist, erhalten wir von Satz 6.17(b), dass es ein $x \in \mathbb{Z}_n$ gibt, so dass $ax \equiv 1 \mod n$ ist. Indem wir nochmals Satz 6.17(b) anwenden und dabei die Rollen von a und x vertauschen, erhalten wir aus der Gleichung $xa \equiv 1 \mod n$, dass $\mathrm{ggT}(x, n) = 1$ ist. Also ist $x \in \mathbb{Z}_n^\times$. □

Eigenschaften von Gruppen

Bemerkung 6.35. Sei $(G, \circ)$ eine Gruppe. Wir wissen bereits, dass es genau ein neutrales Element $e \in G$ gibt und dass es für jedes $g \in G$ genau ein Inverses gibt; wir schreiben im Folgenden g^{-1} um das Inverse von g zu bezeichnen.
Folgende Sachverhalte lassen sich leicht beweisen (Details: Übungsaufgabe):

1. Für alle $g \in G$ gilt: $(g^{-1})^{-1} = g$.
2. Für alle $g, h \in G$ gilt: $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$.

   Man beachte die vertauschte Reihenfolge! Eselsbrücke, um sich dies zu merken: Sei h die Operation „ziehe die Socken an“ und sei g die Operation „ziehe die Schuhe an“. Dann ist $g \circ h$ die Operation „ziehe erst die Socken und dann die Schuhe an“. Das Inverse $(g \circ h)^{-1}$ soll die Operation $g \circ h$ rückgängig machen; dies erreichen wir, indem wir zuerst die Schuhe ausziehen (dies entspricht g^{-1}) und dann die Socken ausziehen (dies entspricht h^{-1}) — also die Operation $h^{-1} \circ g^{-1}$ anwenden. Somit gilt: $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$.
3. *Kürzungsregel*: Für alle $a, b, c \in G$ gilt:
   Wenn $a \circ b = a \circ c$, dann $b = c$. Wenn $b \circ a = c \circ a$, dann $b = c$.

4. Für alle $a, b \in G$ gilt:

   - Die Gleichung $a \circ x = b$ ist eindeutig lösbar, d.h. es gibt genau ein $x \in G$ so dass $a \circ x = b$ ist.

     Beweis: Für $x := a^{-1} \circ b$ gilt:
     $a \circ x = a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$. Die Eindeutigkeit von x folgt dann aus der Kürzungsregel. □

   - Die Gleichung $y \circ a = b$ ist eindeutig lösbar, d.h. es gibt genau ein $y \in G$ so dass $y \circ a = b$ ist.

     Beweis: Für $y := b \circ a^{-1}$ gilt:
     $y \circ a = (b \circ a^{-1}) \circ a = b \circ (a^{-1} \circ a) = b \circ e = b$. Die Eindeutigkeit von y folgt dann aus der Kürzungsregel. □

Untergruppen und Nebenklassen

Definition 6.36. Sei $(G, \circ)$ eine Gruppe und sei $U \subseteq G$.

(a) U ist eine *Untergruppe* von $(G, \circ)$, wenn gilt: U ist abgeschlossen unter der Verknüpfung $\circ$ (d.h. für alle $a, b \in U$ ist $a \circ b \in U$), U enthält das neutrale Element e von $(G, \circ)$ und für jedes $a \in U$ enthält U das Inverse a^{-1} von a in $(G, \circ)$.

(b) Für jedes $a \in G$ setze

$$\begin{aligned} a \circ U &:= \{a \circ u : u \in U\} \qquad \text{und} \\ U \circ a &:= \{u \circ a : u \in U\}. \end{aligned}$$

$a \circ U$ wird *Linksnebenklasse* (von U bzgl. a) genannt;
$U \circ a$ heißt *Rechtsnebenklasse* (von U bzgl. a).

Beispiel 6.37. Betrachte die rationalen Zahlen $\mathbb{Q}$ mit der Verknüpfung $+$ (Addition).
Dann ist $(\mathbb{Q}, +)$ eine Gruppe und $\mathbb{Z}$ ist eine Untergruppe.
Für jedes $n \in \mathbb{N}$ mit $n \geqslant 2$ ist die Menge $n\mathbb{Z}$ ebenfalls eine Untergruppe (Beweis: Übungsaufgabe); aber die Menge $\mathbb{Z}_n$ ist keine Untergruppe (denn sie ist nicht abgeschlossen unter der Addition $+$).
Für jedes $a \in \mathbb{Z}$ ist $a + n\mathbb{Z}$ eine Linksnebenklasse von $n\mathbb{Z}$. Da $+$ kommutativ ist, ist $a + n\mathbb{Z} = n\mathbb{Z} + a$ — d.h. Links- und Rechtsnebenklassen sind gleich.

Eigenschaften von Untergruppen und Nebenklassen

Satz 6.38. *Sei $(G, \circ)$ eine Gruppe und sei $U \subseteq G$ eine Untergruppe von $(G, \circ)$.*

(a) Für jedes $a \in G$ ist die Menge $a \circ U$ gleichmächtig zur Menge U.

(b) Für alle $a, b \in G$ gilt: $a \circ U = b \circ U$ oder $a \circ U \cap b \circ U = \emptyset$.

(c) Es gibt eine Menge $A \subseteq G$ so dass gilt: $G = \bigcup_{a \in A} a \circ U$, und die Mengen $a \circ U$ für $a \in A$ sind paarweise disjunkt.

Beweis. (a): Betrachte die Abbildung $f : U \to a \circ U$ mit $f(u) := a \circ u$ für alle $u \in U$. Gemäß der Definition von $a \circ U$ ist die Abbildung f surjektiv. Die Kürzungsregel liefert, dass f injektiv ist. Somit ist f eine bijektive Abbildung von U nach $a \circ U$, und daher sind die Mengen U und $a \circ U$ gleichmächtig.

(b): Wenn $a \circ U \cap b \circ U \neq \emptyset$, dann gibt es ein $c \in a \circ U \cap b \circ U$. D.h. es gibt $u, v \in U$ so dass $c = a \circ u = b \circ v$.
Dann ist $c \circ u^{-1} = (a \circ u) \circ u^{-1} = a \circ (u \circ u^{-1}) = a$.
Und es gilt: $c \circ u^{-1} = (b \circ v) \circ u^{-1} = b \circ (v \circ u^{-1})$. Da U eine Untergruppe von $(G, \circ)$ ist, gilt: $u^{-1} \in U$ und $v \circ u^{-1} \in U$. Somit ist $b \circ (v \circ u^{-1}) \in b \circ U$.
Wegen $a = b \circ (v \circ u^{-1})$ ist also $a \in b \circ U$.
Daraus folgt: $a \circ U \subseteq b \circ U$ (denn: für jedes beliebige $w \in U$ gilt: $a \circ w = (b \circ (v \circ u^{-1})) \circ w = b \circ ((v \circ u^{-1}) \circ w) \in b \circ U$).
Analog erhält man, dass auch gilt: $b \circ U \subseteq a \circ U$. Somit ist also $a \circ U = b \circ U$.

(c): Die Relation $\sim$ mit $a \sim b \iff a \circ U = b \circ U$ (f.a. $a, b \in G$) ist eine Äquivalenzrelation auf G. Sei M die Menge der Äquivalenzklassen von $\sim$ auf G. Für jedes Element $m \in M$ wähle ein $a_m \in G$, so dass $m = \{g \in G : g \sim a_m\}$. Sei $A := \{a_m : m \in M\}$. Man kann sich leicht davon überzeugen, dass $G = \bigcup_{a \in A} a \circ U$ ist und dass die Mengen $a \circ U$ für $a \in A$ paarweise disjunkt sind (Details: Übungsaufgabe). □

Folie 353

Der Satz von Lagrange

Satz 6.39 (Satz von Lagrange)**.** *Sei $(G, \circ)$ eine endliche Gruppe*[3]*.*
Dann gilt für jede Untergruppe U von $(G, \circ)$: $|U| \,|\, |G|$
(d.h. $|G|$ ist ein ganzzahliges Vielfaches von $|U|$),
und die Anzahl der verschiedenen Linksnebenklassen von U in G ist $\frac{|G|}{|U|}$.

Beweis. Gemäß Satz 6.38 gibt es eine Menge $A \subseteq G$ so dass $G = \bigcup_{a \in A} a \circ U$ ist und die Mengen $a \circ U$ für $a \in A$ paarweise disjunkt und gleichmächtig zu U sind. Somit gilt: $|G| = \sum_{a \in A} |a \circ U| = \sum_{a \in A} |U| = |A| \cdot |U|$. □

Als einfache Folgerung aus dem Satz von Lagrange erhalten wir:

Folgerung 6.40. *Sei p eine Primzahl und sei $+_p$ die „Addition modulo p“. Die Gruppe $(\mathbb{Z}_p, +_p)$ besitzt als Untergruppen nur sich selbst und die Menge $\{0\}$, die nur aus dem neutralen Element besteht.*

[3] d.h. G ist eine endliche Menge und $(G, \circ)$ ist eine Gruppe

Ringe und Körper

Folie 354

Definition 6.41 (Ringe und Körper)**.**
Ein *Ring* $(M, \oplus, \odot)$ besteht aus einer Menge M und zwei Verknüpfungen $\oplus$ und $\odot$ auf M, so dass gilt:

1.) $(M, \oplus)$ ist eine abelsche Gruppe, und für deren neutrales Element $\mathtt{0}$ gilt:

2.) $(M \setminus \{\mathtt{0}\}, \odot)$ ist ein Monoid (d.h. $\odot$ ist assoziativ und besitzt ein neutrales Element $\mathtt{1} \in M \setminus \{\mathtt{0}\}$), und

3.) es gelten die folgenden *Distributivgesetze*: für alle $a, b, c \in M$ gilt:

$$\begin{aligned} a \odot (b \oplus c) &= (a \odot b) \oplus (a \odot c) \qquad \text{und} \\ (b \oplus c) \odot a &= (b \odot a) \oplus (c \odot a). \end{aligned}$$

Ein Ring $(M, \oplus, \odot)$ heißt *kommutativ*, wenn auch die Verknüpfung $\odot$ kommutativ ist.

Ein *Körper* ist ein Ring $(M, \oplus, \odot)$, für den $(M \setminus \{\mathtt{0}\}, \odot)$ eine abelsche Gruppe ist.

Folie 355

Beispiele 6.42.
Seien $+$ und $\cdot$ die herkömmliche Addition und Multiplikation reeller Zahlen.
Es gilt:
$(\mathbb{R}, +, \cdot)$ und $(\mathbb{Q}, +, \cdot)$ sind Körper.
$(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring, aber kein Körper (da z.B. die Zahl $2 \in \mathbb{Z} \setminus \{0\}$ kein multiplikatives Inverses in $\mathbb{Z} \setminus \{0\}$ besitzt).
$(\mathbb{N}, +, \cdot)$ ist kein Ring (da z.B. die Zahl $2 \in \mathbb{N}$ kein additives Inverses in $\mathbb{N}$ besitzt).

Folie 356

Der Restklassenring $\mathbb{Z}_n$

Bemerkung 6.43. Sei $n \in \mathbb{N}$ mit $n \geqslant 2$.
Wir betrachten $\mathbb{Z}_n$ mit den Verknüpfungen $+_n$ und $\cdot_n$ (Addition und Multiplikation modulo n).
Dann ist $(\mathbb{Z}_n, +_n, \cdot_n)$ ein kommutativer Ring (Beweis: Übungsaufgabe); er wird *Restklassenring (modulo n)* genannt.

Ist p eine Primzahl, so ist $(\mathbb{Z}_p, +_p, \cdot_p)$ ein Körper.

Beweis: Dass es ein kommutativer Ring ist, wissen wir bereits. Und aus Beispiel 6.34(c) wissen wir, dass $(\mathbb{Z}_p^\times, \cdot_p)$ eine abelsche Gruppe mit neutralem Element 1 ist. Es genügt daher, zu zeigen, dass $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ ist. Es gilt: $\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p \,:\, a \neq 0 \text{ und } \mathrm{ggT}(a,p) = 1\}$. Da p eine Primzahl ist, folgt: $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$. □

Ist $n \geqslant 2$ keine Primzahl, so ist $(\mathbb{Z}_n, +_n, \cdot_n)$ kein Körper.

Beweis: Sei $a \geqslant 2$ ein Teiler von n. Dann ist $\mathrm{ggT}(a,n) = a \neq 1$. Gemäß Satz 6.17(b) besitzt die Gleichung $ax \equiv 1 \mod n$ keine Lösung in $\mathbb{Z}_n$. Somit besitzt a kein Inverses in $(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$. Also ist $(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$ keine Gruppe. □

Folie 357

Endliche Körper

Bemerkung 6.44. Es ist Folgendes bekannt (hier ohne Beweis):

(a) Für jeden endlichen Körper $(K, \oplus, \odot)$ (d.h.: K ist eine endliche Menge und $(K, \oplus, \odot)$ ist ein Körper) gilt: Es gibt eine Primzahl p und ein $n \in \mathbb{N}_{\geqslant 1}$, so dass $|K| = p^n$ ist.

(b) Für jede Primzahl p und jedes $n \in \mathbb{N}_{\geqslant 1}$ gibt es einen endlichen Körper $(K, \oplus, \odot)$ mit $|K| = p^n$. Dieser Körper ist bis auf Isomorphie eindeutig bestimmt; er wird auch *Galoiskörper* bzw. *Galois-Feld* (engl.: Galois field) der Ordnung p^n genannt und mit $\mathrm{GF}(p^n)$ bzw $\mathbb{F}_{p^n}$ bezeichnet.

Für $n = 1$ ist $\mathrm{GF}(p)$ genau der Restklassenkörper $(\mathbb{Z}_p, +_p, \cdot_p)$.

Für $n \geqslant 2$ ist $\mathrm{GF}(p^n)$ *nicht* der Restklassenring $(\mathbb{Z}_{p^n}, +_{p^n}, \cdot_{p^n})$ (wir wissen ja bereits, dass dies kein Körper ist, da p^n keine Primzahl ist).

Folie 358

Funktionenring

Beispiel 6.45. Sei M eine nicht-leere Menge und sei $(R, \oplus, \odot)$ ein Ring. Betrachte die Menge $F := \mathrm{Abb}(M, R)$ aller Abbildungen $f : M \to R$.
Seien $\boxplus$ und $\boxdot$ die wie folgt definierten Verknüpfungen auf F:
Für alle $f, g \in F$ sei

- $f \boxplus g$ die Abbildung h in F mit $h(m) := f(m) \oplus g(m)$ für alle $m \in M$,

- $f \boxdot g$ die Abbildung h in F mit $h(m) := f(m) \odot g(m)$ für alle $m \in M$.

Dann ist $(F, \boxplus, \boxdot)$ ein Ring (Beweis: Übungsaufgabe); und F ist genau dann kommutativ, wenn R kommutativ ist.

Folie 359

Polynomring $K[x]$

Bemerkung 6.46. Sei $(K, \oplus, \odot)$ ein Körper.
Ein *Polynom* in einer Variablen x mit Koeffizienten in K ist ein Ausdruck der Form

$$\sum_{i=0}^{n} a_i x^i$$

mit $n \in \mathbb{N}$ und $a_i \in K$ für alle i mit $0 \leqslant i \leqslant n$. $K[x]$ bezeichnet die Menge all dieser Polynome.

Ein solches Polynom beschreibt die wie folgt definierte *Polynomfunktion* $f : K \to K$: für alle $b \in K$ ist $f(b)$ der Wert, den man erhält, wenn man in dem obigen Ausdruck b für x einsetzt und $a_0 b^0$ als a_0 auffasst, für jedes $i \geqslant 1$ $a_i b^i$ als $a_i \odot \underbrace{b \odot \cdots \odot b}_{i \text{ mal}}$ ausrechnet, und diese Werte für alle $i \in \{0, \ldots, n\}$ gemäß der „Addition“ $\oplus$ aufsummiert.

Folie 360

Wir definieren zwei Verknüpfungen $\boxplus$ und $\boxdot$ auf der Menge $K[x]$:

$$\sum_{i=0}^{n} a_i x^i \quad \boxplus \quad \sum_{i=0}^{m} b_i x^i \quad = \quad \sum_{i=0}^{k} c_i x^i$$

mit $k := \max\{n, m\}$ und $c_i = a_i \oplus b_i$ für alle $i \leqslant \min\{n, m\}$ und falls $m < n$ so $c_i = a_i$ für alle i mit $m < i \leqslant n$, bzw. falls $n < m$ so $c_i = b_i$ für alle i mit $n < i \leqslant m$.

$$\sum_{i=0}^{n} a_i x^i \quad \boxdot \quad \sum_{i=0}^{m} b_i x^i \quad = \quad \sum_{i=0}^{k} c_i x^i$$

mit $k := n+m$ und

$$c_i \;:=\; \bigoplus_{\substack{0 \leqslant j \leqslant n, \\ 0 \leqslant j' \leqslant m \,:\, j+j'=i}} (a_j \odot b_{j'})$$

wobei zum Aufaddieren der Summe die Operation $\oplus$ genutzt wird.

Man kann sich leicht davon überzeugen (Übungsaufgabe), dass $(K[x], \boxplus, \boxdot)$ ein kommutativer Ring ist. Dieser Ring wird *Polynomring über dem Körper* K genannt.

6.3 Literaturhinweise

Als vertiefende Lektüre seien die Kapitel 4 und 5 von [Juk08] sowie die Kapitel 3 und 5 von [Ste07] empfohlen.

Quellennachweis: Teile dieses Kapitels basieren auf Teilen der Kapitel 4 und 5 von [Juk08].

6.4 Übungsaufgaben

Aufgabe 6.1.

(I) Beweisen Sie Bemerkung 6.4.

(II) Beweisen Sie Lemma 6.8.

Aufgabe 6.2. Beweisen Sie die Details im Beweis von Satz 6.20 (Schritt 2). Seien dafür $k, \ell \in \mathbb{N}_{\geqslant 1}$ (oBdA $k \leqslant \ell$), $s_i, t_j \in \mathbb{N}_{\geqslant 1}$ für $i \in [k], j \in [\ell]$ und Primzahlen $p_1 < p_2 < \cdots < p_k$ sowie $q_1 < q_2 < \cdots < q_\ell$ gegeben, sodass

$$\prod_{i=1}^{k} p_i^{s_i} \quad = \quad \prod_{i=1}^{\ell} q_i^{t_i}.$$

Beweisen Sie: Dann gilt: $k = \ell$, und für alle $j \in [k]$ gilt $p_j = q_j$ und $s_j = t_j$.

Aufgabe 6.3. Beweisen Sie Beispiel 6.33, also dass die symmetrische Gruppe S_n der bijektiven Abbildungen $f : [n] \to [n]$ tatsächlich eine Gruppe ist.

Aufgabe 6.4. Beweisen Sie die Eigenschaften aus Bemerkung 6.35.

Aufgabe 6.5. Sei $n \in \mathbb{N}$ mit $n \geqslant 2$. Beweisen Sie, dass $(n\mathbb{Z}, +)$ eine Untergruppe von $(\mathbb{Z}, +)$ ist. Dabei ist $+$ die natürliche Addition auf den jeweiligen Mengen.

Aufgabe 6.6. Betrachten Sie den Beweis von Satz 6.38(c) und arbeiten Sie die noch fehlenden Details aus. D.h.: Zeigen Sie, dass für die Repräsentantenmenge A gilt, dass $G = \bigcup_{a \in A} a \circ U$, und dass für alle $a, b \in A$ mit $a \neq b$ die Mengen $a \circ U$ und $b \circ U$ disjunkt sind.

Aufgabe 6.7. Sei $n \in \mathbb{N}_{\geqslant 1}$ mit $n \geqslant 2$. Beweisen Sie, dass der Restklassenring modulo n, also $(\mathbb{Z}_n, +_n, \cdot_n)$, ein kommutativer Ring ist. Dabei sind $+_n, \cdot_n$ die Addition und Multiplikation modulo n.

Aufgabe 6.8. Arbeiten Sie die in Beispiel 6.45 fehlenden Details aus. D.h.: Beweisen Sie, dass $(F, \boxplus, \boxdot)$ ein Ring ist, und dass dieser Ring genau dann kommutativ ist, wenn R kommutativ ist.

Aufgabe 6.9. Arbeiten Sie die in Bemerkung 6.46 fehlenden Details aus. D.h.: Beweisen Sie, dass $(K[x], \boxplus, \boxdot)$ ein kommutativer Ring ist.

Literaturverzeichnis

[Beu02] Albrecht Beutelspacher. *"Das ist o.B.d.A. trivial!". Tipps und Tricks zur Formulierung mathematischer Gedanken.* Vieweg Studium, Braunschweig, 2002.

[Cam94] Peter J. Cameron. *Combinatorics: Topics, Techniques, Algorithms.* Cambridge University Press, 1994.

[Die06] Reinhard Diestel. *Graphentheorie.* Springer-Verlag, Berlin, 2006.

[Ebb03] Heinz-Dieter Ebbinghaus. *Einführung in die Mengenlehre.* Spektrum Akademischer Verlag, Heidelberg Berlin, 2003.

[Gro07] Martin Grohe. „Theoretische Informatik I", Skript zur gleichnamigen Vorlesung am Institut für Informatik der Humboldt-Universität zu Berlin, 2007.

[HU79] John E. Hopcroft and Jeffrey D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 1979.

[Juk08] Stasys Jukna. *Crashkurs Mathematik für Informatiker.* Teubner, 2008. 1. Auflage.

[KB05] Uwe Kastens and Hans Kleine Büning. *Modellierung. Grundlagen und formale Methoden.* Carl Hanser Verlag, München, 2005.

[Kre91] Ulrich Krengel. *Einführung in die Wahrscheinlichkeitstheorie und Statistik*. Vieweg, 1991.

[LPV03] L. Lovász, J. Pelikán, and K. Vesztergombi. *Discrete Mathematics*. Springer Science+Business Media, LLC, New York, 2003.

[MM00] Christoph Meinel and Martin Mundhenk. *Mathematische Grundlagen der Informatik. Mathematisches Denken und Beweisen - Eine Einführung.* B.G. Teubner, Stuttgart, 2000.

[Sch13] Nicole Schweikardt. „Diskrete Modellierung“, Skript zur gleichnamigen Vorlesung am Institut für Informatik der Goethe-Universität Frankfurt am Main, 2013. https://www2.informatik.hu-berlin.de/~wwwlif/lehre/fm-lehre/dismod/skript/.

[Ste07] Angelika Steger. *Diskrete Strukturen. Band 1: Kombinatorik, Graphentheorie, Algebra*. Springer, 2007. 2. Auflage.

[Wol17] Karsten Wolf. *Präzises Denken für Informatiker*. Springer Vieweg, 2017.