Theoretische Grundlagen der Informatik 1

Grundlagen und Algebraische Strukturen

Vorlesung im Wintersemester 2013/2014

Stephan Kreutzer
Technische Universität Berlin

Inhaltsverzeichnis

1. Einführung **1**

2. Mengen, Relationen und Funktionen **3**
2.1. Was sind überhaupt Mengen? 3
2.2. Die Algebra der Mengen 7

3. Grundlagen des Beweisens: Die Aussagenlogik **13**

4. Kartesische Produkte, Relationen und Funktionen **21**
4.1. Paare, Tupel und kartesische Produkte 21
4.2. Relationen und Funktionen 22
4.3. Funktionen 26
4.4. Größe und Kardinalität einer Menge 30
4.5. Umkehrabbildungen 37

5. Ordnungen und Äquivalenzen **41**
5.1. Ordnungen 41
5.2. Äquivalenzrelationen 47

6. Kombinatorik **51**
6.1. Das Schubfachprinzip 51
6.2. Zählen der Elemente einer Menge 52
6.3. Permutationen 53
6.4. Binomialkoeffizienten 54
6.5. Kombinationen und Variationen 60

7. Graphentheorie **65**
7.1. Grundbegriffe 65
7.2. Untergraphen und elementare Graphoperationen 66
7.3. Der Grad von Knoten 67
7.4. Ramsey Theorie 68
7.5. Pfade und Zyklen 70

7.6. Zusammenhang in Graphen 72
7.7. Bäume 74
7.8. Zusammenhang in Graphen 79
7.9. Der Satz von Menger 80
7.10. Alternative Graphmodelle 81
7.11. Multigraphen und Hypergraphen 86

8. Algebraische Strukturen **87**
8.1. Verbände 87
8.2. Halbgruppen, Monoide, Ringe und Körper 92

A. Mathematische Notation **97**
A.1. Standardnotationen 97

B. Griechische Symbole **99**

1. Einführung

2. Mengen, Relationen und Funktionen

2.1. Was sind überhaupt Mengen?

Mengen sind mit die grundlegensten Objekte, die wir in der Mathematik betrachten. Wir werden in diesem Kapitel daher zunächst einmal den Begriff der Mengen sowie gängige Operationen auf Mengen einführen.

Auf den Mathematiker und Philosoph Georg Cantor (1845-1918) geht folgender, naiver Mengenbegriff zurück:

> Eine Menge M is 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 zu sagen, dass m ein Element der Menge M ist und $m \notin M$ um zu sagen, dass m eben kein Element von M ist.

2.1 Beispiel. Im folgenden sehen wir einige Beispiele für Mengen.

(1) Die Menge $\mathbb{A} := \{a, b, \dots, z\}$ der Kleinbuchstaben des lateinischen Alphabets.

(2) Die Menge $\mathbb{N} := \{0, 1, 2, 3, \dots\}$ der natürlichen Zahlen.

(3) Die Menge $\mathbb{T}$ der Teilnehmer und Teilnehmerinnen dieser Vorlesung.

2.2 Notation. Wie im vorhergehenden Beispiel schreiben wir $:=$, wenn wir einen Wert definieren (oder Zuweisen) wollen, z.B. $x := 5$. Dies ist nicht zu verwechseln mit dem einfachen Gleichheitszeichen $=$, mit dem wir einfach die Gleichheit zweier Werte angeben. Die Aussage "es gilt $x = 5$" ergibt nur dann Sinn, wenn x schon einen Wert hat, z.B. in dem wir vorher gesagt haben, dass $x := 6 - 1$. ⊣

2.3 Definition. Für den späteren Gebrauch definieren wir folgende Mengen von Zahlen.

- $\mathbb{N} := \{0, 1, 2, 3, ...\}$ und $\mathbb{N}_+ := \{1, 2, 3, 4, ...\}$ als Menge der natürlichen, bzw. der positiven natürlichen Zahlen.
- $\mathbb{Z}$ ist die Menge der ganzen Zahlen.
- $\mathbb{Q}$ die Menge der rationalen Zahlen.
- $\mathbb{R}$ die Menge der reellen Zahlen.

Wir können Mengen auf verschiedene Weisen angeben. Zum einen können wir eine Menge *extensional* definieren, indem wir ihre Elemente explizit angeben. Auf diese Weise haben wir in den vorherigen Beispielen die Mengen definiert. Alternativ können wir eine Menge auch *intensional*, oder durch *Komprehension* (engl. comprehension) angeben, indem wir chrakteristische Eigenschaften der Element der Menge angeben. Z.B. können wir die Menge der geraden natürlichen Zahlen durch

$$M := \{n : n \in \mathbb{N} \text{ und es existiert ein } m \in \mathbb{N} \text{ mit } n = 2 * m\}$$

angeben.

2.4 Bemerkung. Oft schreibt man auch | statt : und benutzt einfach ein Komma statt des "und". Die Menge M kann daher auch als

$$M := \{n \mid n \in \mathbb{N},\ \text{es existiert ein } m \in \mathbb{N} \text{ mit } n = 2 * m\}$$

geschrieben werden. Während wir oft "und" durch Komma ersetzen werden, führt | bisweilen zu schlechter Lesbarkeit von Mengen und wird daher in dieser Vorlesung nicht benutzt. ⊣

Bei intensionaler Definition von Mengen muss man aber aufpassen, dass die Menge eindeutig definiert ist. So ist

$$M := \{x : 0 \leqslant x \leqslant 5\}$$

nicht eindeutig und definiert daher keine Menge, da nicht klar ist, ob x natürliche Zahlen sind, oder etwa reelle Zahlen. Es muss bei solchen Definitionen also immer klar geschrieben werden, aus welcher Menge x kommen soll, z.B. $M := \{x : x \in \mathbb{N}, 0 \leqslant x \leqslant 5\}$.

Einige grundlegende Eigenschaften von Mengen.

Wir geben im folgenden weitere grundlegende Eigenschaften von Mengen an.

- Alle Elemente einer Menge sind verschieden. D.h. die Menge $\{a, a\}$ ist die gleiche Menge wie $\{a\}$ und enthält als einziges Element das Element a.
- Die Elemente einer Menge haben keine Reihenfolge, d.h. die Menge ist nicht irgendwie "sortiert". D.h. $\{1, 4\} = \{4, 1\}$.
- Die Elemente einer Menge können sowohl elementare Objekte, etwa Zahlen, oder selbst wieder Mengen sein. Ebenso kann eine Menge Objekte verschiedenen "Typs" enthalten, etwa die Menge

  $$\big\{1, a, \{x : x \in \mathbb{R}, x \leqslant 0\}\big\},$$

  die aus drei Elementen besteht, von denen das letzte selbst wieder eine Menge ist.

2.5 Definition. Zwei Mengen A, B sind gleich, geschrieben $A = B$, wenn sie dieselben Elemente enthalten.

Dies wird als *Extensionalität* (lat. für Ausdehnung, Ausprägung), bezeichnet, da wir hier fordern, dass sich Mengen ausschließlich darüber definieren, welche Elemente sie enthalten und nicht etwa durch irgendwelche zusätzlichen Eigenschaften wie z.B. ihr Name. Daraus folgt, dass es genau eine Menge gibt, die keine Elemente enthält.

2.6 Definition (Leere Menge)**.** Die *leere Menge* ist die eindeutig bestimmte Menge, die keine Elemente enthält. Wir bezeichnen sie mit $\varnothing$.

Die leere Menge wird bisweilen auch mit $\{\}$ bezeichnet. Man beachte, dass $\varnothing \neq \{\varnothing\}$, da $\{\varnothing\}$ ja ein Element enhält. Als Anmerkung sei noch erwähnt, dass $\varnothing \subseteq A$ für jede Menge A gilt.

Grenzen des naiven Mengenbegriffs

Der Cantorsche Mengenbegriff, nach dem jede Kollektion von Objekten eine Menge ist, ist nicht ohne Probleme.

Betrachten wir folgendes Beispiel, welches auf Betrand Russel (1872 – 1970) zurückgeht.

2.7 Beispiel (Die Russelsche Antinomie)**.** Wie wir im letzten Beispiel gesehen haben, können Menge als Elemente selbst wieder Mengen enthalten. Nun sind Mengen, die sich selbst als Elemente enthalten, auf den ersten Blick etwas ungewöhnliche Objekte, so dass wir vielleicht die Menge aller Mengen definieren möchten, die sich eben nicht selbst enthalten. Sei also

$$N := \{M : M \text{ eine Menge }, M \notin M\},$$

d.h. für jede Menge M gilt, dass $M \in N$ genau dann, wenn M sich nicht selbst enthält.

Frage: Enthält N sich selbst?

Es ist klar, dass N sich entweder selbst enthält oder eben nicht. Betrachten wir also die beiden möglichen Fälle:

- **Fall 1:** $N \in N$**.** Wenn $N \in \mathbb{N}$, dann gilt gemäß der Definition der Menge N, dass N eine Menge ist und $N \notin N$. Dies ist aber ein Widerspruch zu $N \in N$.
- **Fall 2:** $N \notin N$**.** Wenn $N \notin N$, dann erfüllt N die Bedingungen an die Elemente von N und ist gemäß Definition von N also selbst in N, was ebenfalls zu einem Widerspruch führt.

Es führen also beide Fälle zu einem Widerspruch, obschon einer der beiden zutreffen müsste. Ein solcher Widerspruch, bei dem sich zwei widersprüchliche Aussagen gleichermaßen beweisen lassen, wird als Antinomie bezeichnet (nach griechisch *anti* gegen, *nomos* Gesetz, also sinngemäß eine Unvereinbarkeit von Gesetzen).

Als Ausweg bleibt nur, dass der Cantorsche Mengenbegriff nicht ganz stimmen kann. Denn obschon N aussieht wie eine Menge, kann es keine sein.

Man könnte natürlich versucht sein zu Argumentieren, dass die Russelsche Antinomie dadurch entsteht, dass man hier über etwas seltsame und nicht näher bestimmte Objekte wie sich selbst enthaltende Menge spricht. Um Russells Beispiel und den daraus resultierenden Widerspruch besser zu verstehen, betrachte man folgende Geschichte des Barbiers 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?

Die Russelsche Antinomie besagt (etwas umgangssprachlich formuliert) also, dass nicht alles, was wie eine Menge aussieht, auch eine ist. Man unterscheidet daher bisweilen zwischen *Mengen* und *Klassen*, wobei Klassen beliebige Zusammenstellungen von Objekten und Mengen sein können, aber eben nicht selbst wieder als Elemente anderer Klassen auftreten können. Eine direkte Folgerung aus der Russelschen Antinomie ist, dass die Menge aller Mengen nicht existiert (d.h. keine Menge ist). Denn wenn M die Menge aller Mengen wäre, so wäre $\{N : N \in M, N \notin N\}$ auch eine Menge, im Widerspruch zur Argumentation in der Russelschen Antinomie.

Um die Probleme mit der Russelschen Antinomie zu vermeiden, muss man also genauer definieren, welche Zusammenfassungen von Objekten wir als Mengen bezeichnen wollen und welche nicht. So wurden verschiedene Vorschläge zur Definition von Mengen gemacht, etwa das *Zermelo-Fraenkelsche System mit Auswahlaxiom*, welches heute meistens verwendet wird, oder das System von *von Neumann, Bernays und Gödel*. Diese Systeme vorzustellen geht aber deutlich über den Rahmen dieser Vorlesung hinaus. Für das "tägliche Leben", d.h. den üblichen Umgang mit Mengen in der Informatik und Mathematik, spielen diese Dinge aber auch keine so große Rolle. Wenn man sich den mit der Russelschen Antinomie verbundenen Problemen bewusst ist, kann man sie überlichweise auch vermeiden, da die Dinge, die wir normalerweise als Mengen ansehen wollen, auch solche sind. Wir werden daher weiterhin den naiven Mengenbegriff verwenden.

2.2. Was kann man mit Mengen eigentlich machen: Die Algebra der Mengen

In diesem Abschnitt beschäftigen wir uns mit Operationen aus Mengen, z.B. der Vereinigung und dem Schnitt zweier Mengen. Wir haben ja schon definiert, dass zwei Mengen gleich sind, wenn sie dieselben Elemente enthalten.

2.8 Definition (Teilmengen)**.** Seien M, N Mengen.

(1) M ist eine *Teilmenge* von N, geschrieben $M \subseteq N$, wenn jedes Element von M auch ein Element von N ist.

(2) M ist eine *echte Teilmenge* von N, geschrieben $M \subset N$, wenn $M \subseteq N$ und $M \neq N$.

Wenn $M \subseteq N$, dann sagen wir auch, dass N eine *Obermenge* von M ist, geschrieben $N \supseteq M$. Analog, wenn $M \subset N$, dann ist N eine *echte Obermenge* von M, geschrieben $N \supset M$.

2.9 Proposition. *Seien M, N, P Mengen. Dann gilt*

(1) *$M = N$ genau dann, wenn $M \subseteq N$ und $N \subseteq M$.*

(2) *Wenn $M \subseteq N$ und $N \subseteq P$, dann gilt $M \subseteq P$.*

Beweis. Wir zeigen zuerst den ersten Teil. Nach Definition 2.5, gilt $M = N$ genau dann, wenn M und N exakt die gleichen Elemente enthalten. Das gilt genau dann, wenn jedes $a \in M$ auch in N enthalten ist, und somit nach Definition 2.8 $M \subseteq N$, und jedes $a \in N$ auch in M enthalten und somit, wiederum nach Definition 2.8, $N \subseteq N$.

Nun zum zweiten Teil. Es ist zu zeigen, dass für jedes $a \in M$ auch $a \in P$ gilt. Sei also $a \in M$. Dann gilt, wegen $M \subseteq N$, auch $a \in N$. Da aber $N \subseteq P$, gilt für $a \in N$ auch $a \in P$, was zu zeigen war. □

2.10 Definition. Seien M, N Mengen.

(1) Der *Durchschnitt* von M und N, geschrieben $M \cap N$, ist die Menge

$$M \cap N := \{x : x \in M \text{ und } x \in N\}.$$

(2) Die *Vereinigung* von M und N, geschrieben $M \cup N$, ist die Menge

$$M \cup N := \{x : x \in M \text{ oder } x \in N\}.$$

(3) Die *Differenz* von M und N, geschrieben $M \setminus N$, ist die Menge

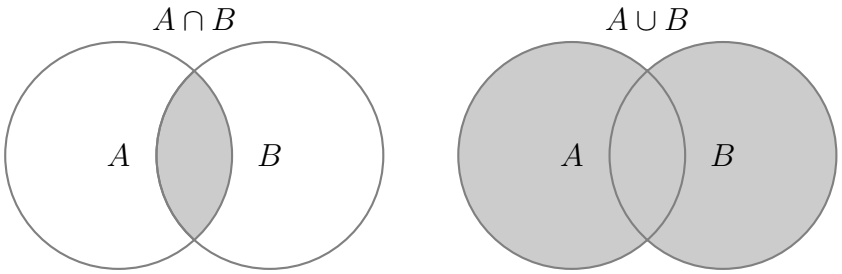
$$M \setminus N := \{x : x \in M \text{ und } x \notin N\}.$$

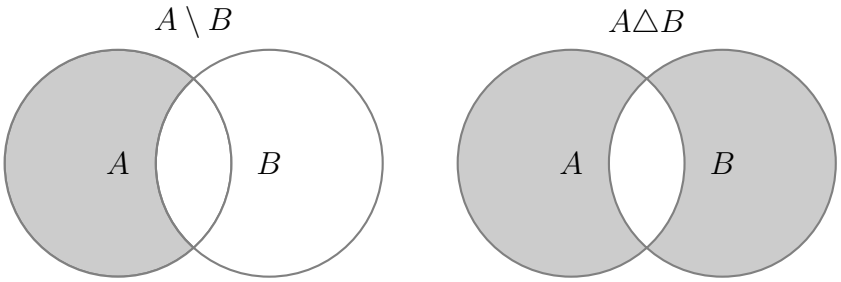
Wir schreiben bisweilen auch $M - N$ statt $M \setminus N$.

(4) Die *symmetrische Differenz* von M und N, geschrieben $M \triangle N$, ist definiert als die Menge

$$M \triangle N := (M \setminus N) \cup (N \setminus M).$$

Obige Definitionen lassen sich gut durch sogenannte *Venn-Diagramme* veranschaulichen.





Im folgenden Satz beweisen wir einige elementare Rechenregeln auf Mengen.

2.11 Satz. *Seien M, N, P Mengen. Dann gilt:*

(1) ***Idempotenz.***

$$M \cap M = M \text{ und } M \cup M = M.$$

(2) ***Kommutativität.***

$$M \cap N = N \cap M \text{ und } M \cup N = N \cup M.$$

(3) ***Assoziativität.***

$$M \cap (N \cap P) = (M \cap N) \cap P \text{ und } M \cup (N \cup P) = (M \cup N) \cup P.$$

(4) ***Distributivität.***

$$M \cap (N \cup P) = (M \cap N) \cup (M \cap P) \text{ und } M \cup (N \cap P) = (M \cup N) \cap (M \cup P).$$

(5) ***Absorption.***

$$M \cap (M \cup N) = M \text{ und } M \cup (M \cap N) = M.$$

Beweis. (1) Es gilt

$$\begin{array}{rcll} M \cap M & = & \{x : x \in M \text{ und } x \in M\} & \text{nach Definition 2.10} \\ & = & \{x : x \in M\} & \\ & = & M. & \end{array}$$

Analog beweist man $M \cup M = M$.

(2) Es gilt

$$\begin{aligned} M \cap N &= \{x : x \in M \text{ und } x \in N\} \quad \text{nach Definition 2.10} \\ &= \{x : x \in N \text{ und } x \in M\} \\ &= N \cap M. \end{aligned}$$

Analog beweist man $M \cup N = N \cup M$.

(3) Es gilt

$$\begin{aligned} M \cap (N \cap P) &= \{x : x \in M \text{ und } x \in (N \cap P)\} && \text{nach Definition 2.10} \\ &= \{x : x \in M \text{ und } x \in N \text{ und } x \in P\} \\ &= \{x : x \in M \cap N \text{ und } x \in P\} && \text{nach Definition 2.10} \\ &= (M \cap N) \cap P. \end{aligned}$$

Analog beweist man $M \cup (N \cup P) = (M \cup N) \cup P$.

(4) Wir beweisen $M \cap (N \cup P) = (M \cap N) \cup (M \cap P)$ in zwei Schritten.

Schritt 1. Wir zeigen zunächst $M \cap (N \cup P) \subseteq (M \cap N) \cup (M \cap P)$. Sei also $a \in M \cap (N \cup P)$. Dann ist, nach Definition 2.10, $a \in M$ und $a \in N \cup P$. Insbesondere ist also $a \in N$ oder $a \in P$.

Wenn $a \in N$ ist, dann gilt also $a \in M \cap N$ und somit $a \in (M \cap N) \cup (M \cap P)$. Wenn $a \in P$, dann gilt $a \in (M \cap P)$ und somit wiederum $a \in (M \cap N) \cup (M \cap P)$.

Damit ist dieser Schritt gezeigt.

Schritt 2. Wir zeigen als nächstes $(M \cap N) \cup (M \cap P) \subseteq M \cap (N \cup P)$.

Sei also $a \in (M \cap N) \cup (M \cap P)$. Dann gilt, nach Definition 2.10, $a \in M \cap N$ oder $a \in M \cap P$. Wenn $a \in M \cap N$, dann gilt also, wiederum nach Definition 2.10, $a \in M$ und $a \in N$. Also gilt auch $a \in N \cup P$ und somit $a \in M \cap (N \cup P)$.

Wenn $a \in M \cap P$, dann gilt $a \in M$ und $a \in P$. Also gilt $a \in N \cup P$ und somit $a \in M \cap (N \cup P)$. ⊣

Analog beweist man $M \cup (N \cap P) = (M \cup N) \cap (M \cup P)$.

(5) Dieser Fall ist ähnlich zum letzten uns zur Übung empfohlen.

□

2.12 Notation. Wir führen folgende Notation ein. Sei $k \in \mathbb{N}_+$ und seien $M_1, \ldots, M_k$ Mengen. Dann definieren wir

$$\bigcup_{i=1}^{k} M_i$$

als die Vereinigung $(\cdots(M_1 \cup M_2) \cup \ldots M_k)$ aller Mengen $M_1, \ldots, M_k$ und, analog,

$$\bigcap_{i=1}^{k} M_i$$

als den Schnitt $(\cdots(M_1 \cap M_2) \cap \ldots M_k)$ aller Mengen $M_1, \ldots, M_k$.

Des weiteren werden wir meistens die Klammern um Ausdrücke $(\cdots(M_1 \cap M_2) \cap \ldots M_k)$ weglassen und kurz $M_1 \cup \cdots \cup M_k$ und bzw. $M_1 \cap \cdots \cap M_k$ schreiben. Da die Operationen $\cup$ und $\cap$ assoziativ sind, spielt die Reihenfolge in der die Vereinigung bzw. der Schnitt gebildet wird, und damit die Klammerung, keine Rolle.

Eine weitere wichtige Operation auf Mengen ist die *Potenzmengenbildung*, bei der man aus einer gegebenen Menge M die Menge aller Teilmengen von M konstruiert.

2.13 Definition. Sei M eine Menge. Die *Potenzmenge* (engl. power set) von M, geschrieben $\mathcal{P}(M)$, ist definiert als die Menge

$$\mathcal{P}(M) := \{N : N \subseteq M\}$$

aller Teilmengen von M.

In der Literatur findet man auch oft die Schreibweise 2^M für $\mathcal{P}(M)$.

2.14 Beispiel.

(1) $\mathcal{P}(\{0,1\}) = \{\varnothing, \{0\}, \{1\}, \{0,1\}\}$

(2) $\mathcal{P}(\varnothing) = \{\varnothing\}$

Zum Schluss betrachten wir noch das Komplement einer Menge M. Intuitiv wollen wir das Komplement einer Menge M als die Menge ansehen, die alle Elemente enthält, die nicht in M enthalten sind. Wir können aber nicht einfach das Komplement von M als Menge $\{a : a \notin M\}$ definieren, da dann z.B. das Komplement von $\varnothing$ die Menge $\{a : a \text{ ist eine Menge und } a \notin \varnothing\}$ und damit die

Menge aller Mengen wäre. Dies ist aber wiederum keine Menge, daher ergibt die Definition keinen Sinn.

Stattdessen werden wir das Komplement immer nur relativ zu einer anderen Menge, dem *Universum*, definieren. Sei also U eine Menge und $M \subseteq U$. Dann ist das *Komplement* $\overline{M}$ *von* M *in* U definiert als die Menge

$$\overline{M} := U \setminus M.$$

Wenn man das Komplement einer Menge bilden möchte, muss man also immer mit angeben, bezüglich welchen Universums man dies tun möchte.

Es gelten folgende Rechenregeln für das Komplement einer Menge.

2.15 Satz. *Sei U das Universum (und insbesondere eine Menge) und seien $M, N \subseteq U$. Dann gilt:*

(1) ***Doppelte Negation.*** $\overline{(\overline{M})} = M$.

(2) ***De Morgansche Regeln.*** $\overline{M \cap N} = \overline{M} \cup \overline{N}$ *und* $\overline{M \cup N} = \overline{M} \cap \overline{N}$

(3) ***Inversion.*** $M \cap \overline{M} = \varnothing$ *und* $M \cup \overline{M} = U$.

(4) ***Identität.*** $M \cap U = M$ *und* $M \cup \varnothing = M$.

Beweis: Der Beweis wird zur Übung empfohlen. □

3. Grundlagen des Beweisens: Die Aussagenlogik

Im letzten Kapitel haben wir schon einige elementare Beweise gesehen, z.B. im Beweis von Satz 2.11. Z.B. haben wir die Kommutativität $M \cap N = N \cap M$ von $\cap$ wie folgt bewiesen. Es gilt

$$\begin{aligned} M \cap N &= \{x : x \in M \text{ und } x \in N\} \quad \text{nach Definition 2.10} \\ &= \{x : x \in N \text{ und } x \in M\} \\ &= N \cap M. \end{aligned}$$

Letzten Endes haben wir dabei die Kommutativität von $\cap$ dadurch bewiesen, dass wir die "Kommutatitivät" des deutschen "und" ausgenutzt haben, d.h., dass "$x \in M$ und $x \in N$" das gleiche sagt, wie "$x \in N$ und $x \in M$". Ebenso haben wir um Beweis des Distributivgesetzes die Distributivität von "und" und "oder" im Deutschen ausgenutzt. In beiden Fällen lag dies nahe. Aber bei Aussagen wie "Es gilt a genau dann, wenn b oder c gilt und wann immer b gilt, gilt auch c und wann immer c gilt, dann gilt a oder weder b noch c" ist das nicht mehr so klar, auch wenn die Aussage korrekt ist.

Wir werden daher jetzt als nächstes die sogenannte *Aussagenlogik* einführen, die es uns erlaubt, Schlussfolgerungen wie die obigen Beispiele sauber zu definieren und zu beweisen. Sie liefert damit die Grundlage jeglichen Beweisens.

Grundsätzlich kann man nur Aussagen beweisen, die entweder wahr oder falsch sind. Entsprechend werden auch in der Aussagenlogik die elementaren Aussagen entweder wahr oder falsch sein. Die Aussagenlogik beschäftigt sich dann mit Methoden, aus Aussagen neue Aussagen korrekt herzuleiten.

Formal ist die Aussagenlogik wie folgt definiert.

3.1 Definition (Syntax der Aussagenlogik)**.** Sei V eine Menge *aussagenlogischer Variablen*, so dass $V \cap \{\bot, \top, \neg, \wedge, \vee, \rightarrow, \leftrightarrow,), (\} = \varnothing$. Die Menge $\mathbf{A}(V)$ der *aussagenlogischen Formeln über* V ist die kleinste Menge mit:

- $V \subseteq \mathbf{A}(V)$ und $\bot, \top \in \mathbf{A}(V)$.
- Wenn $\varphi \in \mathbf{A}(V)$, dann ist auch $\neg\varphi \in \mathbf{A}(V)$.

- Wenn $\varphi, \psi \in \mathbf{A}(V)$, dann sind auch
  - $(\varphi \wedge \psi)$,
  - $(\varphi \vee \psi)$,
  - $(\varphi \to \psi)$ sowie
  - $(\varphi \leftrightarrow \psi)$

  in $\mathbf{A}(V)$.

Formeln, die nur aus Variablen oder $\bot, \top$ bestehen, heißen *atomar*, alle anderen Formeln *zusammengesetzt*. Wir bezeichnen $\neg$ als *Negation*, $\wedge$ als *Konjunktion*, $\vee$ als *Disjunktion*, $\to$ als *Implikation* und $\leftrightarrow$ als *Biimplikation*.

Die obige Definition definiert die sogenannte *Syntax* der Aussagenlogik, beschreibt also, welche Ausdrücke wir als Formeln der Aussagenlogik ansehen wollen. Die Definition sagt aber noch nichts darüber aus, was die Formeln bedeuten. Diese sogenannte *Semantik* werden wir weiter unten definieren.

3.2 Beispiel. Sei $V := \{V_0, V_1, \dots\}$. Die folgenden Ausdrücke sind syntaktisch korrekte Formeln der Aussagenlogik über V.

- $(V_0 \wedge (V_1 \to V_2))$
- $((V_1 \leftrightarrow V_0) \leftrightarrow V_2)$
- $((V_0 \wedge (V_1 \vee V_2)) \leftrightarrow ((V_0 \wedge V_1) \vee (V_0 \vee V_2)))$

Hingegen sind folgende Ausdrücke keine Formeln aus $\mathbf{A}(V)$.

- $V_0 \wedge (V_1 \to V_2)$ (Fehlen der äußeren Klammern)
- $(V_0 \leftarrow V_1)$ (Falsches Symbol)

3.3 Definition (Semantik der Aussagenlogik)**.** Sei V eine Menge aussagenlogischer Variablen. Eine *Variablenbelegung* β ist eine Abbildung, die jeder Variablen $X \in V$ ein Element aus der Menge $\{W, F\}$ der *Wahrheitswerte* zuweist.

Eine Variablenbelegung definiert wie folgt eine Abbildung $[\![\cdot]\!]^\beta$, die jeder Formel aus $\mathbf{A}(V)$ einen Wahrheitswert zuweist:

- $[\![\top]\!]^\beta := W$
- $[\![\bot]\!]^\beta := F$

- Für alle $X \in V$ gilt $[\![X]\!]^\beta := \beta(X)$.
- Die Semantik zusammengesetzter Formeln ist wie folgt über Wahrheitstafeln definiert. Für die Negation gilt

$[\![\varphi]\!]^\beta$	$[\![\neg\varphi]\!]^\beta$
F	W
W	F

Für Disjunktion und Konjunktion gelten

$[\![\varphi]\!]^\beta$	$[\![\psi]\!]^\beta$	$[\![(\varphi \vee \psi)]\!]^\beta$
F	F	F
F	W	W
W	F	W
W	W	W

$[\![\varphi]\!]^\beta$	$[\![\psi]\!]^\beta$	$[\![(\varphi \wedge \psi)]\!]^\beta$
F	F	F
F	W	F
W	F	F
W	W	W

Für Implikation und Biimplikation gelten

$[\![\varphi]\!]^\beta$	$[\![\psi]\!]^\beta$	$[\![(\varphi \to \psi)]\!]^\beta$
F	F	W
F	W	W
W	F	F
W	W	W

$[\![\varphi]\!]^\beta$	$[\![\psi]\!]^\beta$	$[\![(\varphi \leftrightarrow \psi)]\!]^\beta$
F	F	W
F	W	F
W	F	F
W	W	W

3.4 Beispiel. Sei $V := \{V_0, V_1, V_2\}$. Sei β die Abbildung, die V_0, V_1, V_2 den Wahrheitswert F zuweist. Sei nun $\varphi := (V_0 \wedge (V_1 \to V_2))$. Dann gilt $[\![V_0]\!]^\beta = [\![V_1]\!]^\beta = [\![V_2]\!]^\beta = F$. Weiterhin gilt also $[\![(V_1 \to V_2)]\!]^\beta = W$, aber $[\![(V_0 \wedge (V_1 \to V_2))]\!]^\beta = F$.

3.5 Beispiel. Wir betrachten folgende kleine Geschichte: *Auf der Insel Trufa leben zwei Volksstämme: Die Trus, die immer die Wahrheit sagen, und die Fas, die immer lügen.*

Ein Reisender trifft drei Bewohner A, B und C der Insel, die ihm Folgendes mitteilen:

(1) *A sagt: "B und C sagen genau dann die Wahrheit, wenn C die Wahrheit sagt."*

(2) *B sagt: "Wenn A und C die Wahrheit sagen, dann ist es nicht der Fall, dass A die Wahrheit sagt, wenn B und C die Wahrheit sagen."*

(3) *C sagt: "B lügt genau dann, wenn A oder B die Wahrheit sagen."*

Wir wollen nun mit Hilfe der Aussagenlogik entscheiden, zu welchen der beiden Volksstämme die drei Bewohner gehören. Dazu formalisieren wir zunächst die Aussagen der drei Bewohner in der Aussagenlogik. Wir verwenden die Aussagenvariablen A, B, C um zu sagen, dass die entsprechende Person die Wahrheit sagt.

Die Formalisierung ist dann:

- $\varphi_A := \Big(A \leftrightarrow \Big((B \wedge C) \leftrightarrow C\Big)\Big)$
- $\varphi_B := \Big(B \leftrightarrow \Big((A \wedge C) \rightarrow \neg((B \wedge C) \rightarrow A)\Big)\Big)$
- $\varphi_C := \Big(C \leftrightarrow \Big(\neg B \leftrightarrow (A \vee B)\Big)\Big)$

Wir suchen nun Belegungen für A, B, C, so dass $\varphi_A, \varphi_B, \varphi_C$ wahr werden. Mittels Wahrheitstafelmethode erhalten wir

X_A	X_B	X_C	φ_A	φ_B	φ_C
F	F	F	F	F	W
F	F	W	W	F	F
F	W	F	F	W	W
F	W	W	F	W	F
W	F	F	W	F	F
W	F	W	F	W	W
W	W	F	W	W	W
W	W	W	W	F	F

Also erfüllt die Belegung $\beta : A \mapsto W, \quad B \mapsto W, \quad C \mapsto F$ als einzige die drei Formeln.

Also sind A und B vom Stamme Tru und C vom Stamme Fa.

3.6 Definition. Sei V eine Menge von Aussagenvariablen.

(1) Zwei Formeln $\varphi, \psi \in \mathbf{A}(V)$ heißen *logisch äquivalent*, geschrieben $\varphi \equiv \psi$, wenn für alle Variablenbelegungen β gilt: $[\![\varphi]\!]^\beta = [\![\psi]\!]^\beta$.

(2) Eine Formel $\varphi \in \mathbf{A}(V)$ heißt *allgemeingültig*, wenn für alle Variablenbelegungen β gilt: $[\![\varphi]\!]^\beta = W$.

(3) Eine Formel $\varphi \in \mathbf{A}(V)$ heißt *unerfüllbar*, wenn für alle Variablenbelegungen β gilt: $[\![\varphi]\!]^\beta = F$.

(4) Eine Formel $\varphi \in \mathbf{A}(V)$ heißt *erfüllbar*, wenn es eine Variablenbelegung β gibt, so dass $[\![\varphi]\!]^\beta = W$.

3.7 Beispiel. Sei $V := \{X, Y\}$.

(1) Es gilt $(X \vee Y) \equiv (X \vee (X \vee Y))$.

(2) Die Formel $(X \vee \neg X)$ ist allgemeingültig.

(3) Die Formel $(X \wedge \neg X)$ hingegen ist unerfüllbar.

(4) Die Formel $(X \vee Y)$ ist erfüllbar aber nicht allgemeingültig.

Es gelten folgende Äquivalenzen zwischen aussagenlogischen Formeln.

3.8 Satz. *Sei V eine Menge aussagenlogischer Variablen und seien $\varphi, \psi, \vartheta \in \boldsymbol{A}(V)$. Dann gilt*

- $(\varphi \wedge \psi) \equiv (\psi \wedge \varphi)$ *und* $(\varphi \vee \psi) \equiv (\psi \vee \varphi)$ *(Kommutativität)*
- $(\varphi \wedge (\psi \wedge \vartheta)) \equiv ((\varphi \wedge \psi) \wedge \vartheta)$ *und* $(\varphi \vee (\psi \vee \vartheta)) \equiv ((\varphi \vee \psi) \vee \vartheta)$ *(Assoziativität)*
- $((\varphi \wedge \psi) \vee \vartheta) \equiv ((\varphi \vee \vartheta) \wedge (\psi \vee \vartheta))$ *und* $((\varphi \vee \psi) \wedge \vartheta) \equiv ((\varphi \wedge \vartheta) \vee (\psi \wedge \vartheta))$ *(Distributivität)*
- $(\varphi \wedge \varphi) \equiv \varphi$ *und* $(\varphi \vee \varphi) \equiv \varphi$ *(Absorption)*
- $\neg\neg\varphi \equiv \varphi$ *(doppelte Negation)*
- $\neg(\varphi \wedge \psi) \equiv (\neg\varphi \vee \neg\psi)$ *und* $\neg(\varphi \vee \psi) \equiv (\neg\varphi \wedge \neg\psi)$ *(De Morgansche Regeln).*
- $(\varphi \wedge \neg\varphi) \equiv \bot$ *und* $(\varphi \vee \neg\varphi) \equiv \top$ *(tertium non datur)*
- $(\varphi \vee \top) \equiv \top$ *und* $(\varphi \wedge \bot) \equiv \bot$

Beweis: Wir zeigen hier exemplarisch den Beweis der Äquivalenz $\neg(\varphi \wedge \psi) \equiv (\neg\varphi \vee \neg\psi)$. Die anderen Regeln werden zur Übung empfohlen.

Sei β eine Variablenbelegung. Wir müssen zeigen, dass für alle $\varphi, \psi, \vartheta \in V$ gilt: $[\![\neg(\varphi \wedge \psi)]\!]^\beta = [\![(\neg\varphi \vee \neg\psi)]\!]^\beta$.

(1) Angenommen, $[\![\neg(\varphi \wedge \psi)]\!]^\beta = W$. Dann gilt $[\![(\varphi \wedge \psi)]\!]^\beta = F$, nach Definition 3.3. Also gilt $[\![\varphi]\!]^\beta = F$ oder $[\![\psi]\!]^\beta = F$, wiederum nach Definition 3.3.
   - Falls $[\![\varphi]\!]^\beta = F$, dann gilt $[\![\neg\varphi]\!]^\beta = W$ und somit $[\![(\neg\varphi \vee \neg\psi)]\!]^\beta = W$.

- Falls $[\![\psi]\!]^\beta = F$, dann gilt $[\![\neg\psi]\!]^\beta = W$ und wiederum $[\![(\neg\varphi \vee \neg\psi)]\!]^\beta = W$.

(2) Angenommen, $[\![\neg(\varphi \wedge \psi)]\!]^\beta = F$. Dann gilt nach Definition 3.3 $[\![(\varphi \wedge \psi)]\!]^\beta = W$ und somit $[\![\varphi]\!]^\beta = W$ und $[\![\psi]\!]^\beta = W$. Das bedeutet aber, dass $[\![\neg\varphi]\!]^\beta = [\![\neg\psi]\!]^\beta = F$ und somit $[\![(\neg\varphi \vee \neg\psi)]\!]^\beta = F$.

In beiden Fällen werden also beide Seiten zum selben Wahrheitswert ausgewertet. □

Mit Hilfe der Aussagenlogik können wir nun Beweise formal präzise führen. Betrachten wir dazu noch einmal die Behauptung, dass die Mengenoperation $\cap$ assoziativ ist, d.h., dass gilt: $M \cap (N \cap P) = (M \cap N) \cap P$ für alle Mengen M, N, P.

Wir wollen also zeigen, dass ein Element a genau dann in $M \cap (N \cap P)$ enthalten ist, wenn es in $(M \cap N) \cap P$ enthalten ist. Wir benutzen folgende Aussagenvariablen aM, aN, aP, d.h. $V := \{aM, aN, aP\}$. Sei nun a ein Element. Wir definieren die Variablenbelegung β wie folgt: β bildet aM auf W ab, wenn $a \in M$ und sonst auf F. Analog bildet β die Variable aN auf W ab, wenn $a \in N$ und aP auf W ab, wenn $a \in P$.

Dann gilt offenbar $a \in M \cap (N \cap P)$ genau dann, wenn $[\![(aM \wedge (aN \wedge aP))]\!]^\beta = W$, was nach obiger Äquivalenz in Satz 3.8 genau dann der Fall ist, wenn $[\![((aM \wedge aN) \wedge aP)]\!]^\beta = W$, was wiederum genau dann gilt, wenn $a \in (M \cap N) \cap P$.

Üblicherweise wird man in mathematischen Beweisen die Aussagenlogik nicht so explizit wie im letzten Beispiel verwenden. Dennoch kann man mit der Aussagenlogik die Allgemeingültigkeit gängiger Schlussregeln (wie Assoziativität, Distributivität, De Morgen etc.) nachweisen, die man dann in Beweisen verwendet.

Zum Abschluss betrachten wir noch einmal die zu Beginn des Kapitels angegebene Regel

> "Es gilt a genau dann, wenn b oder c gilt und wann immer b gilt, gilt auch c und wann immer c gilt, dann gilt a oder weder b noch c".

In die Aussagenlogik übersetzt liest sich die Behautung wie folgt:

$$\Big(a \leftrightarrow \Big((b \vee c) \wedge (b \to c) \wedge \big(c \to (a \vee (\neg b \wedge \neg c))\big)\Big)\Big)$$

Die Formalisierung in der Aussagenlogik hat offensichtlich mehrere Vorteile: Zum einen wird die Klammerung klar, d.h. es wird überhaupt erst einmal

eindeutig beschrieben, was die Aussage bedeuten soll. Zum anderen lässt sich die Allgemeingültigkeit der Formel mit den Regeln der Aussagenlogik leicht nachweisen (wenn auch etwas länglich), was bei der umgangssprachlichen Formulierung viel schwerer ist.

4. Kartesische Produkte, Relationen und Funktionen

Im ersten Kapitel haben wir den zentralen Begriff der Menge kennengelernt. Mengen bilden die absolute Grundlage des Modellierens in der Informatik, jedoch induziert eine Menge keine Struktur auf ihren Elementen. D.h. eine Menge ist einfach eine Zusammenfassung von Objekten zu einer Menge, ohne dass dadurch irgendeine Beziehung zwischen diesen Elementen hergestellt würde. Für die meisten Modellierungsaufgaben ist das zuwenig. Wir werden daher in den folgenden Kapiteln Möglichkeiten kennen lernen, die Elemente einer Menge miteinaner in Beziehung setzen zu können. Den Anfang machen Tupel und kartesische Produkte.

4.1. Paare, Tupel und kartesische Produkte

4.1 Definition. (1) Für Objekte a und b schreiben wir (a, b) für das *geordenete Paar* mit den Komponenten a und b.

(2) Für $k \in \mathbb{N}$ und Objekte $a_1, \ldots, a_k$ schreiben wir $(a_1, \ldots, a_k)$ für das *k-Tupel* mit den Komponenten $a_1, \ldots, a_k$.

(3) Zwei Tupel $(a_1, \ldots, a_l)$ und $(b_1, \ldots, b_k)$ sind *gleich*, geschrieben $(a_1, \ldots, a_l) = (b_1, \ldots, b_k)$, wenn $k = l$ und $a_i = b_i$ für alle $1 \leqslant i \leqslant k$.

4.2 Bemerkung. Ein Paar (a, b) ist also nichts anderes als ein 2-Tupel. Man beachte aber den Unterschied zwischen dem Paar (a, b) und der Menge $\{a, b\}$, da $(a, b) \neq (b, a)$ aber $\{a, b\} = \{b, a\}$.

Ein Spezialfall ist das 0-Tupel, oder auch *leeres Tupel*, $()$, da es keine Komponenten enthält.

4.3 Definition. Seien M und N Mengen.

(1) Das *kartesische Produkt* (oder auch *Kreuzprodukt*) von M und N, geschrieben $M \times N$, ist definiert als die Menge

$$M \times N := \{(a, b) : a \in M, b \in N\}.$$

(2) Für ein $k \in \mathbb{N}_+$ und Mengen $M_1, \ldots, M_k$ ist das kartesische Produkt der Mengen $M_1, \ldots, M_k$ definiert als die Menge

$$M_1 \times M_2 \times \cdots \times M_k := \{(m_1, \ldots, m_k) : m_i \in M_i \text{ für alle } 1 \leqslant i \leqslant k\}.$$

Falls $M_1 = M_2 = \cdots = M_k =: M$ gilt, so nennen wir $M \times M \times \cdots \times M$ die *k-te Potenz von M*, geschrieben M^k. Wir definieren auch die 0-te Potenz von M als die Menge $M^0 := \{()\}$.

4.4 Beispiel. Wir geben im Folgenden einige Beispiele für Potenzen und kartesische Produkte. Sei $M := \{1, 2\}$ und $N := \{a, b\}$.

- $M \times N = \{(1, a), (1, b), (2, a), (2, b)\}$.
- $M^2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$.
- $M \times \{c\} = \{(1, c), (2, c)\}$.
- Uhrzeiten kann man repräsentieren durch Elemente der Menge

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

  wobei

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

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

4.2. Relationen und Funktionen

Relationen und Funktionen bilden die wichtigsten Mittel zur Strukturierung in der diskreten Modellierung. Relationen sind dabei einfach Teilmengen kartesischer Produkte.

4.5 Definition. (1) Seien M, N Mengen. Eine *Relation zwischen M und N* ist eine Teilmenge $R \subseteq M \times N$.

(2) Sei $k \in \mathbb{N}$ und seien $M_1, \ldots, M_k$ Mengen. Eine *Relation auf* $M_1, \ldots, M_k$ ist eine Teilmenge $R \subseteq M_1 \times \cdots \times M_k$. Dabei wird k die *Stelligkeit* der Relation R genannt.

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

Relationen sind also Mengen, deren Elemente Tupel sind. Ist z.B. R eine Relation über $M \times N$, dann sind deren Elemente also Paare aus $M \times N$.

4.6 Beispiel. Seien $M := \{1, \ldots, 12\}$ die Monate des Jahres, $T := \{1, \ldots, 31\}$ die möglichen Tage und $J := \mathbb{Z}$ die Jahreszahlen. Die Menge der gültigen Daten (bzgl. unseres Kalenders) ist dann eine Teilmenge von $T \times M \times J$, also eine Relation D auf T, M, J. Zum Beispiel ist das Tupel $(19, 12, 1909)$[1] in D, das Tupel $(31, 2, 2014)$ aber nicht.

4.7 Beispiel. Sei M die Menge der Städte in der Bundesrepublik Deutschland. Wir können dann die Relation $F \subseteq M^2$ betrachten, in der alle Paare (a, b) stehen, für die es eine direkte Flugverbindung zwischen den Städten a und b gibt.

4.8 Bemerkung. Das letzte Beispiel führt im Prinzip schon den wichtigen Begriff eines *Graphen* ein. Ein *Graph* $G = (V, E)$ besteht aus einer Menge V, deren Elemente *Knoten* genannt werden, und einer Relation $E \subseteq V \times V$, deren Elemente *Kanten* genannt werden. Im obigen Beispiel war V die Menge der Städte in Deutschland und E die Menge der Paare von Städten zwischen denen direkte Flugverbindungen bestehen. Graphen sind eines der wichtigsten Mittel zur Modellierung in der Informatik und werden Thema des zweiten Teils dieser Vorlesung sein.

Man beachte, dass man Relationen immer nur bezüglich der Mengen angeben kann, über der sie gebildet werden. Z.B. ergibt es wenig Sinn zu sagen, dass $R = \varnothing$ eine Relation ist, da hier nicht angegeben wird, über welchen Mengen R denn eine Relation sein soll. Wir bezeichnen deshalb die Mengen, über denen eine Relation gebildet wird, als den *Typ* der Relation.

4.9 Definition. Sei $k \in \mathbb{N}$ und seien $M_1, \ldots, M_k$ Mengen. Wenn R eine Relation über den Mengen $M_1, \ldots, M_k$ ist, so bezeichnen wir $(M_1, \ldots, M_k)$ als den *Typ* der Relation R.

Entsprechend sagen wir, dass zwei Relationen R_1, R_2 *gleich* sind, wenn sie den gleichen Typ haben und $R_1 = R_2$ gilt.

Folgende Notation werden wir im Skript oft verwenden.

[1] $(19, 12, 1909)$ steht also für das Datum 19.12.1909, ein besonderes Datum in der Geschichte des Fußballs in Deutschland.

4.10 Notation. (1) Wir schreiben oft kurz $R : (M_1, \ldots, M_k)$ um zu bestimmen, dass R eine Relation mit Typ $(M_1, \ldots, M_k)$ ist. In der Literatur findet man auch oft die Schreibweise $R : M_1 \times \cdots \times M_k$, was irgendwie intuitiver ist, aber den Nachteil hat, dass wenn M eine nicht-leere Menge ist, die Mengen $M \times \varnothing$ und $\varnothing \times M$ die gleiche Menge ergibt, nämlich in beiden Fällen die leere Menge, wir den Typ aber unterscheiden wollen.

(2) Eine 2-stellige Relation R wird auch als *binäre Relation* bezeichnet. Wir schreiben binäre Relationen R bisweilen in *Infixschreibweise*, d.h. schreiben aRb anstatt $(a, b) \in R$, insbesondere bei binären Relationen wie $\leqslant, <, =$.

(3) Sei M eine Menge. Wir bezeichnen mit Id_M die *Identitätsrelation* über M, definiert als

$$\mathrm{Id}_M := \{(m, m) : m \in M\}.$$

Zum Schluss dieses Abschnitts betrachten wir noch einige Eigenschaften von Relationen.

4.11 Definition. Seien M, N Mengen. Eine Relation $R : (M, N)$ über M, N heißt

(1) *linkstotal*, wenn es für alle $m \in M$ ein $n \in N$ gibt mit $(m, n) \in R$.

(2) *rechtstotal*, wenn es für alle $n \in N$ ein $m \in M$ gibt mit $(m, n) \in R$.

(3) *linkseindeutig*, wenn es für alle $n \in N$ höchstens ein $m \in M$ gibt mit $(m, n) \in R$. D.h. für alle $n \in N$ und $m, m' \in M$ mit $(m, n) \in R$ und $(m', n) \in R$ gilt $m = m'$.

(4) *rechtseindeutig*, wenn es für alle $m \in M$ höchstens ein $n \in N$ gibt mit $(m, n) \in R$. D.h. für alle $m \in M$ und $n, n' \in N$ mit $(m, n) \in R$ und $(m, n') \in R$ gilt $n = n'$.

4.12 Beispiel. (1) Sei M die Menge aller Menschen und D die Menge aller gültigen Daten (siehe Beispiel 4.6). Dann ist die Relation $R : (M, D)$ definiert als

$$\{(m, d) : d \text{ ist der Geburtstag von } m\}$$

rechtsseindeutig, da jeder Mensch nur genau einen Geburtstag hat aber nicht linkseindeutig, da mehrere Menschen am selben Tag Geburtstag haben können.

(2) Die Relation $R : (\mathbb{N}, \mathbb{N})$ definiert als

$$\{(n, n') : n, n' \in \mathbb{N} \text{ und } n' = n * n\}$$

ist sowohl rechts- als auch linkseindeutig. Sie ist auch linkstotal aber nicht rechtstotal.

4.13 Definition (Komposition)**.** Seien A, B, C Mengen und seien $P : (A, B)$ und $Q : (B, C)$ Relationen. Dann ist die *Komposition* $P; Q : (A, C)$ definiert als Relation

$$P; Q := \{(a, c) : \text{ es ex. } b \in B \text{ mit } (a, b) \in P \text{ und } (b, c) \in Q\}.$$

4.14 Beispiel. (1) Seien $A := \{a, b, c\}, B := \{1, 2, 3\}$ und $C := \{x, y, z\}$. Sei

$$P := \{(a, 1), (a, 2), (b, 3), (c, 1), (c, 2), (c, 3)\}$$

und

$$Q := \{(1, x), (2, y), (3, z)\}.$$

Dann ist $P; Q := \{(a, x), (c, x), (a, y), (c, y), (b, z), (c, z)\}$.

(2) Seien A die Menge aller Filmschauspieler, $B := \mathbb{N}$ und C die Menge aller Filme.

Sei

$$P := \{(Hawke, 1), (Firth, 2), (Dunst, 3), (Gainsbourg, 4)\}$$

eine Relation, die Schauspielern eindeutige "ID"s zuweist. Sei

$$Q := \{(3, Melancholia), (4, Melancholia), (2, King'sSpeech)\}.$$

Dann ist

$$P; Q := \left\{ \begin{array}{l} (Dunst, Melancholia), (Gainsbourg, Melancholia), \\ (Firth, King'sSpeech) \end{array} \right\}$$

eine Relation, die zu jedem Film die Schauspieler auflistet, die in dem Film mitgespielt haben.

4.15 Bemerkung. Das letzte Beispiel zeigt, dass Relationskomposition ein wichtiges Konzept für den Datenbankbereich ist. Dort wird die Komposition als *join* bezeichnet, geschrieben $\bowtie$, und auf Relationen beliebiger Stelligkeiten definiert. Ist also z.B. $R : (M_1, \ldots, M_k, A_1, \ldots, A_r)$ und $Q : (N_1, \ldots, N_t, A_1, \ldots, A_r)$ dann ist $R \bowtie Q : (M_1, \ldots, M_k, N_1, \ldots, N_t)$ die Relation, in der alle Tupel aus R mit allen Tupeln aus Q kombiniert werden, wenn sie auf den gemeinsamen Komponenten $(A_1, \ldots, A_r)$ übereinstimmen.

4.16 Proposition (Assoziativität der Komposition)**.** *Seien A, B, C, D Mengen und $P : (A, B)$, $Q : (B, C)$, $R : (C, D)$ Relationen. Dann gilt*

$$(P; Q); R = P; (Q; R).$$

Beweis: Übung. □

Zum Schluss behandeln wir noch eine oft verwendete Operation auf Relationen.

4.17 Definition (Restriktion)**.** Für ein $k \in \mathbb{N}_+$ seien $M_1, \ldots, M_k$ Mengen und $R : (M_1, \ldots, M_k)$ eine Relation. Sei $1 \leqslant i \leqslant k$ und $N \subseteq M_i$. Die *Restriktion* von R auf $M_1, \ldots M_{i-1}, N, M_{i+1}, \ldots, M_k$ ist die Relation

$$\{(m_1, \ldots, m_k) : (m_1, \ldots, m_k) \in R \text{ und } m_i \in N\}.$$

In die Restriktion von R auf $M_1, \ldots M_{i-1}, N, M_{i+1}, \ldots, M_k$ werden also nur die Tupel aus R übernommen, deren i-te Komponente aus der Teilmenge N kommt. Besonders interessant ist der Fall, wenn $R \subseteq M^k$, für eine Menge M ist und $N \subseteq N$. Dann bilden wir die Restriktion von R auf N^k und bezeichnen sie als $R_{|N}$.

4.3. Funktionen

4.3.1. Totale und partielle Funktionen

4.18 Definition (Funktionen)**.** Seien A, B Mengen. Eine *(partielle) Funktion* von A nach B ist eine rechtseindeutige Relation $f : (A, B)$, d.h. für alle $a \in A$ gibt es höchstens ein $b \in B$ mit $(a, b) \in f$.

Eine Funktion $f : (A, B)$ ist *total*, wenn es für jedes $a \in A$ auch ein (eindeutiges) $b \in B$ gibt mit $(a, b) \in f$.

Wir verwenden die Begriffe *Abbildung* und *Funktion* synonym, werden also Funktionen auch oft als Abbildungen bezeichnen.

Man beachte, dass jede totale Funktion auch eine partielle Funktion ist. Umgekehrt gilt das aber nicht unbedingt.

4.19 Notation. (1) Wir schreiben üblicherweise $f : A \to B$ um auszudrücken, dass f eine totale Funktion *von A nach B* ist.

Wir schreiben üblicherweise $f : A \rightharpoonup B$ um auszudrücken, dass f eine partielle Funktion *von A nach B* ist.

(2) Entsprechend schreiben wir $f(a) = b$ statt $(a, b) \in f$. Wir nennen $f(a)$ den *Funktionswert* an der Stelle a.

4.20 Definition. Seien A, B Mengen und $f : A \rightharpoonup B$ eine (partielle) Funktion von A nach B.

(1) Für $A' \subseteq A$ definieren wir $f(A') := \{f(a) : a \in A'\}$.

(2) Die Menge A heißt *Argumentationsbereich*, oder *Domain*, von f, geschrieben $\mathrm{dom}(f)$. Die Menge B heißt der *Zielbereich*, oder *co-Domain*, von f, geschrieben $\mathrm{cod}(f)$.

(3) Seien $A_0 \subseteq A$ und $B_0 \subseteq B$. Dann heißt die Menge

$$f(A_0) = \{f(a) : a \in A'\}$$

das *Bild* von A_0 bzgl. f und die Menge

$$f^{-1}(B_0) := \{a : f(a) \in B_0\}$$

das *Urbild* von B_0 unter f.

(4) Der *Bildbereich* von f, geschrieben $\mathrm{Bild}(f)$, ist definiert als $f(A)$ und der *Definitionsbereich* von f, geschrieben $\mathrm{Def}(f)$, ist definiert als $f^{-1}(B)$.

Man beachte, dass bei totalen Funktionen der Definitionsbereich gleich dem Argumentationsbereich ist.

Wie schon bei Relationen definieren wir auch für Funktionen einen Kompositionsbegriff. Da Funktionen spezielle Relationen sind, überträgt sich die Komposition ; aus Definition 4.13 auch auf Funktionen. Für Funktionen ist aber folgende Konvention oft intuitiver.

4.21 Definition (Komposition von Funktionen)**.** Seien A, B, C Mengen und $f : A \rightharpoonup B$ und $g : B \rightharpoonup C$ partielle Abbildungen. Dann ist deren Komposition $(g \circ f) : (A, C)$ definiert als Relation

$$\{(a, c) : \text{ es ex. } b \in B \text{ mit } f(a) = b \text{ und } g(b) = c\}.$$

4.22 Proposition. *Seien A, B, C Mengen und $f : A \rightharpoonup B$ und $g : B \rightharpoonup C$ partielle Abbildungen. Dann ist $(g \circ f)$ eine partielle Abbildung von A nach C. Es gilt $(g \circ f) = f; g$ und für alle $x \in A$ ist $(g \circ f)(a) = g(f(a))$.*

Beweis: Wir zeigen zunächst, dass $(g \circ f)$ eine partielle Abbildung, also rechtseindeutig ist. Sei dazu $a \in A$. Es ist zu zeigen, dass es keine zwei verschiedenen $c, c' \in C$ gibt mit $(a, c) \in (g \circ f)$ und $(a, c') \in (g \circ f)$. Sei also $c, c' \in C$ mit $(a, c) \in (g \circ f)$ und $(a, c') \in (g \circ f)$. Also gibt es b, b' mit $f(a) = b$ und $g(b) = c$ sowie $f(a) = b'$ und $g(b') = c'$. Da f eine partielle Funktion ist, gilt $b = b'$. Und da g eine partielle Funktion ist, somit $c = c'$.

Dass $(g \circ f)(a) = g(f(a))$ für alle $a \in A$ folgt sofort aus der Definition. Man rechnet nun leicht nach, dass $(g \circ f) = f; g$. □

Zum Schluss betrachten wir noch eine weitere, oft verwendete Operation auf Funktionen.

4.23 Definition (Restriktion)**.** Seien A, B Mengen. Sei $f : A \rightharpoonup B$ eine Funktion und $A' \subseteq A$. Die *Restriktion*, oder *Einschränkung*, von f auf A' ist die Funktion

$$f_{|A'} : A' \rightharpoonup B$$

definiert wie folgt: für alle $a \in A'$ ist $f_{|A'}(a) := f(a)$.

Die Restriktion von Funktionen stimmt also mit dem Begriff auf Relationen überein, indem die Funktion $f : (A, B)$ auf (A', B) eingeschränkt wird.

4.24 Definition (Gleichheit von Funktionen)**.** Zwei partielle Funktionen $f_1 : A_1 \rightharpoonup B_1$ und $f_2 : A_2 \rightharpoonup B_2$ sind *gleich*, geschrieben $f_1 = f_2$, wenn sie als Relationen gleich sind, d.h. wenn $A_1 = A_2, B_1 = B_2$, $\mathrm{Def}(f_1) = \mathrm{Def}(f_2)$ und für alle $a \in \mathrm{Def}(f_1)$ gilt $f_1(a) = f_2(a)$.

4.3.2. Eigenschaften von Relationen und Funktionen

4.25 Definition. Seien M, N Mengen und $R : (M, N)$ eine Relation.

(1) R heißt *injektiv*, wenn es für jedes $n \in N$ höchstens ein $m \in M$ gibt mit $(m, n) \in R$.

(2) R heißt *surjektiv*, wenn es für jedes $n \in N$ mindestens ein $m \in M$ gibt mit $(m, n) \in R$.

(3) R heißt *bijektiv*, wenn es für jedes $n \in N$ genau ein $m \in M$ gibt mit $(m, n) \in R$.

4.26 Bemerkung. Wir haben die Begriffe injektiv, surjektiv und bijektiv zwar für allgemeine Relationen eingeführt, werden sie aber fast ausschließlich für Funktionen verwenden.

Offensichtlich gilt für jede totale Funktion $f : M \to N$:

f ist bijektiv genau dann, wenn f injektiv und surjektiv ist.

4.27 Beispiel. (1) Die Funktion $f : \mathbb{N} \to \mathbb{N}$ mit $f(n) := (-1)^n \cdot n$ ist injektiv, aber nicht surjektiv.

(2) Die Funktion $f : \mathbb{Z} \to \mathbb{N}$ mit $f(n) := |n|$ (wobei $|n|$ der Betrag von n ist, also $|n| = n$ wenn $n \geqslant 0$ und $|n| = -n$ sonst) ist surjektiv aber nicht injektiv.

(3) Die Funktion $f : \mathbb{N} \to \mathbb{N}_+$ mit $f(n) := n + 1$ ist bijektiv.

4.28 Definition. Seien M, N Mengen und $f : M \to N$ eine totale Funktion.

(1) f heißt *Injektion*, wenn f injektiv ist.

(2) f heißt *Surjektion*, wenn f surjektiv ist.

(3) f heißt *Bijektion*, wenn f bijektiv ist.

4.29 Notation. Seien M, N Mengen. Mit N^M bezeichnen wir die Menge der Abbildungen von M nach N. Bisweilen verwenden wir auch $\mathrm{Abb}(M, N)$.

4.30 Satz. *Für jede Menge M gibt es eine Bijektion von $\{0,1\}^M$ nach $\mathcal{P}(M)$.*

Beweis: Sei M eine Menge. Wir definieren eine Funktion $F : \{0,1\}^M \to \mathcal{P}(M)$ durch $F(f) := \{m \in M : f(m) = 1\}$ für alle $f \in \{0,1\}^M$.

Behauptung: F ist eine Bijektion.

Beweis: Offensichtlich ist F total, da $F(f)$ für alle $f \in \{0,1\}^M$ definiert ist.

F **injektiv.** Seien $f, g \in \{0,1\}^M$ mit $F(f) = F(g)$. Dann gilt für alle $m \in M$:

$$f(m) = 1 \quad \text{gdw.} \quad g(m) = 1.$$

Also auch $f(m) = 0$ gdw. $g(m) = 0$ und somit $f = g$.

F **surjektiv.** Sei $N \in \mathcal{P}(M)$ beliebig. Es ist zu zeigen, dass eine Funktion $f_N \in \{0,1\}^M$ existiert mit $F(f_N) = N$.

Wir definieren $f_N : M \to \{0,1\}$ durch

$$f_N(m) := \begin{cases} 1 & \text{falls } m \in N \\ 0 & \text{sonst} \end{cases}$$

Dann gilt offensichtlich $F(f_N) = N$.

⊣

□

4.31 Bemerkung. Die Funktion f_N, die im vorherigen Beweis konstruiert wurde, nennt man die *charakteristische Funktion* der Menge N.

4.4. Größe und Kardinalität einer Menge

4.32 Definition. Eine Menge M ist endlich, wenn sie nur endlich viele Elemente enthält. Die *Größe* einer Menge M, geschrieben $|M|$, ist definiert als

$$|M| := \begin{cases} \text{Anzahl Elemente in } M & \text{falls } M \text{ endlich} \\ \infty & \text{sonst} \end{cases}$$

(∞ wird unendlich gesprochen)

4.33 Beispiel. Es gilt $|\{2, 4, 6\}| = 3$ und $|\mathbb{N}| = \infty$.

Die Definition der Größe einer Menge unterscheidet also nicht zwischen unendlichen Mengen. Wie das folgende Beispiel zeigt, ist die Definition der Größe einer unendlichen Menge auch nicht ganz einfach und zunächst auch nicht völlig intuitiv.

4.34 Beispiel (Hilberts Hotel)**.** Hilberts Hotel ist ein Hotel mit unendlich vielen Zimmern. Genauer gesagt, hat Hilberts Hotel die Zimmer Z_i für alle $i \in \mathbb{N}$. Eines Nachts sind alle Zimmer belegt, sagen wir in Zimmer Z_i wohnt Gast G_i, für alle $i \in \mathbb{N}$. Nun kommt zu später Stunde noch ein weiterer Gast, S, und bittet den Hotelmanager um ein Zimmer. Der Manager bittet daraufhin jeden Gast G_i, aus Zimmer Z_i in das Zimmer Z_{i+1} umzuziehen. Dann ist das Zimmer Z_0 frei und der Gast S kann dort einziehen. ⊣

Das Beispiel zeigt ein besonderes Verhalten unendlicher Mengen. Die Zahl der Zimmer hat sich in dem Beispiel ja nicht erhöht. Die Zahl der Gäste jedoch schon. Das bedeutet aber, dass die "Größe" der Mengen $\{G_i : i \in \mathbb{N}\}$ und $\{G_i : i \in \mathbb{N}\} \cup \{S\}$ gleich ist, obschon ja in der rechten Menge ein neues Element hinzugekommen ist, also $\{G_i : i \in \mathbb{N}\} \subsetneq \{G_i : i \in \mathbb{N}\} \cup \{S\}$. Allerdings kann man zeigen, dass zum Beispiel die Menge der reelen Zahlen wirklich größer ist, als die der natürlichen Zahlen. Wir müssen also die "Größe" unendlicher Mengen etwas anders definieren.

4.35 Definition. Seien M, N möglicherweise unendliche Mengen.

(1) M und N sind *gleichmächtig*, wenn es eine Bijektion zwischen M und N gibt. Wir schreiben kurz $\operatorname{card}(M) = \operatorname{card}(N)$.

(2) M ist *höchstens so mächtig* wie N, oder hat höchstens die Kardinalität von N, wenn es eine Injektion von M nach N gibt. Wir schreiben kurz $\operatorname{card}(M) \leqslant \operatorname{card}(N)$.

Gibt es darüber hinaus keine Surjektion von M nach N, so schreiben wir $\operatorname{card}(M) < \operatorname{card}(N)$ und sagen, dass die Kardinalität von M echt kleiner ist als die von N.

(3) M ist *mindestens so mächtig* wie N, oder hat mindestens die Kardinalität von N, wenn es eine Surjektion von M nach N gibt. Wir schreiben kurz $\operatorname{card}(M) \geqslant \operatorname{card}(N)$.

Gibt es darüber hinaus keine Injektion von M nach N, so schreiben wir $\operatorname{card}(M) > \operatorname{card}(N)$ und sagen, dass die Kardinalität von M echt größer ist als die von N.

4.36 Beispiel. (1) Wenn M, N endliche Mengen sind, dann gilt $|M| = |N|$ genau dann, wenn $\operatorname{card}(M) = \operatorname{card}(N)$.

(2) Eine Menge M ist genau dann endlich, wenn es ein $n \in \mathbb{N}$ gibt mit $\operatorname{card}(M) = \operatorname{card}(\{1, \ldots, n\})$.

Hinweis. $\{1, \ldots, n\} = \varnothing$ falls $n = 0$.

Aus Theorem 4.30 folgt sofort folgende Beobachtung.

4.37 Satz. *Für jede Menge M gilt:* $\operatorname{card}(\{0,1\}^M) = \operatorname{card}(\mathcal{P}(M))$.

4.38 Definition. Sei M eine Menge.

(1) M ist *abzählbar unendlich*, wenn $\operatorname{card}(M) = \operatorname{card}(\mathbb{N})$.

(2) M ist *abzählbar*, wenn M endlich ist oder aber abzählbar unendlich.

(3) M ist überabzählbar, falls $\operatorname{card}(M) > \operatorname{card}(\mathbb{N})$.

Ohne Beweis geben wir folgendes Lemma an.

4.39 Lemma. *Eine nicht-leere Menge M ist genau dann abzählbar, wenn es eine Surjektion von $\mathbb{N}$ nach M gibt.*

Intuitiv kann man sich sich eine Surjektion von $\mathbb{N} \to M$ als eine Aufzählung $m_0, m_1, \ldots$ der Elemente von M vorstellen (mit Wiederholung), mit $m_i := f(i)$.

4.40 Korollar. *Jede Teilmenge einer abzählbaren Menge ist abzählbar.*

4.41 Satz. *$\mathbb{Z}$ und $\mathbb{Q}$ sind abzählbar.*

Beweis: Da $\mathbb{Z}$ und $\mathbb{Q}$ unendlich sind, reicht es nach Lemma 4.39 eine Surjektion von $\mathbb{N}$ nach $\mathbb{Z}$ bzw. $\mathbb{Q}$ zu finden.

Wir betrachten zunächst $\mathbb{Z}$. Sei $F_{\mathbb{Z}} : \mathbb{N} \to \mathbb{Z}$ definiert als

$$f_{\mathbb{Z}}(n) := \begin{cases} -\frac{n}{2} & \text{falls } n \text{ gerade} \\ \frac{n+1}{2} & \text{sonst} \end{cases}$$

für alle $n \in \mathbb{N}$.

Es gilt also z.B. $f_{\mathbb{Z}}(0) = 0$, $f_{\mathbb{Z}}(1) = \frac{1+1}{2} = 1$ und $f_{\mathbb{Z}}(2) = -\frac{2}{2} = -1$ etc. Intuitiv zählen wir also $\mathbb{Z}$ als $0, 1, -1, 2, -2, 3, -3, ...$ auf.

Behauptung. f ist surjektiv.

Beweis. Sei $z \in \mathbb{Z}$ beliebig. Falls $z \leqslant 0$, so ist $z = f_{\mathbb{Z}}(-2z)$. Falls $z > 0$, so ist $z = f(2z - 1)$.

Wir betrachten als nächstes $\mathbb{Q}$. Wir verzichten hier auf einen formalen Beweis und geben nur intuitiv an, wie man eine Aufzählung von $\mathbb{Q}_+ = \{q \in \mathbb{Q} : q > 0\}$ erhält. Dieses Argument wird als *Cantors erstes Diagonalisierungsargument* bezeichnet. Abbildung 4.1 zeigt, wie man $\mathbb{Q}$ aufzählen kann, indem man den Pfeilen folgt. □

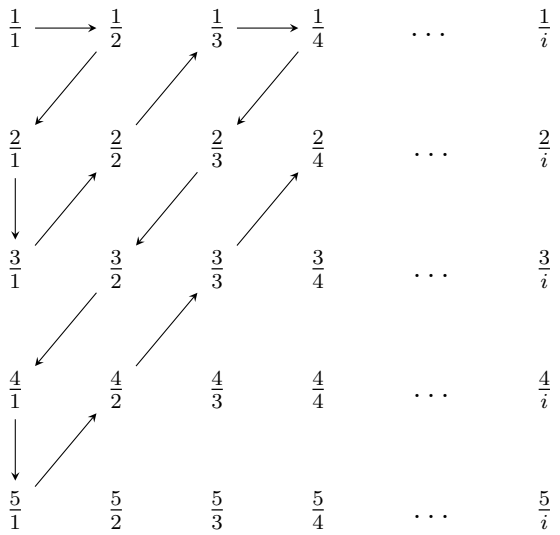


Abbildung 4.1.: Abzählbarkeit von $\mathbb{Q}$.

4.42 Satz. *Für jede Menge M gilt* $\mathrm{card}(M) < \mathrm{card}(\mathcal{P}(M))$.

Beweis: Es ist zu zeigen, dass es eine Injektion von M nach $\mathcal{P}(M)$ gibt, aber keine Surjektion.

Injektion. Definiere $F : M \to \mathcal{P}(M)$ als $F(m) := \{m\}$ für alle $m \in M$. Offensichtlich ist F injektiv.

Surjektion. Wir müssen noch zeigen, dass es keine Surjektion von M nach $\mathcal{P}(M)$ gibt.

Wir beweisen dies durch Widerspruch.

Angenommen, es gäbe eine totale, surjektive Funktion F von M nach $\mathcal{P}(M)$. Sei $N := \{m \in M : m \notin F(m)\}$.

Es ist klar, dass $N \in \mathcal{P}(M)$. Da F surjektiv ist, existiert ein $n \in M$ mit $F(n) = N$. Dann gilt aber

$$\begin{array}{lll} n \in F(n) & \text{gdw.} \quad n \in N & \text{da } F(n) = N \\ & \text{gdw.} \quad n \notin F(n) & \text{nach Definition von } N. \end{array}$$

□

Das im vorherigen Beweis verwendete Argument wird als *Cantors zweites Diagonalisierungsargument* bezeichnet.

Wir erläutern den Namen anhand des Spezialfalls $M = \mathbb{N}$, also der Behautung, dass $\mathrm{card}(\mathbb{N}) < \mathrm{card}(\mathcal{P}(\mathbb{N}))$. Wiederum nehmen wir an, es gäbe eine Surjektion F von $\mathbb{N}$ nach $\mathcal{P}(\mathbb{N})$. Wir repräsentieren F durch folgende unendliche Matrix.

	0	1	2	3	4	5	6	7	8	9	10	$\cdots$	i	$\cdots$
0	**0**	0	1	0	1	1	0	1	1	0	0	$\cdots$		
1	1	**1**	1	1	0	1	1	0	1	0	0	$\cdots$		
2	1	1	**0**	1	1	0	1	0	1	1	1	$\cdots$		
3	0	1	0	**1**	0	0	1	0	1	1	1	$\cdots$		
4	0	0	0	1	**1**	0	0	0	1	1	1	$\cdots$		
5	1	0	0	1	0	**0**	0	0	1	0	1	$\cdots$		
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$			
i	1	0	0	1	0	0	1	1	0	1	1	$\cdots$	$\mathbf{a_{i,i}}$	$\cdots$

Wir bezeichnen den Eintrag in Zeile i und Spalte j als $a_{i,j}$. In jeder Zeile i wird die Menge $F(i)$ repräsentiert, indem wir in Spalte mit Nummer j eine 1 schreiben, wenn $j \in F(i)$. D.h. für $i = 1$ wären im Beispiel oben also $2, 4, 5, 7, 8 \in F(0)$, $0, 1, 3, 6, 9, 10$ hingegen nicht. Man betrachte nun die *Diagonale*, also die Folge $a_{0,0}, a_{1,1}, \ldots$. Diese bezeichnet auch eine Teilmenge D

von $\mathbb{N}$, wobei $i \in D$ wenn $a_{i,i} = 1$. Wir können nun die Menge N bilden, wobei für alle $i \in \mathbb{N}$ gilt: $i \in N$ genau dann, wenn $a_{i,i} = 0$. Anders formuliert erhalten wir die Menge N wie folgt. Sei für alle $i \in \mathbb{N}$, $b_{i,i} := 1 - a_{i,i}$. D.h. wir erhalten die Sequenz $b_{0,0}, \ldots$ dadurch, dass wir die Werte in der Sequenz $a_{i,i}, \cdots$ "umdrehen". Die Sequenz $b_{0,0}, \ldots$ entspricht auch einer Menge N' mit $i \in N'$ wenn $b_{i,i} = 1$. Offensichtlich ist $N = N'$.

Da F surjektiv ist, muss es also ein n geben mit $F(n) = N$. Dann gilt aber: Per Definition der Matrix steht an Stelle (n, n) der Wert $a_{n,n}$. Dieser ist 1, wenn $n \in F(n)$. Das ist aber genau dann der Fall, wenn $b_{n,n} = 0$ ist und somit $n \notin N$, was einen Widerspruch ergibt.

4.43 Einschub (Beweis durch Widerspruch.)**.** Im letzten Beweis haben wir eine wichtige Beweismethode kennen gelernt, die *Widerspruchsbeweis* genannt wird.

Abstrakt wollen wir eine Aussage P dadurch beweisen, in dem wir das Gegenteil $\neg P$ annehmen und zeigen, dass dies zu einem Widerspruch führt.

Oft hat die Aussage P die Form:

> Wenn die Voraussetzungen A erfüllt sind, dann gilt die Aussage B.

Beim Widerspruchsbeweis nimmt man dann an, dass die Voraussetzungen A erfüllt sind, aber B falsch ist. Dies führt man dann zu einem Widerspruch. Damit ist gezeigt, dass in jedem Fall, in dem die Voraussetzungen A erfüllt sind, auch die Folgerung B gelten muss. ⊣

4.44 Einschub (Beweis durch Kontraposition.)**.** Eine Variante des Widerspruchsbeweis ist der *Beweis durch Kontraposition*.

Hier wollen wir eine Aussage der folgenden Form beweisen.

> Wenn die Voraussetzungen A erfüllt sind, dann gilt die Aussage B.

Beim Beweis durch Kontraposition zeigt man diese Aussagen, indem man folgendes beweist:

> Wenn B falsch ist, dann ist auch A falsch.

Wir nehmen also an, dass B nicht gilt und folgern daraus dann, dass auch A falsch sein muss. ⊣

Wir werden als nächstes eine weitere wichtige Beweistechnik kennen lernen, den Beweis durch vollständige Induktion. Wir führen zunächst abstrakt die Beweistechnik ein und demonstrieren sie dann anhand des folgenden Lemmas.

4.45 Lemma. *Seien A, B endliche Mengen. Dann gilt*

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

4.46 Einschub (Beweis durch vollständige Induktion)**.** Wir betrachten zunächst abstrakt das Beweisprinzip der vollständigen Induktion. Sei dazu $A(n)$ eine Aussage über die natürlich Zahl n. Im Fall des Lemmas 4.45 könnte die Aussage $A(n)$ z.B. wie folgt sein: Wir fixieren eine Menge B. Dann ist $A(n)$ die Aussage, dass für jede Menge A mit $|A| = n$ gilt: $|A \cup B| = |A| + |B| - |A \cap B|$. Um Lemma 4.45 zu beweisen, müssen wir also die Aussage $A(n)$ für jede Zahl n beweisen.

Sei nun $A(n)$ eine beliebige Aussage über n. Wir wollen zeigen, dass $A(n)$ für alle $n \in \mathbb{N}$ gilt. Das Prinzip der vollständigen Induktion besteht aus folgenden Schritten:

(1) Wir zeigen zunächst, dass $A(0)$ gilt, d.h. $A(n)$ für $n = 0$. Dieser Schritt heißt *Induktionsverankerung* oder auch *Induktionsanfang*.

(2) Als nächstes zeigen wir, dass wenn die Aussage $A(n)$ für ein $n \in \mathbb{N}$ gilt, dann gilt auch $A(n+1)$. Genauer:

Induktionsvoraussetzung (I.V.). Wir nehmen an, dass $A(n)$ für ein $n \geqslant 0$ gilt.

Induktionsschritt. Unter der Induktionsvoraussetzung zeigen wir nun, dass auch $A(n+1)$ gilt.

Wenn man beide Teile gezeigt hat, folgt daraus, dass die Aussage $A(n)$ für alle $n \in \mathbb{N}$ gilt. Denn aus der Induktionsverankerung folgt die Aussage $A(n)$ für $n = 0$. Wegen Schritt 2 folgt daraus aber auch $A(n)$ für $n = 1$ und wiederum mit Schritt 2 auch $A(n)$ für $n = 2$ und so weiter. Da man jede natürliche Zahl dadurch erzeugen kann, dass man bei 0 beginnend immer wieder 1 aufaddiert, erhält man auf diese Art die Aussage $A(n)$ für jede Zahl $n \in \mathbb{N}$.

Wir verwenden nun das Prinzip der vollständigen Induktion zum Beweis des Lemmas 4.45.

Beweis von Lemma 4.45. Sei B eine beliebige Menge die wir für den Rest des Beweises fixieren.

Wir wollen die Aussage

$$A(n) : \textit{für alle Mengen } A \textit{ mit } |A| = n \textit{ gilt: } |A \cup B| = |A| + |B| - |A \cap B|$$

zeigen.

Induktionsverankerung. Wir zeigen $A(0)$: für alle Mengen A mit $|A| = 0$ gilt $|A \cup B| = |A| + |B| - |A \cap B|$. Da nur die leere Menge keine Elemente enthält gilt also $A = \varnothing$ und somit $A \cup B = B$ sowie $A \cap B = \varnothing$. Also gilt $|A \cup B| = |B| = |A| + |B| - |A \cap B|$.

Induktionsvoraussetzung. Es gilt $A(n)$ für ein $n \in \mathbb{N}$. D.h. es gilt $|A \cup B| = |A| + |B| - |A \cap B|$ für alle Mengen A mit $|A| = n$.

Induktionsschritt. Wir müssen zeigen, dass $A(n+1)$ gilt, das heißt, dass $|A \cup B| = |A| + |B| - |A \cap B|$ für alle Mengen A mit $n+1$ Elementen gilt.

Sei also A eine solche Menge mit $|A| = n+1 > 0$. Sei $a \in A$ beliebig und sei $A' := A \setminus \{a\}$. Also gilt $|A'| = n$ und somit, nach Induktionsvoraussetzung, $|A' \cup B| = |A'| + |B| - |A' \cap B|$.

Wir unterscheiden zwei Fälle:

Fall 1: $a \in B$. Dann gilt

$$|A' \cup B| = |A \cup B| \text{ und } |A' \cap B| = |A \cap B| - 1. \tag{4.1}$$

Also gilt nun

$$\begin{array}{rcll} |A \cup B| & = & |A' \cup B| & \text{nach (4.1)} \\ & = & |A'| + |B| - |A' \cap B| & \text{nach I.V.} \\ & = & (|A| - 1) + |B| - (|A \cap B| - 1) & \text{nach (4.1)} \\ & = & |A| + |B| - |A \cap B| & \end{array}$$

was zu zeigen war.

Fall 2: $a \notin B$. Dann gilt

$$|A \cup B| = |A' \cup B| + 1 \text{ und } |A \cap B| = |A' \cap B| \tag{4.2}$$

Also gilt

$$\begin{array}{rcll} |A \cup B| & = & |A' \cup B| + 1 & \text{nach (4.2)} \\ & = & \big(|A'| + |B| - |A' \cap B|\big) + 1 & \text{nach I.V.} \\ & = & \big((|A| - 1) + |B| - |A \cap B|\big) + 1 & \text{nach (4.2)} \\ & = & |A| + |B| - |A \cap B| & \end{array}$$

was zu zeigen war.

In beiden Fällen ergibt sich also die Behauptung.

□

4.47 Einschub. In vielen Situationen sind leichte Varianten des Prinzips der vollständigen Induktion sehr nützlich.

Variante 1.

Induktionsverankerung. Man zeigt $A(0)$.

Induktionsvoraussetzung. Es gilt $A(0), \ldots, A(n)$.

Induktionsschritt. Zu zeigen ist, dass $A(n+1)$ gilt.

In dieser Variante verwendet man eine stärkere Voraussetzung, nämlich dass die Aussage schon für alle $i \leqslant n$ gezeigt ist. Das ist oft sehr praktisch.

Variante 2. Sei $n_0 \in \mathbb{N}$.

Induktionsverankerung. Man zeigt $A(n_0)$.

Induktionsvoraussetzung. Es gilt $A(n)$ für ein $n \geqslant n_0$.

Induktionsschritt. Zu zeigen ist, dass $A(n+1)$ gilt.

In dieser Variante verankert man die Induktion nicht bei 0 sondern bei einer beliebigen Zahl n_0. Auf diese Weise kann man aber auch nur beweisen, dass $A(n)$ für alle $n \geqslant n_0$ gilt. Für die ersten Zahlen $0, ..., n_0 - 1$ ist damit nichts bewiesen.

Natürlich kann man die Varianten 1 und 2 auch kombinieren.

4.5. Umkehrabbildungen

4.48 Definition. Seien M, N Mengen und sei $R : (M, N)$ eine Relation. Die *Umkehrrelation* $R^{-1} : (N, M)$ ist definiert als

$$R^{-1} := \{(n, m) : m \in M, n \in N \text{ und } (m, n) \in R\}.$$

4.49 Beispiel. Seien $M, N := \mathbb{N}$ und sei $R := \{(1, 3), (1, 5), (1, 7), (3, 7)\}$. Dann ist $R^{-1} := \{(3, 1), (5, 1), (7, 1), (7, 3)\}$.

4.50 Bemerkung. Da Funktionen spezielle Relationen sind, nämlich rechtseindeutige Relationen, liefert dies auch einen Begriff der Umkehrfunktion f^{-1} zu einer Funktion f. Man beachte aber, dass f^{-1} nicht unbedingt eine Funktion ist.

4.51 Beispiel. Seien $M, N := \mathbb{N}$. Sei $f : M \to N$ gegeben durch $f(n) := 1$ für alle $n \in \mathbb{N}$. Dann ist $f^{-1} := \{(1, n) : n \in \mathbb{N}\}$ und somit keine Funktion.

Allerdings ist die Umkehrrelation einer Funktion immer injektiv.

4.52 Lemma. *Seien M, N Mengen. Sei $f : M \to N$ eine partielle Abbildung. Dann ist f^{-1} injektiv.*

Beweis. Beweis durch Widerspruch. Angenommen, f^{-1} sei nicht injektiv. Dann existieren also $n, n' \in \mathbb{N}$ mit $n \neq n'$ und ein $m \in M$ so dass $(n, m) \in f^{-1}$ und $(n', m) \in f^{-1}$. Also gilt, nach Definition von f^{-1}, dass $(m, n) \in f$ und $(m, n') \in f$, im Widerspruch dazu, dass f eine Funktion ist. □

Wir können also nicht immer die Umkehrfunktion zu jeder Funktion bilden, jedenfalls ist das nicht immer eine Funktion. Wie das folgende Lemma zeigt, geht das aber immer für injektive Funktionen.

4.53 Lemma. *Seien M, N Mengen. Sei $f : M \to N$ eine partielle Abbildung. Ist f injektiv, dann ist auch die Umkehrabbildung $f^{-1} : (N, M)$ eine injektive partielle Abbildung.*

Beweis. Wir haben schon in Lemma 4.52 gezeigt, dass f^{-1} injektiv ist. Es bleibt also noch zu zeigen, dass f^{-1} rechtseindeutig ist. Seien also $n \in N$ und $m, m' \in M$ mit $m \neq m'$ und sei $(n, m) \in f^{-1}$ und $(n, m') \in f^{-1}$. Also gilt $(m, n) \in f$ und $(m, n') \in f$ und somit, da f injektiv ist, $n = n'$. □

Zum Abschluss des Abschnitts beweisen wir noch einige einfache Eigenschaften von Umkehrrelationen.

4.54 Lemma. *Seien A, B, C Mengen und $R : (A, B)$ und $Q : (B, C)$ Relationen. Es gilt*

(1) $(R^{-1})^{-1} = R$

(2) $(R; Q)^{-1} = Q^{-1}; R^{-1}$.

Beweis. Teil 1 folgt sofort aus der Definition. Wir beweisen also noch Teil 2. Zur Erinnerung: Es gilt $R; Q = \{(a, c) :$ es existiert $b \in B$ mit $(a, b) \in R$ und $(b, c) \in Q\}$.

Also gilt für alle m, n:

$$\begin{array}{lll} (m,n) \in (R;Q)^{-1} & \text{gdw.} & (n,m) \in R;Q \\ & \text{gdw.} & \text{es ex. } b \in B \text{ mit } (n,b) \in P \text{ und } (b,m) \in Q \\ & \text{gdw.} & \text{es ex. } b \in B \text{ mit } (b,n) \in R^{-1} \text{ und } (m,b) \in Q^{-1} \\ & \text{gdw.} & (m,n) \in Q^{-1}; R^{-1} \end{array}$$

□

4.5.1. Multimengen, Indexmengen und Mengenfamilien

Die folgende Definition liefert eine Art Mengen zu definieren, die oft sehr nützlich ist.

4.55 Definition (Indexmengen und Mengenfamilien)**.** Sei M eine Menge von Mengen und I eine Menge, die wir *Indexmenge* nennen.

Eine surjektive totale Abbildung $A : I \to M$ heißt *Mengenfamilie*. Wir schreiben die Familie meistens als $(A_i)_{i\in I}$, wobei $A_i := A(i)$.

4.56 Definition. Sei M eine Menge von Mengen. Dann gilt:

$$\begin{array}{rcl} \bigcup M & := & \{x : \text{ es ex. } m \in M \text{ mit } x \in m\} \\ \bigcap M & := & \{x : \text{ für alle } m \in M \text{ gilt } x \in m\} \end{array}$$

Als Spezialfälle werden häufig indizierte Vereinigungen verwendet.

$$\begin{array}{rcl} \bigcup_{i\in I} m_i & := & \{x : \text{ es ex. } i \in I \text{ mit } x \in m_i\} \\ \bigcap_{i\in I} m_i & := & \{x : \text{ für alle } i \in I \text{ gilt } x \in m_i\} \end{array}$$

Per Definition kommt in einer Menge jedes Element höchstens einmal vor. Bisweilen möchte man diese Restriktion etwas lockern. Das führt zum Begriff der Multimengen.

4.57 Definition (Multimengen)**.** Sei A eine Menge. Dann bezeichnet eine totale Abbildung $M_T : A \to \mathbb{N}$ eine sogenannte *Multimenge* T. Die *Größe* einer Multimenge T ist $|T| := \sum_{a\in A} M_T(a)$.

5. Ordnungen und Äquivalenzen

In diesem Kapitel behandeln wir zwei fundamentale Klassen von Relationen, *Ordnungen* und *Äquivalenzrelationen*. Zunächst definieren wir einige wichtige Eigenschaften von Relationen. Deren Kombinationen ergeben dann Ordnungen oder Äquivalenzrelationen.

5.1 Definition (Eigenschaften von Relationen)**.** Sei A eine Menge und $R : (A, A)$ eine Relation. R heißt

- *reflexiv*, wenn $(a, a) \in R$ für alle $a \in A$.
- *irreflexiv*, wenn $(a, a) \notin R$ für alle $a \in A$.
- *symmetrisch*, wenn für alle $a, b \in A$ gilt: wenn $(a, b) \in R$ dann auch $(b, a) \in R$.
- *antisymmetrisch*, wenn für alle $a, b \in A$ gilt: wenn $(a, b) \in R$ und $(b, a) \in R$ dann ist $a = b$.
- *transitiv*, wenn für alle $a, b, c \in A$ gilt: wenn $(a, b) \in R$ und $(b, c) \in R$ dann auch $(a, c) \in R$.
- *linear*, wenn für alle $a, b \in A$ gilt: $(a, b) \in R$ oder $(b, a) \in R$.

5.1. Ordnungen

5.1.1. Partielle und Lineare Ordnungen

5.2 Definition (Ordnungen)**.** Sei A eine Menge.

- Eine *Quasiordnung*, oder auch *Präordnung*, über A ist eine reflexive und transitive Relation $R : (A, A)$.
- Eine *partielle Ordnung*, oder *Halbordnung*, über A ist eine reflexive, transitive und antisymmetrische Relation $R : (A, A)$.

- Eine *totale Ordnung*, oder *lineare Ordnung*, über A ist eine reflexive, transitive, antisymmetrische und lineare Relation $R : (A, A)$.

Die folgende Tabelle benennt die Mindestkriterien, so dass für R der jeweilige Ordnungsbegriff gilt.

Ordnungsbegriff	reflexiv	transitiv	antisymmetrisch	linear
Quasiordnung	•	•		
partielle Ordnung	•	•	•	
totale Ordnung	•	•	•	•

Oft verwenden wir auch die entsprechenden irreflexiven Relationen und nennen diese *strikt*.

5.3 Definition. Eine *strikte lineare Ordnung* über einer Menge A ist eine irreflexive, transitive, antisymmetrische und lineare Relation $R : (A, A)$.

5.4 Beispiel.

- Die Relation $R_{\mathbb{N}} : (\mathbb{N}, \mathbb{N})$ definiert als $R_{\mathbb{N}} := \{(n, m) : n \leqslant m\}$ ist eine lineare Ordnung.
- Sei M eine Menge. Die Relation $R_{\subseteq} : (\mathcal{P}(M), \mathcal{P}(M))$ definiert als

  $$R_{\subseteq} := \big\{(N, M) : N \subseteq M\big\}$$

  ist eine partielle Ordnung.
- Sei $\mathbb{R}_+ := \{r : r \in \mathbb{R}, r > 0\}$. Die Relation $R_{\mathbb{R}} : (\mathbb{R}_+, \mathbb{R}_+)$ definiert als $R_{\mathbb{R}} := \{(n, m) : m \leqslant 2 * n\}$ ist eine strikte lineare Ordnung auf $\mathbb{R}_+$.

5.5 Notation. Wir verwenden für Ordnungen üblicherweise Symbole wie $\leqslant$ oder $<$ und schreiben sie in Infixschreibweise. D.h. anstatt $(m, n) \in \leqslant$ schreiben wir wie gewöhnlich $m \leqslant n$.

5.1.2. Wohl-Fundierte und Wohl-Quasi-Ordnungen

Wir behandeln noch zwei wichtige Spezialfälle von Ordnungen.

5.6 Definition (wohl-fundierte Ordnungen und Wohl-Quasi-Ordnungen)**.** Sei M eine Menge.

(1) Eine lineare Ordnung $\leqslant : (M, M)$ heißt *wohl-fundiert*, wenn es keine bzgl. $\leqslant$ unendlichen echt absteigenden Ketten $a_1 \geqslant a_2 \geqslant a_3 ....$ mit $a_i \neq a_j$ für alle $1 \leqslant i < j$ gibt. Formal ausgedrückt ist $\leqslant$ eine wohl-fundierte lineare Ordnung, wenn es in jeder unendlichen Folge $(a_1, \ldots,)$ mindestens ein Paar $i < j$ gibt, so dass $a_i \leqslant a_j$.

(2) Eine Quasiordnung $\leqslant : (M, M)$ heißt *Wohl-Quasi-Ordnung*, wenn es in jeder unendlichen Folge $(a_1, a_2, \dots)$ von Elementen aus M ein Paar $i < j$ gibt mit $a_i \leqslant a_j$.

In Wohl-Quasi-Ordnungen gibt es also weder unendlich lange absteigende Ketten noch unendliche Folgen von paarweise unvergleichbaren Elementen.

5.7 Beispiel. Betrachten wir noch einmal die Ordnungen aus Beispiel 5.4.

- Die Relation R_N ist eine wohl-fundierte lineare Ordnung.
- Die Relation $R_{\mathbb{R}}$ ist hingegen nicht wohl-fundiert.
- Die Relation $R_{\subseteq}$ ist nur dann eine Wohl-Quasi-Ordnung, wenn M endlich ist.

Wohl-Quasi-Ordnungen haben folgende interessante Eigenschaft.

5.8 Lemma. *Sei M eine Menge und $\leqslant$ eine Wohl-Quasi-Ordnung auf M. Sei $A \subseteq M$ eine Menge, die* unter $\leqslant$ abgeschlossen *ist, d.h. so dass für alle $m, n \in M$ mit $n \leqslant m$ gilt: Wenn $m \in A$ dann auch $n \in A$. Dann existiert eine endliche Menge $O \subseteq M \setminus A$, so dass für alle $a \in M$ gilt: $a \in A$ genau dann, wenn es kein $o \in O$ gibt mit $o \leqslant a$.*

Beweis. Wir definieren

$$O := \{m \in M : m \notin A \text{ und es gibt kein } n \in M \setminus A \text{ so dass } n \leqslant m \text{ und } n \neq m\}.$$

Nun gilt für alle $a \in M$: $a \in A$ genau dann, wenn es kein $o \in O$ gibt mit $o \leqslant a$. Denn wenn $a \in A$, dann sind auch alle $b \leqslant a$ in A und somit kann es nach Definition von O kein $o \in O$ geben mit $o \leqslant a$. Andererseits, wenn es ein $o \in O$ gibt mit $o \leqslant a$, dann kann a nicht in A sein, denn sonst wäre ja auch $o \in A$ im Widerspruch zur Definition von O.

Es bleibt also nur noch zu zeigen, dass O endlich ist. Nach Definition von O gibt es aber keine $o, o' \in O$ mit $o \neq o'$ und $o \leqslant o'$. Da $\leqslant$ aber eine Wohl-Quasi-Ordnung ist, muss also O endlich sein. □

Das Lemma hat folgende interessante Folgerung.

5.9 Korollar. *Sei M eine Menge und $\leqslant$ eine Wohl-Quasi-Ordnung auf M. Angenommen, wir können für jedes Paar $a, b \in M$ in Polynomialzeit entscheiden, ob $a \leqslant b$.*

Dann kann jede unter $\leqslant$ abgeschlossene Teilmenge in Polynomialzeit entschieden werden.

Genauer: Ist $A \subseteq M$ eine Menge mit der Eigenschaft, dass für alle $a, b \in M$ mit $a \leqslant b$ gilt: Wenn $b \in A$ dann auch $a \in A$. Dann gibt es einen Algorithmus der in Polynomialzeit für alle $a \in M$ entscheidet, ob $a \in A$.

Beweis. Nach Lemma 5.8 gibt es eine endliche Menge $O \subseteq M \setminus A$ so dass für alle $a \in M$ gilt: $a \in A$ genau dann, wenn es kein $o \in O$ gibt mit $o \leqslant a$.

Um zu entscheiden, ob ein $a \in M$ in A enthalten ist, brauchen wir also nur für alle $o \in O$ zu entscheiden, ob $o \leqslant a$. Da jeder dieser Tests in Polynomialzeit durchgeführt werden kann und O selbst endlich ist, ist dies ein Polynomialzeitverfahren. □

5.10 Bemerkung. (1) Man beachte, dass wir nur die *Existenz* eines solchen Algorithmus bewiesen haben. Da wir aber im Allgemeinen nicht wissen, wie die Menge O aussieht, können wir den Algorithmus im Allgemeinen auch nicht konkret angeben. Wir nennen solche Verfahren *nichtkonstruktiv*, da wir zwar wissen, dass es einen effizienten Algorithmus gibt, ihn aber nicht konstruieren können.

(2) Die Menge O, die wir zu einer Teilmenge $A \subseteq M$ konstruiert haben, nennt man *Obstruktion* (engl. obstruction) für A.

5.1.3. Minimale Elemente in Partiellen Ordnungen

5.11 Definition (Partiell geordnete Mengen)**.** Eine *partiell geordnete Menge* (engl. partially ordered set, poset) ist ein Paar $(M, \preceq)$ bestehend aus einer Menge M und einer partiellen Ordnung $\preceq$ auf M.

5.12 Definition (Minimale und Maximale Elemente)**.** Sei $(M, \preceq)$ eine partiell geordnete Menge.

(1) Ein Element $m \in M$ heißt *minimales Element* von $\preceq$, oder $\preceq$-minimales Element, wenn es kein $n \in M$ gibt mit $n \neq m$ und $n \preceq m$.

(2) Ein Element $m \in M$ heißt *maximales Element* von $\preceq$, oder $\preceq$-maximales Element, wenn es kein $n \in M$ gibt mit $n \neq m$ und $m \preceq n$.

Wir zeigen als nächstes, dass jede endliche partielle Ordnung mindestens ein minimales und mindestens ein maximales Element enthält.

5.13 Satz. *Sei $(M, \preceq)$ eine partiell geordnete Menge. Dann enthält M mindestens ein $\preceq$-minimales Element.*

Beweis: Für jedes $a \in M$ definieren wir die Menge $L(a) := \{n \in M : n \preceq a\}$. Sei nun $z := \min\{|L(a)| : a \in M\}$ und sei $m \in M$ ein Element so dass $|L(m)| = z$. Wir behaupten, dass m ein $\preceq$-minimales Element ist. Angenommen, es gäbe ein n mit $n \preceq m$ und $n \neq m$. Da $\preceq$ transitiv ist (nach Definition einer Ordnung), gilt $L(n) \subseteq L(m)$. Da aber $m \notin L(n)$ und $L(n)$ sowie $L(m)$ endlich sind, folgt $|L(n)| < |L(m)|$, im Widerspruch zur Wahl von m. □

Auf ähnliche Weise kann man auch zeigen, dass jede endliche durch eine Relation $\preceq$ partielle geordnete Menge auch ein $\preceq$-maximales Element enthält. Man beachte aber, dass die entsprechende Aussage für unendliche Mengen falsch ist. So hat z.B. die Menge $\mathbb{Z}$ bzgl. der üblichen Ordnung $\leqslant$ kein minimales Element.

Neben minimalen Elementen einer Ordnung spielen auch das *kleinste* Element einer Ordnung, oder das Minimum, ein wichtige Rolle.

5.14 Definition. Sei $(M, \preceq)$ eine partiell geordnete Menge.

(1) Ein Element $m \in M$ heißt *kleinstes Element*, oder *Minimum*, von $\preceq$, wenn $m \preceq n$ für alle $n \in M$ gilt.

(2) Ein Element $m \in M$ heißt *größtes Element*, oder *Maximum*, von $\preceq$, wenn $n \preceq m$ für alle $n \in M$ gilt.

Man beachte den Unterschied zwischen kleinsten und minimalen Elementen. Zu einem minimalen Element gibt es kein kleineres, ein Minimum, oder kleinstes Element, hingeben ist kleiner als alle anderen. Nicht jede partielle Ordnung, nicht einmal jede endliche, hat ein Minimum oder ein Maximum.

5.15 Beispiel. (1) Sei $M := \mathbb{N}$ und $\leqslant$ die natürliche Ordnung auf $\mathbb{N}$. Dann ist die 0 sowohl ein minimales als auch ein kleinstes Element von $(\mathbb{N}, \leqslant)$.

(2) Sei nun $M := \mathbb{N} \setminus \{0, 1\}$ und $\preceq$ definiert als $\preceq := \{(n, m) : n, m \in M$ und n teilt m, d.h. es existiert ein $b \in \mathbb{N}$ mit $m = b \cdot n\}$. Dann hat $(M, \preceq)$ kein kleinstes Element aber unendlich viele minimale Elemente (die Primzahlen).

Wir zeigen als letztes noch folgenden Satz, der besagt, dass sich jede partielle Ordnung in eine lineare Ordnung derselben Menge einbetten läßt. Wir beweisen hier den Satz nur für Ordnungen über endlichen Mengen. Der Beweis für unendliche Mengen ist schwieriger und hängt vor allem von der Wahl der Axiome für Mengen ab (insbesondere vom sogenannten Auswahlaxiom).

5.16 Satz. *Sei $(M, \preceq)$ eine partiell geordnete Menge. Dann gibt es eine lineare Ordnung $\leqslant$ auf M, so dass für alle $a, b \in M$ gilt: wenn $a \preceq b$, dann auch $a \leqslant b$. Wir nennen $\leqslant$ eine* lineare Erweiterung *von $\preceq$.*

Beweis: Wir beweisen die Behauptung per Induktion über $n := |M|$.

Induktionsbasis $n := |M| = 1$. Wenn $|M| = 1$, dann enthält M nur ein Element a und $\preceq = \{(a, a)\}$ ist daher schon eine totale Ordnung.

Induktionsvoraussetzung. Die Aussage gilt für alle Mengen M mit n Elementen.

Induktionsschritt. Sei M eine Menge mit $n + 1$ Elementen. Sei $m \in M$ ein minimales Element von M (so ein Element existiert nach Satz 5.13). Sei $M' := M \setminus \{m\}$ und $\preceq'$ die *Restriktion* von $\preceq$ auf M', d.h. die Relation

$$\preceq' := \{(a, b) : a, b \in M', a \preceq b\}.$$

Offensichtlich ist $\preceq'$ eine partielle Ordnung auf M' (die Eigenschaften Reflexivität, Transitivität und Antisymmetrie bleiben erhalten). Nach Induktionsvoraussetzung existiert also eine lineare Ordnung $\leqslant'$ auf M, so dass für alle $a, b \in M'$ gilt: Wenn $a \preceq' b$ dann auch $a \leqslant' b$. Wir definieren nun $\leqslant : (M, M)$ wie folgt: für alle $a, b \in M$

$$a \leqslant b \text{ gdw. } \begin{cases} a = m \text{ oder} \\ a, b \neq m \text{ und } a \leqslant' b. \end{cases}$$

Wir behaupten, dass $\leqslant$ eine lineare Ordnung auf M ist.

- $\leqslant$ ist reflexiv, da $m \leqslant m$ nach Definition gilt und für alle $a \neq m$, also $a \in M'$, $a \leqslant a$ aus der Definition von $\leqslant'$ folgt.
- $\leqslant$ ist antisymmetrisch. Sei dazu $a, b \in M$ mit $a \leqslant b$ und $b \leqslant a$. Zu zeigen ist $a = b$. Wenn $a, b \neq m$, dann folgt dies aus der Antisymmetrie von $\leqslant'$. Wenn aber z.B. $a = m$ dann gilt $b \leqslant a$ nur dann, wenn $b = m$, was zu zeigen war.
- $\leqslant$ ist transitiv. Seien dazu $a, b, c \in M$ mit $a \leqslant b$ und $b \leqslant c$. Wir müssen zeigen, dass $a \leqslant c$. Wenn $a, b, c \neq m$, dann folgt dies sofort aus der Transitivität von $\leqslant'$. Wenn $b = m$ oder $c = m$ dann folgt aus der Definition von $\leqslant$ auch $a = m$. Und wenn $a = m$, dann gilt $a \leqslant c$ per Definition von $\leqslant$.

□

5.2. Äquivalenzrelationen

5.17 Definition (Äquivalenzrelation)**.** Sei M eine Menge. Eine Relation $R : (M, M)$ heißt *Äquivalenzrelation*, wenn R *reflexiv*, *symmetrisch* und *transitiv* ist.

Eine Äquivalenzrelation ist also eine symmetrische Quasi-Ordnung.

5.18 Beispiel. Sei M eine Menge.

(1) Dann ist $\mathrm{Id}_M = \{(m, m) : m \in M, m = m\}$ eine Äquivalenzrelation auf M.

(2) Ebenso ist die Relation $T_M := \{(m, n) : m, n \in M\}$ eine Äquivalenzrelation.

(3) In Definition 3.6 haben wir den Begriff der logischen Äquivalenz $\varphi \equiv \psi$ zwischen Formeln $\varphi, \psi \in A(V)$ der Aussagenlogik kennen gelernt. Für jede Menge V von Variablen ist die Relation $R : (\mathbf{A}(V), \mathbf{A}(V))$ definiert als
$$R := \{(\varphi, \psi) : \varphi \equiv \psi\}$$
eine Äquivalenzrelation auf $\mathbf{A}(V)$.

(4) Sei $k \in N_+$. Zwei Zahlen $n, m \in \mathbb{Z}$ sind *kongruent modulo* k, geschrieben $a \equiv b \mod k$, wenn $(a - b)$ durch k teilbar ist. Dann ist
$$Z_k := \{(a, b) : a, b \in \mathbb{Z}, a \equiv b \mod k\}$$
eine Äquivalenzrelation über $\mathbb{Z}$.

5.19 Definition (Äquivalenzklassen)**.** Sei M eine Menge und $R : (M, M)$ eine Äquivalenzrelation. Sei $a \in M$. Dann heißt
$$[a]_R := \{m \in M : (a, m) \in R\}$$
die *Äquivalenzklasse* von a bzgl. R.

5.20 Notation. Wenn aus dem Zusammenhang klar ist, bzgl. welcher Äquivalenzrelation wir Äquivalenzklassen bilden, dann schreiben wir oft kurz $[a]$ statt $[a]_R$.

Man beachte, dass Äquivalenzklassen selbst Mengen sind. Wir können also die üblichen Mengenoperationen $\subseteq, \cap, ...$ auf Äquivalenzklassen ebenso wie auf Äquivalenzrelationen anwenden.

5.21 Beispiel. Betrachten wir noch einmal Beispiel 5.18, Teil (4). Die Äquivalenzklasse einer Zahl $z \in \mathbb{Z}$ bzgl. Z_k ist die Menge $[z]_{Z_k} := \{x : x \equiv z \mod k\}$.

Bzgl. der Relation R aus Teil (3) ist die Äquivalenzklasse einer Formel φ also gerade die Klasse aller Formeln ψ, die zu φ logisch äquivalent sind.

Das folgende Lemma beweist einige wichtige Eigenschaften von Äquivalenzklassen.

5.22 Lemma. *Sei M eine Menge und $R : (M, M)$ eine Äquivalenzrelation. Für alle $m, n \in M$ gilt:*

(1) $m \in [m]_R$.

(2) $(m, n) \in R$ *genau dann, wenn* $[m]_R = [n]_R$.

(3) $(m, n) \notin R$ *genau dann, wenn* $[m]_R \cap [n]_R = \varnothing$.

Beweis. Teil (1) ist offensichtlich. Zu Teil (2), seien $m, n \in M$. Angenommen, $(m, n) \in R$. Dann ist $[m]_R = \{z : z \in M, (m, z) \in R\}$ und somit, da R transitiv ist, $[m]_R \subseteq \{z : z \in M, (n, z) \in R\}$. Also $[m]_R \subseteq [n]_R$. Völlig symmetrisch folgt $[n]_R \subseteq [m]_R$ und somit $[m]_R = [n]_R$.

Umgekehrt sei $[n]_R = [m]_R$. Dann gilt nach Definition $n \in [m]_R$ und somit $(m, n) \in R$.

Zu Teil (3) seien $m, n \in M$. Wenn $[m]_R \cap [n]_R = \varnothing$, dann gilt $(m, n) \notin R$, da sonst $n \in [m]_R$ und somit $n \in [m]_R \cap [n]_R$.

Sei nun $(m, n) \notin R$. Angenommen, es gäbe ein $b \in [m]_R \cap [n]_R$. Dann ist $(m, b) \in R$ und $(n, b) \in R$, somit auch $(b, n) \in R$ wegen der Symmetrie von R und daher $(m, n) \in R$, wegen der Transitivität von R. Also kann es ein solches b nicht geben. □

In verschiedenen Anwendungen hat man folgendes Problem. Man hat eine Menge M von Objekten und eine Relation, die gewisse Objekte miteinander in Beziehung setzt. Z.B. könnte die Menge M eine Menge von Molekülen sein und die Relation R zwei Moleküle mit einander in Relation setzten, wenn sie "ähnliche" chemische Eigenschaften haben. Man möchte dann gerne die Menge M in Klassen von Molekülen mit ähnlichnen Eigenschaften einteilen. D.h. abstrakt gesehen, möchte man gerne eine möglichst minimale Äquivalenzrelation haben, die R erweitert. Den Schlüssel dazu liefert die nächste Definition.

5.23 Definition. Sei M eine Menge und $R : (M, M)$ eine Relation.

(1) Der *reflexive Abschluss* $r(R)$ von R ist definiert als $r(R) := R \cup \mathrm{Id}_M$.

(2) Der *symmetrische Abschluss* $s(R)$ von R ist definiert als $s(R) := R \cup R^{-1}$.

(3) Für $n \in N_+$ definieren wir R^n induktiv wie folgt: $R^1 := R$ und für $n > 1$ ist $R^n := R; R^n$. Der *transitive Abschluss* $t(R)$ von R ist definiert als $t(R) := \bigcup_{n \in \mathbb{N}_+} R^n$.

Man beachte, dass der Typ des reflexiven, symmetrischen oder transitiven Abschlusses immer noch (M, M) ist. Wir können also verschiedene Abschlüsse schachteln.

5.24 Lemma. *Sei M eine Menge und $R : (M, M)$ eine Relation.*

(1) *$r(R)$ ist die bzgl. $\subseteq$ kleinste reflexive Obermenge von R.*

(2) *$s(R)$ ist die bzgl. $\subseteq$ kleinste symmetrische Obermenge von R.*

(3) *$t(R)$ ist die bzgl. $\subseteq$ kleinste transitive Obermenge von R.*

(4) *$t(s(r(R)))$ ist die bzgl. $\subseteq$ kleinste Äquivalenzrelation, die Obermenge von R ist.*

Beweis: Wir zeigen hier exemplarisch den Fall (1). Offensichtlich ist $r(R)$ eine Obermenge von R und reflexiv. Wir müssen also nur zeigen, dass für jede andere reflexive Obermenge $R' \supseteq R$ von R gilt: $r(R) \subseteq R'$. Sei also $(m, n) \in r(R)$. Nach Definition von $r(R)$ ist $(m, n) \in R$ oder aber $m = n$. Da R' reflexiv ist und $R \subseteq R'$, ist also in beiden Fällen $(m, n) \in R'$. Somit gilt $r(R) \subseteq R'$.

Die anderen Fälle lassen sich ähnlich beweisen. □

5.25 Definition (Quotienten)**.** Sei M eine Menge und $R : (M, M)$ eine Äquivalenzrelation. Die Menge M/R aller Äquivalenzklassen, definiert als

$$M/R := \{[m]_R : m \in M\}$$

heißt der *Quotient* von M bzgl. R.

5.26 Beispiel. Betrachten wir noch einmal Beispiel 5.18, Teil (4). Die Äquivalenzklasse einer Zahl $z \in \mathbb{Z}$ bzgl. Z_k ist die Menge $[z]_{Z_k} := \{x : x \equiv z \mod k\}$. Der Quotient ist dann $\{[z]_{Z_k} : x \in Z\}$.

5.27 Definition. Sei M eine Menge und $R : (M, M)$ eine Äquivalenzrelation. Eine Menge $S \subseteq M$ heißt ein *Repräsentatensystem von A/R*, wenn es für alle $m \in M$ genau ein $s \in S$ gibt, so dass $s \in [m]_R$.

Repräsentatensysteme enthalten aus jeder Äquivalenzklasse bzgl. R genau einen *Repräsentanten*. Wenn man die Elemente einer Äquivalenzklasse bzgl. R als "gleich" auffasst, beschreibt also S die Menge M vollständig bis auf diese "Gleichheit". S ist aber auch die kleinste Menge mit dieser Eigenschaft, da jede echt kleinere Menge eine Äquivalenzklasse "vergisst" und damit nicht repräsentiert.

Die folgende Proposition formalisiert diese Aussage. Der Beweis folgt sofort aus der Definition eines Repräsentantensystems.

5.28 Proposition. *Sei M eine Menge, $R : (M, M)$ eine Äquivalenzrelation und $S \subseteq M$ ein Repräsentantensystem von M/R.*

(1) *Es gibt eine Bijektion zwischen S und M/R.*

(2) $M = \bigcup_{s \in S} [s]_R$.

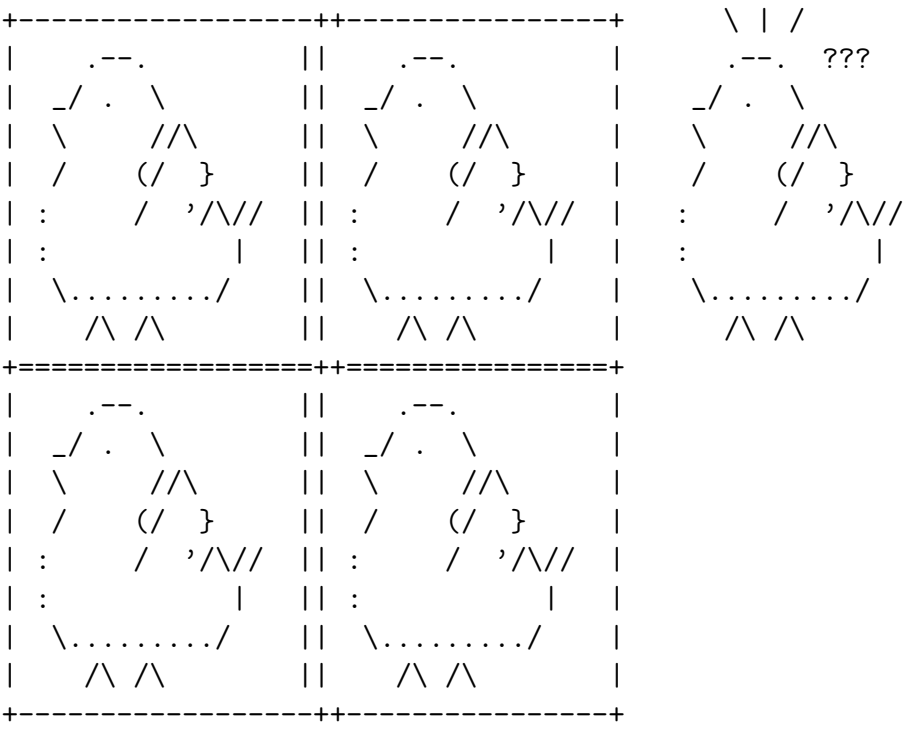
6. Kombinatorik

6.1. Das Schubfachprinzip

Wir beginnen mit einem einfachen aber wichtigen Beweisprinzip.

6.1 Satz. *Seien M, N endliche Mengen mit $|N| = n \in \mathbb{N}$ und $|M| = m \in \mathbb{N}$. Wenn $m < n$, dann existiert keine injektive Abbildung $f : N \to M$.*

Der Satz ist besser bekannt als das Schubfachprinzip (Pigeonhole principle, Taubenschlagprinzip). Es besagt, dass immer wenn man n Objekte auf weniger als n Fächern verteilen will, wird es ein Fach mit mindestens zwei Objekten geben. In der Abbildung muss die fünfte Taube in ein Häuschen rein, das schon belegt ist und somit wird es in einem der vier Häuschen zwei Tauben geben:



Der Beweis des Satzes erfolgt per Induktion über n und wird dem Leser als Übung überlassen.

6.2. Zählen der Elemente einer Menge

6.2 Lemma. *Seien $n \geqslant 1$ und $M_1, \ldots M_n$ endliche Mengen.*

(1) *Wenn $M_i \cap M_j = \varnothing$ für alle $1 \leqslant i < j \leqslant n$ gilt, dann ist*

$$|\bigcup_{i=1}^{n} M_i| = \sum_{i=1}^{n} |M_i|.$$

(2) $|\bigtimes_{i=1}^{n} M_i| = \prod_{i=1}^{n} |M_i|$.

Zur Erinnerung:

$$\bigtimes_{i=1}^{n} M_i = \{\ (m_1,\ \ldots,\ m_n) : m_i \in M_i \text{ für alle } 1 \leqslant i \leqslant n\ \}.$$

Beweis:

(1) Wir haben in Lemma 4.45 schon gezeigt, dass für alle endlichen Mengen A, B gilt: $|A \cup B| = |A| + |B| - |A \cap B|$. Wenn $A \cap B = \varnothing$, gilt demnach $|A \cup B| = |A| + |B|$. Teil (1) folgt sofort per Induktion über n.

(2) Wir beweisen die Aussage per Induktion über n.

Induktionsverankerung. $n = 1$:

$|\bigtimes_{i=1}^{n} M_i| = |\{\ (m_1) : m_1 \in M_1\ \}| = |M_1|$.

Wir zeigen auch $n = 2$:

D.h. zu zeigen ist $|M_1 \times M_2| = |M_1| \cdot |M_2|$

Für $a \in M_1$ sei $P_a := \{\ (a,\ m) : m \in M_2\ \}$. Offensichtlich ist $|P_a| = |M_2|$. Es gilt also: $M_1 \times M_2 = \bigcup_{a \in M_1} P_a$ und für $a, b \in M_1$ mit $a \neq b$ gilt $P_a \cap P_b = \varnothing$. Nach Teil (1) ist also:

$$|M_1 \times M_2| = |\bigcup_{a \in M_1} P_a| \overset{\text{Teil (1)}}{=} \sum_{a \in M_1} |P_a| = \sum_{a \in M_a} |M_2| = |M_1| \cdot |M_2|$$

Induktionsvoraussetzung. Für $n \in \mathbb{N}$ gilt $|\bigtimes_{i=1}^{n} M_i| = \prod_{i=1}^{n} |M_i|$.

Induktionsschritt. Wir zeigen, dass $|\bigtimes_{i=1}^{n+1} M_i| = \prod_{i=1}^{n+1} |M_i|$. Seien $A := \bigtimes_{i=1}^{n} M_i$, $B := M_{n+1}$ (intuitiv gilt also $\underbrace{M_1 \times \cdots \times M_n}_{:=A} \times \underbrace{M_{n+1}}_{:=B}$).

Wir zeigen zunächst, dass $|A \times B| = |\bigtimes_{i=1}^{n+1} M_i|$. Dazu definieren wir eine Abbildung $f : A \times B \to \bigtimes_{i=1}^{n+1} M_i$ durch

$$((m_1, \ldots, m_n), m_{n+1}) \mapsto (m_1, \ldots, m_{n+1}).$$

Diese Abbildung ist offensichtlich eine Bijektion. Da für beliebige Mengen M und N gilt $|M| = |N|$ genau dann, wenn es eine Bijektion zwischen M und N gibt, folgt die Behauptung.

Wir müssen also nur noch zu zeigen, dass $|A \times B| = \prod_{i=1}^{n+1} |M_i|$.

$$|A \times B| \overset{\text{Nach Fall } n=2}{=} |A| \cdot |B| \overset{\text{IV}}{=} \prod_{i=1}^{n} |M_i| \cdot \underbrace{|B|}_{=|M_{n+1}|} = \prod_{i=1}^{n+1} |M_i|$$

□

6.3. Permutationen

6.3 Definition (Permutation)**.** Sei M eine Menge. Eine *Permutation* auf M ist eine bijektive Abbildung $\pi : M \to M$.

6.4 Beispiel. Sei $M := \{ a, b, c, d \}$.

$$\pi : \begin{array}{cccc} a & b & c & d \\ \downarrow & \downarrow & \downarrow & \downarrow \\ d & a & b & c \end{array}$$

Die Permutationen sind besser bekannt als Abbildungen, die die „Positionen“$(1, \ldots, n)$ der Elemente der Menge vertauschen, d.h. $\pi : \{ 1, \ldots, n \} \to \{ 1, \ldots, n \}$, wobei $n = |M|$. Obige Permutation würde dann geschrieben als

$$\pi : \begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \end{array}$$

⊣

Sei M eine Menge mit $n \in \mathbb{N}$ Elementen. Eine naheliegende Frage ist nun, wieviele Permutationen π es auf der Menge M gibt.

Wir können die Zahl der Permutationen wie folgt berechnen. Sei $M := \{a_1, \ldots, a_n\}$.

- a_1 muss auf ein Element $\pi(a_1) \in M$ abgebildet werden. Dazu gibt es n Möglichkeiten, da wir $\pi(a_1)$ beliebig wählen können.
- a_2 muss auf ein Element $\pi(a_2) \in M \backslash \{ \pi(a_1) \}$ abgebildet werden. Dazu gibt es nur noch $n-1$ Möglichkeiten, da ja $\pi(a_1)$ schon gewählt wurde.
- ...
- a_n muss auf ein Element $\pi(a_n) \in M \backslash \{ \pi(a_1), \ldots, \pi(a_{n-1}) \}$ abgebildet werden. Dazu gibt es nur noch eine Möglichkeitn, da alle anderen Elemente schon gewählt wurden.

Es gibt also $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1 = \prod_{i=1}^{n} i$ Möglichkeiten. Für $n \in \mathbb{N}$ nennen wir diese Zahl die *Fakultät* von n.

6.5 Definition. Für $n \in \mathbb{N}$ definieren wir die *Fakultät* $n!$ von n durch:

$$n! = \begin{cases} 1, & \text{falls } n = 0 \\ \prod_{i=1}^{n} i = n \cdot (n-1)!, & \text{sonst} \end{cases}$$

Obige Überlegung zeigt also folgenden Satz.

6.6 Satz. *Die Anzahl der Permutationen einer Menge M mit n Elementen ist $n!$.*

6.4. Binomialkoeffizienten

Wir werden in diesem Abschnitt die Zahl der Teilmengen einer Menge mit bestimmten Eigenschaften berechnen. Z.B. interessieren wir uns für die Zahl der k-Elementigen Teilmengen einer Menge, oder die Zahl der Möglichkeiten, k Elemente aus einer Menge auszuwählen, wobei die Reihenfolge der Auswahl der Elemente wichtig ist. Solche Zahlen werden z.B. in der Analyse von Algorithmen oft benötigt. Möchte man z.B. die Laufzeit eines Algorithmus' abschätzen, der für alle k-elementigen Teilmengen einer Eingabemenge etwas ausführen soll, dann muss man natürlich wissen, wie viele solcher Mengen es gibt.

Wir erinnern daran, dass für eine n-elementige Menge M gilt: $|\mathcal{P}(M)| = 2^n$, wobei $\mathcal{P}(M)$ die Menge aller Teilmengen von M ist.

6.7 Definition. Sei M eine Menge und $k \in \mathbb{N}$. Wir definieren $\mathcal{P}_k(M) := \{ X : X \subseteq M \text{ und } |X| = k \}$

6.8 Beispiel. Sei $M := \{ 1, 2, 3, 4 \}$. Dann ist

$$\mathcal{P}_3(M) = \{ \{ 1, 2, 3 \}, \{ 2, 3, 4 \}, \{ 1, 2, 4 \}, \{ 1, 3, 4 \} \}.$$

Offensichtlich hängt $|\mathcal{P}_k(M)|$ nur von $|M|$ und nicht von der Menge M selbst ab. Das motiviert die folgende Definition. Dies motiviert die Schreibweise in der folgenden Definition.

6.9 Definition (Binomialkoeffizient)**.** Seien M eine Menge mit n Elementen und $k \in \mathbb{N}$. Der *Binomialkoeffizient* $\binom{n}{k}$ ist definiert als die Anzahl der k-elementigen Teilmengen von M, d.h.

$$\binom{n}{k} := |\mathcal{P}_k(M)|.$$

Wie oben schon gesagt, hängt $\binom{n}{k}$ nur von n ab und nicht von der Wahl von M. Denn wenn M, M' Mengen mit $n = |M| = |M'|$, dann existiert eine Bijektion $\pi : M \to M'$ und somit existiert auch eine Bijektion $\pi_k : \mathcal{P}_k(M) \to \mathcal{P}_k(M')$, definiert durch $\pi_k(X) := \{ \pi(z) : z \in X \}$, für alle $X \in \mathcal{P}_k(M)$. Da π eine Bijektion ist, und insbesondere also injektiv, ist $\pi_k(X)$ wieder eine k-elementige Menge. Man sieht nun leicht, dass π_k eine Bijektion ist und somit gilt $|\mathcal{P}_k(M)| = |\mathcal{P}_k(M')|$.

6.4.1. Eigenschaften des Binomialkoeffizienten

Die folgende Beobachtung fasst einige leichte Eigenschaften von Binomialkoeffizienten zusammen.

6.10 Beobachtung. Für alle $n \in \mathbb{N}$ gilt:

(1) $\binom{n}{k} = 0$ für alle $k > n$

(2) $\binom{n}{k} = 0$ für alle $k < 0$

(3) $\binom{n}{1} = n$, da es n 1-elementige Teilmengen einer Menge mit n Elementen gibt

(4) $\binom{n}{0} = 1 = \binom{n}{n}$, da es genau eine 0-elementige und eine n-elementige Teilmenge einer Menge mit n Elementen gibt

6.11 Satz. *Seien $n \in \mathbb{N}$ und $k \in \{ 0, \ldots, n \}$. Dann gilt:*

$$\binom{n}{k} = \binom{n}{n-k}$$

Beweis: Sei N eine beliebige Menge mit $|N| = n \in \mathbb{N}$. Wir zeigen, dass $\binom{n}{k} := |\mathcal{P}_k(N)| = |\mathcal{P}_{n-k}(N)| =: \binom{n}{n-k}$. Wir definieren dazu eine Abbildung $\pi : \mathcal{P}_k(N) \to \mathcal{P}_{n-k}(N)$ durch $\pi(X) := N \backslash X$ und zeigen, dass π eine Bijektion ist.

Totalität. Offensichtlich ist $N \backslash X \in \mathcal{P}_{n-k}(N)$ für alle $X \in \mathcal{P}_n(N)$. Damit ist π total.

Injektivität. Seien $X, X' \in \mathcal{P}_k(N)$ mit $X \neq X'$. Da $X \neq X'$, gibt es ein $x \in X$ mit $x \notin X'$. Dann ist aber $x \in N \backslash X' = \pi(X')$ und $x \notin N \backslash X = \pi(X)$ und somit gilt $\pi(X) \neq \pi(X')$. Damit ist π injektiv.

Surjektivität. Sei $M \in \mathcal{P}_{n-k}(N)$. Wähle $X \in \mathcal{P}_k(N)$ so, dass $M = N \backslash X$. Dann ist $\pi(X) = N \backslash X$. Also ist π surjektiv.

Damit gilt insgesamt $|\mathcal{P}_k(N)| = |\mathcal{P}_{n-k}(N)|$. □

6.4.2. Rekursionsformel für Binomialkoeffizienten

Wir werden nun einige Methoden kennen lernen um die Werte von $\binom{n}{k}$ zu berechnen bzw. abzuschätzen. Als erstes beweisen wir eine Rekursionsformel.

6.12 Satz. *Seien $n, k \in \mathbb{N}_+$. Dann ist:*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Beweis: Die Aussage ist klar für $k > n$. Im folgenden sei also $k \leqslant n$.

Fall 1: $n = 1$. Dann ist $n - 1 = 0$ und k entweder 0 oder 1 und somit:

$$\binom{1}{0} = 1 = 0 + 1 = \binom{0}{-1} + \binom{0}{0}$$

$$\binom{1}{1} = 1 = 1 + 0 = \binom{0}{0} + \binom{0}{1}$$

Fall 2: $n > 1$. Sei N eine Menge mit $|N| = n \in \mathbb{N}$. Zu zeigen ist, dass $|\mathcal{P}_k(N)| = |\mathcal{P}_{k-1}(N')| + |\mathcal{P}_k(N')|$.

Sei $a \in N$ und $N' := N \backslash \{ a \}$. Wir teilen $\mathcal{P}_k(N)$ in zwei disjunkte Mengen P_1 und P_2 auf:

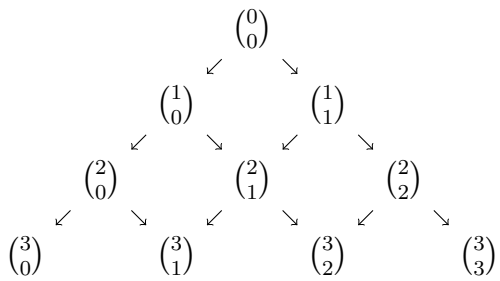
$$P_1 := \{ X : X \in \mathcal{P}_k(N),\ a \in X \}$$
$$P_2 := \{ X : X \in \mathcal{P}_k(N),\ a \notin X \} = \mathcal{P}_k(N) \backslash P_1$$

Nun gilt: $X \in P_1$ genau dann, wenn es ein $X' \in \mathcal{P}_{k-1}(N')$ existiert mit $X = \{ a \} \cup X'$, also ist $|P_1| = |\mathcal{P}_{k-1}(N')| = \binom{n-1}{k-1}$. Es gilt $X \in P_2$ genau dann, wenn $X \in \mathcal{P}_k(N')$ also $|P_2| = |\mathcal{P}_k(N')| = \binom{n-1}{k}$. Nach Lemma 6.2 Teil (1) ist dann

$$\binom{n}{k} = |\mathcal{P}_k(N)| = |P_1 \cup P_2| \overset{\text{Lemma 6.2}}{=} |P_1| + |P_2| = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

□

Der Satz liefert das Pascal'sche Dreieck. Hier ist jeder Koeffizient so geordnet, dass er die Summe beiden über ihn liegende Koeffizienten ist:



Das Dreieck liefert eine rekursive Methode $\binom{n}{k}$ auszurechnen. Eine konkrete Methode gibt uns der nächste Satz.

6.13 Satz. *Seien $n \in \mathbb{N}$ und $k \in \{ 0, \ldots, n \}$. Es gilt:*

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

Beweis: Wir beweisen die Aussage per Induktion über n.

Induktionsverankerung $n = 0$. Dann hat unsere Menge 0 Elemente und somit gibt es keine Elemente zum Auswählen, d.h. $k = 0$. Dann gilt:

$$\binom{n}{k} = \binom{0}{0} = 1 = \frac{0!}{0!\,0!} = \frac{n!}{k!(n-k)!}$$

Induktionsvoraussetzung Sei $n \in \mathbb{N}$ beliebig. Gelte $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

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

Induktionsschluss Wir zeigen die Induktionsbehauptung. Dabei unterscheiden wir zwei Fälle:

Fall 1: $k = 0$. Dann ist $\binom{n+1}{0} = 1 = \frac{(n+1)!}{0!(n+1)!}$

Fall 2: $k = n + 1$. Dann ist $\binom{n+1}{n+1} = 1 = \frac{(n+1)!}{(n+1)!0!} = \frac{(n+1)!}{(n+1)!(n+1-(n+1))!}$

Fall 3: $1 \leqslant k \leqslant n$. Dann ist:

$$\begin{aligned}
\binom{n+1}{k} &\overset{6.12}{=} \binom{n+1-1}{k-1} + \binom{n+1-1}{k} \\
&\overset{\text{IV}}{=} \frac{n!}{(k-1)!(n-(k-1))!} + \frac{n!}{k!(n-k)!} \\
&= \frac{n!}{(k-1)!(n-k+1)!} \cdot \frac{k}{k} + \frac{n!}{k!(n-k)!} \cdot \frac{n-k+1}{n-k+1} \\
&= \frac{k \cdot n!}{k!(n-k+1)!} + \frac{(n-k+1)n!}{k!(n-k+1)!} \\
&= \frac{n!(k+n-k+1)}{k!(n-k+1)!} \\
&= \frac{(n+1)!}{k!((n+1)-k)!}.
\end{aligned}$$

□

6.14 Satz (Binomialsatz)**.** *Seien $x, y \in \mathbb{R}$ und $n \in \mathbb{N}$. Dann gilt:*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Beweis: Wir beweisen die Aussage per Induktion über n.

Induktionsanfang $n = 0$. Dann ist $(x+y)^0 = 1 = \sum_{k=0}^{0} \binom{n}{k} x^k y^{0-k}$.

Wir zeigen auch $n = 2$:

$$\begin{aligned}(x+y)^2 &= (x^2 + 2xy + y^2) \\ &= \binom{2}{0} x^0 y^{2-0} + \binom{2}{1} x^1 y^{2-1} + \binom{2}{2} x^2 y^{2-2} \\ &= \sum_{k=1}^{2} \binom{n}{k} x^k y^{n-k}\end{aligned}$$

Induktionsvoraussetzung Sei $n \in \mathbb{N}$ und für alle $x, y \in \mathbb{R}$ gelte

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Induktionsbehauptung Für alle $x, y \in \mathbb{R}$ gilt:

$$(x+y)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k}$$

Induktionsschritt Seien $x, y \in \mathbb{R}$:

$$\begin{aligned}(x+y)^{n+1} &= (x+y)^n (x+y) \\ &\overset{\text{IV}}{=} \left(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \right) (x+y) \\ &= x \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} + y \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k}\end{aligned}$$

Hier können wir den Index der ersten Summe verschieben und erhalten:

$$= \sum_{k=1}^{n+1} \binom{n}{k-1} x^k y^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k}$$

Für $k = n+1$ bei der ersten Summe erhalten wir $\binom{n}{(n+1)-1} x^{n+1} y^{n+1-(n+1)} = x^{n+1}$ und für $k = 0$ bei der zweiten Summe erhalten wir $\binom{n}{0} x^0 y^{n+1-0} = y^{n+1}$. Daher können wir diese beide Summanden aus den Summen herausnehmen und bekommen dann nach Anpassung der Indizies:

$$\begin{aligned}
&= x^{n+1} + y^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} x^k y^{n+1-k} + \sum_{k=1}^{n} \binom{n}{k} x^k y^{n+1-k} \\
&= x^{n+1} + y^{n+1} + \sum_{k=1}^{n} x^k y^{n+1-k} \left(\binom{n}{k-1} + \binom{n}{k} \right) \\
&\overset{6.12}{=} x^{n+1} + y^{n+1} + \sum_{k=1}^{n} x^k y^{n+1-k} \binom{n+1}{k}
\end{aligned}$$

Fügen wir x^{n+1} und y^{n+1} zurück in die Summe, erhalten wir:

$$= \sum_{k=0}^{n+1} x^k y^{n+1-k} \binom{n+1}{k}$$

□

6.5. Kombinationen und Variationen

In diesem Abschnitt interessieren wir uns für die Zahl der Möglichkeiten, aus einer gegebenen Menge von Objekten k Objekte auszuwählen. Dies spielt z.B. in der Wahrscheinlichkeitsrechnung, aber auch in der Analyse von Algorithmen eine wichtige Rolle. Zur Lösung bestimmter algorithmischer Probleme muss man z.B. an einem Punkt einfach alle Lösungsmöglichkeiten ausprobieren. Zur Analyse dieser Algorithmen benötigt man daher eine Abschätzung über die Zahl der Möglichkeiten. In diesem Abschnitt betrachten wir daher einige einfache aber häufig vorkommende Abschätzungen.

Seien $n, k \in \mathbb{N}$ und sei M eine Menge mit n Elementen. Um die Zahl der Möglichkeiten zu bestimmen, aus M k Elemente auszuwählen, müssen wir zunächst festlegen, ob die gewählten Elemente sofort wieder zurück gelegt werden, und somit mehrfach gezogen werden können, und ob die Reihenfolge in der die Elemente gezogen werden können eine Rolle spielt. Dies führt zu den folgenden vier grundlegenden Begriffen.

Kombinationen/Auswahl ohne Reihenfolge. Mit *Kombinationen* bezeichnen wir die Auswahl von Elementen aus einer Menge, in der die Reihenfolge der Wahl **keine** Rolle spielt.

(1) Die Zahl der *Kombinationen ohne Wiederholung*, also die Zahl der Möglichkeiten, aus einer Menge mit n Elementen k Elemente so auszuwählen, dass **kein** Element doppelt gewählt wird und die Reihenfolge, in der die Elemente gezogen werden **nicht** berücksichtigt wird, bezeichnen wir mit $\mathrm{K}_{\mathrm{oW}}(n,k)$.

(2) Die Zahl der *Kombinationen mit Wiederholung*, also die Zahl der Möglichkeiten, aus einer Menge mit n Elementen k Elemente so auszuwählen, dass Elemente mehrfach gewählt werden können aber die Reihenfolge, in der die Elemente gezogen werden **nicht** berücksichtigt wird, bezeichnen wir mit $\mathrm{K}_{\mathrm{mW}}(n,k)$.

Variationen/Auswahl mit Reihenfolge. Mit *Variationen* bezeichnen wir die Auswahl von Elementen aus einer Menge, in der die Reihenfolge der Wahl eine Rolle spielt.

(1) Die Zahl der *Variationen ohne Wiederholung*, also der Möglichkeiten, aus einer Menge mit n Elementen k Elemente so auszuwählen, dass **kein** Element doppelt gewählt wird aber die Reihenfolge, in der die Elemente gezogen werden, berücksichtigt wird, bezeichnen wir mit $\mathrm{V}_{\mathrm{oW}}(n,k)$.

(2) Die Zahl der *Kombinationen mit Wiederholung*, also die Zahl der Möglichkeiten, aus einer Menge mit n Elementen k Elemente so auszuwählen, dass Elemente mehrfach gewählt werden können und die Reihenfolge, in der die Elemente gezogen werden, berücksichtigt wird, bezeichnen wir mit $\mathrm{V}_{\mathrm{mW}}(n,k)$.

Der folgende Satz bestimmt die Zahl der Möglichkeiten von Kombinationen und Variationen.

6.15 Satz. *Seien $n,k \in \mathbb{N}$ und M eine n-elementige Menge. Dann gilt*

(1) $\mathrm{K}_{\mathrm{oW}}(n,k) := \binom{n}{k}$

(2) $\mathrm{K}_{\mathrm{mW}}(n,k) := \binom{n+k-1}{k}$

(3) $\mathrm{V}_{\mathrm{oW}}(n,k) := \binom{n}{k} \cdot k!$

(4) $\mathrm{V}_{\mathrm{mW}}(n,k) := n^k$

Beweis:

(1) Offensichtlich ist die Zahl der Möglichkeiten, aus n Elementen genau k auszuwählen, wobei die Reihenfolge keine Rolle spielt und kein Element zurückgelegt wird, genau die Zahl der k-elementigen Teilmengen einer n-elementigen Menge, also gerade $\binom{n}{k}$.

(2) Anders ist es, wenn Elemente mehrfach gezogen werden können. Da hier die Reihenfolge keine Rolle spielt, können wir die gezogenen Elemente so grupieren, dass die mehrfach gezogenen Elemente nebeneinander stehen. D.h. wenn wir beispielsweise aus der Menge $N := \{\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8\ \}$ die 5 Elemente $2, 4, 2, 6, 4$ gezogen haben, können wir diese in der Reihenfolge $2, 2, 4, 4, 6$ aufschreiben. Da wir jedes Mal andere Elemente ziehen, können wir jeden möglichen Zug kodieren, indem wir jedes Element aus N in einer Kette hinschreiben so dass neben jedes Element der Kette so viele Striche (|) stehen, wie wir das Element gezogen haben. In userem Beispiel hätten wir dann die Kette 12||34||56|78. Nach der 1 gibt es keine Striche, also wurde sie nicht gezogen, nach der 2 gibt es zwei Striche, also wurde sie 2 Mal gezogen, nach der 3 gibt es keine Striche, also wurde sie nicht gezogen, usw. Betrachten wir nun die Menge aller möglichen solchen Ketten, erhalten wir im Grunde die Menge aller möglichen Zügen. Nun müssen wir zählen wie viele Möglichkeiten gibt es solche Ketten zu bilden.

Die Länge einer Kette ist $n+k$, wobei n die Anzahl der Elemente ist, aus denen wir ziehen (entspricht im Beispiel der 8 Zahlen) und k die Anzahl der gezogenen Elemente (entspricht im Beispiel der 5 Strichen). D.h. wir haben $n+k$ Positionen, an denen entweder Zahlen, oder ein Strich stehen kann. Da aber an erster Stelle jeder Kette immer die 1 steht und nie ein Strich, müssen wir nur die restlichen $n + k - 1$ Positionen betrachten, an denen wir die verschiedenen Zahlen und Strichen platzieren können. Also kann ein Strich an jeder dieser $n + k - 1$ Positionen stehen. Um die Anzahl der möglichen Ketten zu bestimmen, reicht es also aus zu bestimmen wie viele Möglichkeiten es gibt die k Striche auf $n + k - 1$ Positionen zu verteilen. Das ist genau $\binom{n+k-1}{k}$.

(3) Dies folgt sofort aus Teil 1. Es gibt $\binom{n}{k}$ k-elementige Teilmengen von M. Jede kann in $k!$ verschiedenen Reihenfolgen gezogen werden.

(4) Hier werden einfach k mal ein Element aus einer Menge von n Elementen gezogen. Für jeden Zug gibt es n Möglichkeiten, insgesamt also n^k.

□

7. Graphentheorie

7.1. Grundbegriffe

7.1 Definition. Ein *ungerichteter, einfacher Graph* G besteht aus einer Menge $V(G)$ von *Knoten* und einer Menge $E(G) \subseteq \mathcal{P}_2\big(V(G)\big)$ von *Kanten*. Die Zahl $|V(G)|$ heißt die *Ordnung* von G, die Zahl $|E(G)|$ heißt die *Größe*.

Wir werden ungerichtete, einfache Graphen einfach als Graphen bezeichnen. Den *leeren Graphen* mit Knotenmenge $\varnothing$ bezeichnen wir mit $\varnothing$.

Adjazenz und Inzidenz. Sei G ein Graph. Zwei Knoten $u, v \in V(G)$ heißen *adjazent*, wenn $\{u, v\} \in E(G)$. Ein Knoten $u \in V(G)$ und eine Kante $e \in E(G)$ sind *inzident*, wenn $u \in e$. Zwei Kanten $e, e' \in E(G)$ heißen *adjazent*, wenn es einen Knoten $u \in V(G)$ gibt, der zu beiden Kanten inzident ist. Die zu einer Kante inzidenten Knoten sind die *Endknoten* der Kante.

Zwei adjazente Knoten heißen auch *benachbart*, oder sie sind *Nachbarn*. Die *Nachbarschaft* eines Knoten $v \in V(G)$, geschrieben $N_G(v)$, ist die Menge

$$N_G(v) := \{u \in V(G) : u \text{ und } v \text{ sind adjazent}\}.$$

Zeichnen von Graphen. Wir werden Graphen überlicherweise "graphisch" darstellen, indem Knoten als Punkte $p \in \mathbb{R}^2$ und Kanten durch Linien $P \subseteq \mathbb{R}^2$ dargestellt werden, die die beiden Endpunkte verbinden, so dass keine dieser Linien einen Knoten schneidet außer den Endpunkten der Kante. Einfachheitshalber nennen wir die Punkte und Linienzüge ebenfalls Knoten und Kanten.

Besonders schön sind Zeichnungen, in denen sich keine zwei Kanten schneiden außer an ihren Endpunkten. Graphen, die auf diese Weise gemalt werden können, heißen *planare Graphen*.

Einige spezielle Graphklassen. Ein Graph G heißt *vollständig*, oder eine *Clique*, wenn $E(G) = \mathcal{P}_2\big(V(G)\big)$. Wir bezeichnen den vollständigen Graphen G mit Knotenmenge $\{1, \dots, n\}$ als K_n.

7.2 Definition. Ein Graph G heißt *bipartit*, wenn eine Partition von $V(G)$ in zwei disjunkte Mengen A, B existiert, so dass

$$E \subseteq \big\{\{u, v\} : u \in A \text{ und } v \in B\big\}.$$

Allgemeiner heißt ein Graph G *k-partit*, wenn sich $V(G)$ in k disjunkte Mengen $A_1, \ldots, A_k$ partitionieren läßt, so dass es keine Kante $e \in E(G)$ gibt, die beide Endpunkte in der selben Menge A_i hat.

Wir werden bipartite Graphen G oft als $G = (A \cup B, E)$ schreiben, wobei dann A, B die beiden Partitionen der Knotenmenge $V(G) = A \cup B$ sind und $E = E(G)$ die Kantenmenge ist.

Isomorphie zwischen Graphen.

7.3 Definition. Seien G, H Graphen. Ein *Isomorphismus* zwischen G und H ist eine Bijektion $\pi : V(G) \to V(H)$, so dass für alle Knoten $u, v \in V(G)$ gilt: $\{u, v\} \in E(G)$ genau dann, wenn $\{\pi(u), \pi(v)\} \in E(H)$. Zwei Graphen G, H heißen *isomorph*, wenn es einen Isomorphismus zwischen G und H gibt.

Isomorphe Graphen unterscheiden sich also ausschließlich in der Benennung der Knoten. Da wir uns für die Namen der Knoten nicht sonderlich interessieren, werden wir in Zukunft nicht mehr zwischen isomorphen Graphen unterscheiden. Insbesondere sind für jedes $n \in \mathbb{N}$ alle vollständigen Graphen der Ordnung n paarweise isomorph. Wir können daher sagen, dass K_n *die* Clique der Ordnung n ist.

7.2. Untergraphen und elementare Graphoperationen

7.4 Definition. Seien G, H Graphen.

(1) H ist ein *Untergraph* eines Graphs G, geschrieben $H \subseteq G$, wenn $V(H) \subseteq V(G)$ und $E(H) \subseteq E(G)$.

(2) H ist ein *induzierter Untergraph* von G, wenn $H \subseteq G$ und $E(H) = E(G) \cap \mathcal{P}_2(V(H))$.

(3) H ist ein *spannender Untergraph* von G, wenn $H \subseteq G$ und $V(H) = V(G)$.

Sei G ein Graph und $X \subseteq V(G)$. Der von X *in* G *induzierte Untergraph*, geschrieben $G[X]$, ist der induzierte Untergraph von G mit Knotenmenge $V(G[X]) = X$.

Seien G, H Graphen. Mit $G - H$, oder $G \setminus H$, bezeichnen wir den durch $V(G) \setminus V(H)$ in G induzierten Untergraphen. Für einen Knoten $v \in V(G)$

definieren wir $G - v$ als $G[V(G) \setminus \{v\}]$. Für eine Kante $e \in E(G)$ definieren wir $G - e$ als den Graphen mit der Knotenmenge $V(G)$ und Kantenmenge $E(G) - e$.

Mit $G \cup H$ bezeichnen wir die *Vereinigung* der Graphen G und H, d.h. den Graph $G \cup H$ mit Knotenmenge $V(G) \cup V(H)$ und Kantenmenge $E(G) \cup E(H)$. Wenn $V(H) \cap V(G) = \varnothing$ gilt, dann nennen wir $G \cup H$ die *disjunkte Vereinigung* von G und H.

Entsprechend definieren wir den Schnitt $G \cap H$ als den Graph mit Knotenmenge $V(G) \cap V(H)$ und Kantenmenge $E(G) \cap E(H)$.

7.3. Der Grad von Knoten

7.5 Definition. Sei G ein Graph und $v \in V(G)$.

(1) Der *Grad* (oder die Valenz) von v in G, geschrieben $d_G(v)$, ist die Zahl der zu v inzidenten Kanten.

(2) Der *Minimalgrad* von G, geschrieben $\delta(G)$, ist definiert als $\delta(G) := \min\{d_G(v) : v \in V(G)\}$.

(3) Der *Maximalgrad* von G, geschrieben $\Delta(G)$, ist definiert als $\Delta(G) := \max\{d_G(v) : v \in V(G)\}$.

(4) Der *Durchschnittsgrad* von G, geschrieben $d(G)$, ist definiert als $d(G) := \frac{1}{|V(G)|} \sum_{v \in V(G)} d_G(v)$.

Ein Knoten mit Grad 0 heißt *isoliert*. Wir werden oft den Index G in $d_G(v)$ und $N_G(v)$ weglassen, wenn G aus dem Zusammenhang klar ist.

7.6 Proposition. *Für jeden Graph G gilt*

$$|E(G)| = \frac{1}{2} d(G) \cdot |V(G)|.$$

Beweis: Es gilt $d(G) \cdot |V(G)| = \sum_{v \in V(G)} d_G(v)$. In dieser Summe wird aber jede Kante doppelt gezählt, nämlich einmal für jeden der beiden Endpunkte. Also gilt $|E(G)| = \frac{1}{2} \sum_{v \in V(G)} d_G(v) = \frac{1}{2} d(G) \cdot |V(G)|$. □

7.7 Lemma. *Jeder Graph G mit mindestens einer Kante enthält einen Untergraph H mit $\delta(H) > \frac{1}{2} d(H) \geqslant \frac{1}{2} d(G)$.*

Beweis: Wir konstruieren H aus G indem wir nacheinander Knoten mit kleinem Grad eliminieren. Sei $\varepsilon = \frac{1}{2}d(G)$ und sei $v \in V(G)$. Wenn $d_G(v) \leqslant \varepsilon$, dann gilt $d(G-v) \geqslant d(G)$. Sei $d = d(G)$. Dann gilt $d(G) \cdot |V(G)| = \sum_{u \in V(G)} d_G(v) \leqslant \sum_{u \in V(G-v)} d_{G-v}(u) + 2d_G(v)$, da wir ja jede zu v inzidente Kante zweimal aus der Summe abziehen müssen.

Weiterhin gilt $\sum_{u \in V(G-v)} d_{G-v}(u) + 2d_G(v) \leqslant \sum_{u \in V(G-v)} d_{G-v}(u) + d(G)$, da $d_G(v) \leqslant \varepsilon = 2d(G)$.

Also gilt $d(G) \cdot |V(G)| \leqslant \sum_{u \in V(G-v)} d_{G-v}(u) + d(G)$ und somit $d(G) \leqslant \frac{\sum_{u \in V(G-v)} d_{G-v}(u)}{|V(G)|-1} = d(G-v)$.

Wir können nun also eine Kette $G = G_0 \supseteq G_1 \ldots$ von induzierten Untergraphen von G wie folgt bilden. Wir setzen $G_0 = G$. Angenommen, G_i sei schon definiert. Wenn G_i einen Knoten v vom Grad $d_{G_i}(v) \leqslant \frac{1}{2}d(G_i)$ enthält, definieren wir $G_{i+1} := G_i - v$. Anderenfalls hört die Konstruktion hier auf und wir setzen $H := G_i$. Wie oben gezeigt gilt $d(G_i) \leqslant d(G_{i+1})$ für alle i so dass $i+1$ definiert ist. Da $d(G) > 0$ (denn G enthält eine Kante nach Voraussetzung) enthält also auch jeder Graph G_i eine Kante und somit auch einen Knoten, insbesondere also auch H. Da aber kein Knoten aus H mehr gelöscht werden kann, folgt also $\delta(H) > \frac{1}{2}d(H) \geqslant \frac{1}{2}d(G)$. □

7.4. Ramsey Theorie

Zur Erinnerung: Sei G ein Graph. $H \subseteq G$ wenn $V(G) \subseteq V(G)$ und $E(H) \subseteq E(G) \cap (V(H) \times V(H))$. H ist ein induzierter Untergraph von G wenn $V(G) \subseteq V(G)$ und $E(H) = E(G) \cap (V(H) \times V(H))$

K_n ist eine Clique mit n Knoten.

7.8 Definition (Stabile Menge)**.** Sei G ein Graph. Eine Menge $X \subseteq V(G)$ heißt *unabhängig* oder *stabil*, wenn für alle $u, v \in X$ gilt $\{u, v\} \notin E(G)$.

7.4.1. Originalsatz von Ramsey

7.9 Satz (Ramsey 1930)**.** *Für alle $r \in \mathbb{N}$ existiert ein $n \in \mathbb{N}$ so, dass jeder Graph der Ordnung $|G| \geqslant n$ eine stabile Menge der Größe r enthält oder es gilt $K_r \subseteq G$.*

Beweis: Setze $n \geqslant 2^{2r-1}$. Sei nun G mit $|G| \geqslant n = 2^{2r-1}$. Konstruieren wir für $i = 0, \ldots, 2r-1$ die Sequenz V_i, C_i, S_i mit:

(1) $V_i \subseteq V(G)$, $|V_i| = 2^{2r-(i+1)}$

(2) $C_i, S_i \subseteq V(G)$, $|C_i| + |S_i| = i$

(3) jeder $v \in C_i$ hat eine Kante zu allen $u \in C_i \cup V_i$, $u \neq v$

(4) **kein** Knoten $v \in S_i$ hat eine Kante zu einem Knoten aus $S_i \cup V_i$

Wir beweisen per Induktion, dass solche Mengen existieren.

Induktionsverankerung Setze $V_0 \subseteq V(G)$ beliebig mit $|V_0| = 2^{r-1}$, $C_0, S_0 = \varnothing$. Offensichtlich erfüllen V_0, C_0 und S_0 die Bedingungen 1-4 oben.

Induktionsvoraussetzung Seien V_i, C_i, S_i schon so definiert, dass die Bedingungen 1-4 erfüllt sind.

Induktionsschritt Konstruieren wir $V_{i+1}, C_{i+1}, S_{i+1}$. Wähle dann $v \in V_i$ beliebig.

Sei $C := (N_G(V) \cap V_i) \subseteq V_i \backslash \{ v \}$ die Menge der Nachbarn von v in V_i.

Sei $S := V_i \backslash C$. Also hat v keine Kanten zu allen $u \in S$.

Es gilt $|V_i \backslash \{ v \}| = 2^{2r-i} - 1$, ist also ungerade.

Weiterhin gilt $C \cup S = V_i \backslash \{ v \}$ und da per Konstruktion $C \cap S = \varnothing$, gilt $|V_i \backslash \{ v \}| = |C \cup S| \overset{\text{Lemma6.2}}{=} |C| + |S|$ $(*)$.

Wir wollen nun zeigen, dass entweder C oder S mindestens die Hälfte der Knoten aus V_i enthält, d.h, dass entweder $|C| \geqslant \frac{2^{2r-i}}{2}$ oder $|S| \geqslant \frac{2^{2r-i}}{2}$. Dazu führen wir einen kurzen Widerspruchsbeweis:

Angenommen, beide $|C|, |S| \leqslant \frac{2^{2r-i}}{2} - 1$. Somit wäre

$$\begin{aligned} |C| + |S| &\leqslant \frac{2^{2r-i}}{2} - 1 + \frac{2^{2r-i}}{2} - 1 \\ &= 2^{2r-i} - 2 \\ &< |V_i \backslash \{ v \}| \text{ was aber ein Widerspruch zu } (*) \text{ wäre} \end{aligned}$$

Daher gilt entweder $|C| \geqslant \frac{2^{2r-i}}{2}$ oder $|S| \geqslant \frac{2^{2r-i}}{2}$.

- Falls $|C| \geqslant \frac{2^{2r-i}}{2}$, dann setze $V_{i+1} := C$, $C_{i+1} := C_i \cup \{ v \}$ und $S_{i+1} := S_i$
- Falls $|S| \geqslant \frac{2^{2r-i}}{2}$, dann setze $V_{i+1} := S$, $C_{i+1} := C_i$ und $S_{i+1} := S \cup \{ v \}$.

Nach Konstruktion und I.V. gelten in beiden Fällen die Bedingungen 1-4.

Seien nun $V_{2r-1}, C_{2r-1}, S_{2r-1}$ definiert. Dann ist $|C_{2r-1}|+|S_{2r-1}| = 2r-1$ also entweder $|C_{2r-1}| \geqslant r$ oder $|S_{2r-1}| \geqslant r$. Im ersten Fall induziert C_{2r-1} eine Clique in G mit r Knoten und im zweiten Fall ist S_{2r-1} eine stabile Menge in G mit r Knoten.

□

7.10 Beispiel. Ein ausführliches Beispiel findet man auf der ISIS-Webseite.

7.4.2. Allgemeine Variante von Ramseys Satz

7.11 Definition (Eine Färbung von $\mathcal{P}_M(P)$ mit c Farben)**.** Sei M eine Menege und $k, c \in \mathbb{N}_+$. Dann ist die Abbildung $\gamma : \mathcal{P}_M(k) \to \{ 1, \ldots c \}$ eine *Färbung* von $\mathcal{P}_M(k)$ mit c Farben.

Eine Menge $Y \subseteq M$ heißt monochromatisch bzgl γ, wenn es ein $i \in \{ 1, \ldots, c \}$ gibt so, dass für alle $X \in \mathcal{P}_Y(k)$ gilt $\gamma(X) = i$ (d.h. alle k-elementigen Teilmengen von Y haben dieselbe Farbe).

7.12 Satz. *Für alle $k, c, n \in \mathbb{N}_+$ existiert ein $N \geqslant 1$, so dass für jede Menge M mit $|M| \geqslant N$ gilt:*

Wenn $\gamma : \mathcal{P}_M(k) \to \{ 1, \ldots, c \}$ eine Färbung ist, dann existiert $Y \subseteq M$ mit $|Y| = n$, so dass Y monochromatisch ist.

Anmerkung: Sei $r \geqslant 1$. Setze $c = 2, n = r, k = 2$. Sei G ein Graph mit $|G| \geqslant N$ aus dem Satz. Sei $\gamma : \mathcal{P}_{V(G)}(2) \to \{ 1, 2 \}$ mit

$$\gamma(\{ u, v \}) = \begin{cases} 1, & \text{falls } \{ u, v \} \in E(G) \\ 2, & \text{sonst} \end{cases}$$

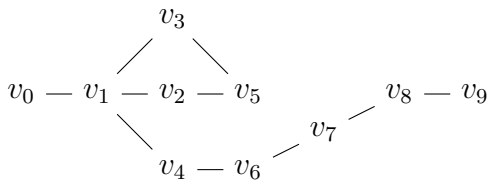
Z.B. stehe die 1 für die Farbe blau und die zwei für die Farbe rot.

Also existiert $Y \subseteq V(G)$ mit $|Y| = n = r$ und $i \in \{ 1, 2 \}$ so dass $\gamma(\{ u, v \}) = i$ für alle $u, v \in Y$. Wenn $i = 1$ (blau), dann induziert Y eine Clique. Wenn $i = 2$ (rot), dann ist Y eine stabile Menge.

7.5. Pfade und Zyklen

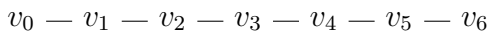
7.13 Definition (Weg)**.** Ein *Weg* W ist ein nicht-leerer Graph P der Form $V(W) := \{ v_1, \ldots v_n \}$ und $E(W) := \{ \{ v_i, v_{i+1} \} : 1 \leqslant i < n \}$. Die *Länge* von W ist die Anzahl der Kanten in W.

Wir sagen, dass der Weg W die Knoten v_1 und v_n *verbindet* und bezeichnen v_1 und v_n als die Endpunkte von W.

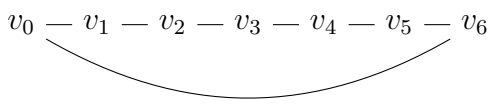


7.14 Definition (Pfad)**.** Ein *Pfad* P ist ein Weg mit Knotenmenge $\{ v_0, \ldots, v_k \}$, so dass $v_i \neq v_j$ für alle $i \neq j$, $1 \leqslant i, j \leqslant k$. Wir schreiben oft nur $P := (v_0, \ldots, v_k)$

Das heißt in Pfade darf jeder Knoten nur ein Mal vorkommen.

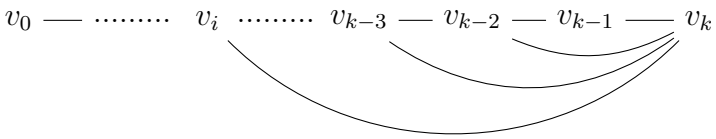


7.15 Definition (Zyklus)**.** Ein *Zyklus* oder *Kreis* ist ein nicht-leerer Graph Z, der aus einem Pfad $P := (v_1, \ldots, v_n)$ mit mindestens 3 Knoten und der Kante $e := \{ v_n, v_1 \}$ besteht, d.h. $Z := P + e$



7.16 Proposition. *Jeder Graph G enthält einen Pfad der Länge $\delta(G)$ und Kreis der Länge $\geqslant \delta(G) + 1$ (vorausgesetzt $\delta(G) \geqslant 1$).*

Beweis: Sei G ein Graph mit Minimalgrad $\delta(G) = n$ und $P := (v_0, \ldots, v_k)$ ein Pfad in G maximaler Länge. Da P maximale Länge hat, müssen alle Nachbarn von v_k in P liegen. Da aber $\delta(G) = n$, muss also $k \geqslant d(v_k) \geqslant \delta(G) = n$ und somit hat P mindestens die Länge $n = \delta(G)$. Betrachten wir nun das minimale $i < k$, so dass $\{ v_i, v_k \} \in E(G)$, d.h. v_k und v_j sind **nicht** benachbart für alle $j < i$. Sei $P' := (v_i, \ldots v_k)$ der Pfad von v_i zu v_k. Dieser Pfad hat mindestens Länge $\delta(G)$ (da v_k mindestens $\delta(G)$ Nachbarn hat). Dann ist $Z := P + \{ v_i, v_k \}$ ein Zyklus der Länge $\delta(G) + 1$



□

7.6. Zusammenhang in Graphen

7.17 Definition. Ein Graph G ist *zusammenhängend*, wenn es zwischen je zwei Knoten $u, v \in V(G)$ einen Pfad in G gibt.

7.18 Beispiel. In Abbildung 7.4 ist G ein zusammenhängender Graph.

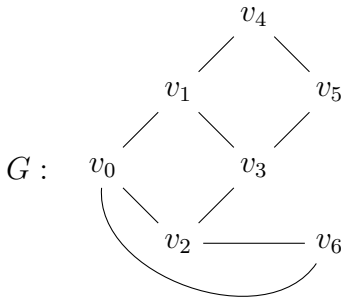


Abbildung 7.1.: Ein zusammenhängender Graph

7.19 Definition. Sei G ein Graph. Die zusammenhängenden Untergraphen $C_1, C_2, \ldots, C_k$ von G **maximaler** Ordnung heißen *Zusammenhangskomponenten.*

7.20 Beispiel. In Abbildung 7.2 ist G ein nicht zusammenhängender Graph mit genau drei Zusammenhangskomponenten.

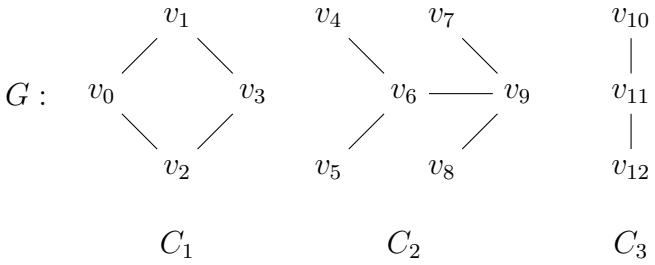


Abbildung 7.2.: Zusammenhangskomponenten eines Graphen

7.21 Definition. Sei G ein Graph und $u, v \in V(G)$.

(1) Die *Distanz* zwischen u, v in G ist: $\operatorname{dist}_G(u,v) := \infty$, falls es kein Pfad von u zu v in G gibt und ansonsten

$$\operatorname{dist}_G(u,v) := \min\{\, k : \text{ es. ex. einen Pfad von } u \text{ zu } v \text{ der Länge } k \,\}.$$

Wenn der Graph klar ist, schreiben wir auch kurz $\operatorname{dist}(u,v)$ oder auch $d(u,v)$.

(2) Der *Durchmesser* $\operatorname{diam}(G)$ (oder auch diam_G) von G ist definiert als:

$$\operatorname{diam}(G) := \max_{u,v \in V(G)} \operatorname{dist}_G(u,v) = \max_{u \in V(G)} \max_{v \in V(G)} \operatorname{dist}_G(u,v).$$

(3) Der *Radius* $\operatorname{rad}(G)$ (oder auch rad_G) von G ist definiert als:

$$\operatorname{rad}(G) := \min_{u \in V(G)} \max_{v \in V(G)} \operatorname{dist}_G(u,v).$$

(4) Ein *Zentrum* von G ist ein Knoten $c \in V(G)$ mit $\max_{v \in V(G)} \operatorname{dist}_G(c,v) = \operatorname{rad}(G)$. Ein solcher Knoten nennen wir auch zentral.

Wenn G nicht zusammenhängend ist, dann ist $\operatorname{diam}(G) = \operatorname{rad}(G) = \infty$. (Warum?)

Es gilt $\operatorname{rad}(G) \leqslant \operatorname{diam}(G) \leqslant 2\operatorname{rad}(G)$. Der Beweis dazu wird dem Leser als Übung überlassen (siehe Tutorium 11).

7.22 Beispiel. In Abbildung 7.3 ist $\operatorname{diam}(G) = 4$, $\operatorname{rad}(G) = 2$ und v_3 ein Zentrum.

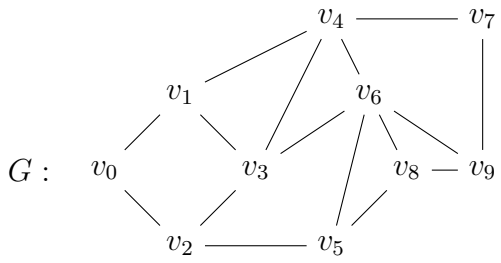


Abbildung 7.3.: Durchmesser, Radius und zentrale Knoten

7.7. Bäume

7.23 Definition. Sei G ein Graph. G ist *azyklisch*, wenn G keinen Kreis (Zyklus) $C \subseteq G$ enthält.

7.24 Definition. Ein *Baum* T ist ein zusammenhängender azyklischer Graph. Ein Knoten von T mit Grad 1 heißt *Blatt*.
Azyklische Graphen (möglicherweise also nicht zusammenhängend) heißen Wälder.

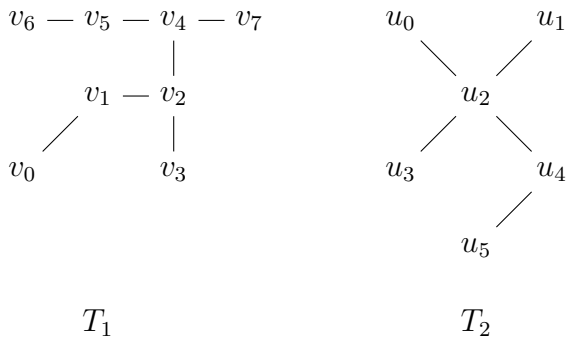


Abbildung 7.4.: T_1 und T_2 sind Bäume

7.25 Beobachtung. (1) Jeder Baum T hat mindestens ein Blatt.

(2) Sei T ein Baum und $b \in V(T)$ ein Blatt. Dann ist $T - b$ auch ein Baum. Ist $v \notin V(T)$, dann ist für alle $u \in V(T)$ auch $T' := (V \cup \{ v \}, E \cup \{ u, v \})$ ein Baum.

Zum Beweis von Teil (1) betrachte man einen längsten Pfad in T. Deren Endknoten ist ein Blatt. Der Beweis von Teil (2) ist dem Leser als Übung überlassen (siehe Großübung 11).

7.26 Lemma. *Sei T ein Baum.*

(1) *Zwischen je zwei Knoten $u, v \in V(T)$ gibt es genau einen Pfad in T.*

(2) *T ist minimal zusammenhängend, d.h. T ist zusammenhängend, aber für jede $e \in E(T)$ ist $T - e$ nicht zusammenhängend.*

(3) *T ist maximal azyklisch, d.h. T ist azyklisch, aber für alle $u, v \in V(T)$, $u \neq v$ ist $T + \{u, v\}$ nicht azyklisch.*

7.27 Lemma. *Ein zusammenhängender Graph mit $n \geqslant 1$ Knoten ist ein Baum gdw. $|E(G)| = |V(G)| - 1$.*

Beweis: Wir beweisen die Aussage per Induktion über n □

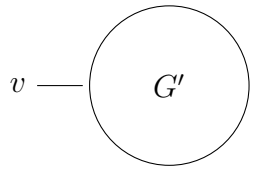
Induktionsverankerung $n = 1$. Sei G ein zusammenhängender Graph mit 1 Knoten. G hat also 0 Kanten. Daher ist G auch azyklisch und somit ein Baum.

Induktionsvoraussetzung Sei $n \in \mathbb{N}_+$ und gelte, dass jeder Graph mit n Knoten ein Baum ist, gdw. $|E(G)| = |V(G)| - 1$.

Induktionsbehauptung Die Aussage gilt für $n + 1$.

Induktionsschluss Nun zeigen wir die Induktionsbehauptung. Sei G ein zusammenhängender Graph mit $n + 1$ Knoten. Wir betrachten zwei Fälle.

- Fall 1: Der Minimalgrad $\delta(G) \geqslant 2$. Dann hat G insbesondere kein Knoten vom Grad 1 und ist kein Baum, da nach Beobachtung 7.25 ein Baum mindestens ein Knoten vom Grad 1 haben muss. Außerdem gilt, dass $|E(G)| \geqslant |V(G)|$ (Da jeder Knoten mindestens zwei Nachbarn hat). Somit gilt in deisem Fall die zu zeigende Aussage.
- Fall 2: Es gibt mindestens einen Knoten $v \in V(G)$ vom Grad 1. Sei $G' := G - v$.



Es gilt, dass $|E(G')| = |E(G)| - 1$ und $|V(G')| = |V(G)| - 1$ $(*)$. Also ist G' nach IV genau dann ein Baum, wenn $|E(G')| = |V(G')| - 1$. Fügen wir nun v wieder hinzu, erhalten wir G. Für die Hinrichtung sei G ein Baum. Dann ist G' auch ein Baum. Folglich ist $|E(G)| \overset{(*)}{=} |E(G')| + 1 \overset{\text{IV}}{=} |V(G')| - 1 + 1 = |V(G')| \overset{(*)}{=} |V(G)| - 1$.

Für die Rückrichtung sei nun $|E(G)| = |V(G)| - 1$ $(**)$. Dann haben wir $|E(G')| \overset{(*)}{=} |E(G)| - 1 \overset{(**)}{=} |V(G)| - 1 - 1 \overset{(*)}{=} |V(G')| - 1$. Daher gilt nach IV, dass G' ein Baum ist. Da aber v den Grad 1 hat, ist nach Beobachtung 7.25 Teil (2) auch G ein Baum.

7.7.1. Spannbäume

7.28 Definition (Wurzelbaum)**.** Seien T ein Baum und $w \in V(T)$. Wir nennen das Paar (T, w) einen Baum mit Wurzel w, oder *Wurzelbaum*.

7.29 Notation. Sei (T, w) ein Wurzelbaum mit Wurzel w. Seien $v, t \in V(T)$.

(1) t ist ein *Nachfolger* von s und s ist ein *Vorgänger* von t, wenn $t \in N_T(s)$ und der (eindeutig bestimmte) Pfad in T von w nach t den Knoten s enthält.

(2) Wir schreiben T_t für die Komponente von $T - v$, die t enthält.

(3) Ein Wurzelbaum, in dem jeder Knoten höchstens 2 Nachfolger hat, heißt *Binärbaum*.

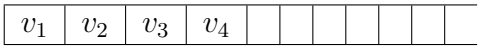
Allgemeine Bäume T, in denen jeder Knoten höchstens den Grad 3 hat, heißen *subkubisch*.

7.30 Definition. Sei G ein Graph. Ein *Spannbaum* von G ist ein Baum $T \subseteq G$ mit $V(T) = V(G)$, d.h. T ist spannender Untergraph.

7.31 Beobachtung. Spannbäume existieren nur für zusammenhängende Graphen. Für allgemeine Graphen gibt es *Spannwälder*.

Wir werden zwei Arten kennenlernen Spannbäume zu konstruieren.

Breitensuche Sei G ein Graph $v \in V(G)$ bezeichne den *Startknoten*. Wir verwenden die Datenstruktur *Queue* (Schlange):



Eine Queue ist eine Folge $Q = (v_1, \ldots, v_k)$ von Knoten. Auf einer Queue können wir die folgenden Operationen anwenden:

(1) Lesen des ersten Elements v_1: Q bleibt unverändert.

(2) Löschen des ersten Elements:

$$Q = (v_1, v_2, \ldots, v_k) \to Q' = (v_2, \ldots, v_k)$$

(3) Schreiben von $\mathbf{v}$ auf Q:

$$Q = (v_1, v_2, \ldots, v_k) \to Q' = (v_1, v_2, \ldots, v_k, \mathbf{v})$$

Mit Hilfe der Queue können wir nun den Breitensuchalgorithmus zum Erstellen eines Spannbaums angeben. Seien also G ein zusammenhängender Graph und $v \in V(G)$ der Startknoten. Wir erstellen den Spannbaumm T wie folgt:

Initialisierung: $Q := (v)$, $T := (\{ v \}, \varnothing)$. Invariante: alle Knoten in Q kommen auch in T vor.

Solange Q nicht leer ist , tue folgendes:

- Lese das erste Element u aus Q.
- Lösche u aus Q.
- Sei U die Menge der Nachbarn von u in G, die nicht in T vorkommen, d.h. $U = N_G(u) \backslash V(T)$.
- Falls $U \neq \varnothing$,
  - füge alle $x \in U$ zu Q hinzu.
  - füge alle $x \in U$ als Nachfolgern von u zu T hinzu.

Man nennt T einen *BFS-Baum* oder *Breitensuchbaum* von G.

7.32 Beobachtung. T ist nicht eindeutig und hängt von der Reihenfolge ab, in der Nachbarn eingefügt werden.

7.33 Satz. *Sei G ein zusammenhängender Graph mit $v \in V(G)$. Dann liefert die Breitensuche mit Startknoten v einen Spannbaum T von G mit Wurzel v zurück.*

Weiterhin gilt für alle $u \in V(G)$:

$$\mathrm{dist}_T(v, u) = \mathrm{dist}_G(v, u)$$

d.h. T enthält die kürzesten Pfade von v zu jedem anderen Knoten.

Den Beweis wird dem Leser als Übung überlassen.

Tiefensuche Die Tiefensuche funktioniert ähnlich wie die Breitensuche, wir verwenden aber einen *Stack* anstatt einer Queue.

Ein Stack $S = (v_1, \ldots, v_k)$ ist eine Folge von Knoten, auf der folgende Operationen angewandt werden können:

(1) Lesen des obersten Elements v_1: S bleibt unverändert.

(2) Löschen des obersten Elements:

$$S = (v_1, v_2, \ldots, v_k) \to S' = (v_2, \ldots, v_k)$$

(3) Ablegen von $\mathbf{v}$ auf S:

$$S = (v_1, v_2, \ldots, v_k) \to S' = (\mathbf{v}, v_1, \ldots, v_k)$$

Sei nun G ein zusammenhängender Graph mit $v \in V(G)$. Wir erstellen den Spannbaumm T wie folgt:

Initialisierung: $S := (v)$, $T := (\{ v \}, \varnothing)$. Invariante: alle Knoten in Q kommen auch in T vor.

Solange S nicht leer ist , tue folgendes:

- Lese das oberste Element u aus Q.
- Sei $U := N_G(u) \backslash V(T)$.
- Falls $U \neq \varnothing$,
  - wähle ein x aus
  - Lege x auf den Stack S ab.
  - füge $x \in U$ als Nachfolger von u zu T hinzu.
- sonst (d.h. $U = \varnothing$) entferne u vom Stack S.

7.34 Satz. *Sei G ein zusammenhängender Graph mit $v \in V(G)$. Dann liefert die Tiefensuche mit Startknoten v einen Spannbaum T von G mit Wurzel v.*

7.35 Beobachtung. Die Tiefensuche erzeugt einen Spannbaum mit Wurzel v, der *nicht* mehr die kürzesten Wege von v zu allen anderen Knoten enthält.

Der Tiefensuchbaum kann auch benutzt werden, um eine Ordnung auf $V(G)$ zu definieren.

Travesieren von T Sei T ein durch Tiefensuche erzeugter Spannbaum. Wir laufen T mit einer Tiefensuche (oder auch Breitensuche) ab.

Dies liefert uns eine Ordnung auf $V(G)$, nämlich die Reihenfolge, in der die Knoten durchsucht werden. Hierbei kam der Vorgänger vor den Nachfolgern vor. Man nennt das *pre-order*. Daneben gibt es auch *post-order*, in der der Vorgänger erst *nach* den Nachfolgern gezählt wird. Bei Binärbäume macht die sogennante *in-order* auch Sinn: dort kommt der linke Nachfolger zuerst vor, dann der Vorgänger und danach der rechte Nachfolger.

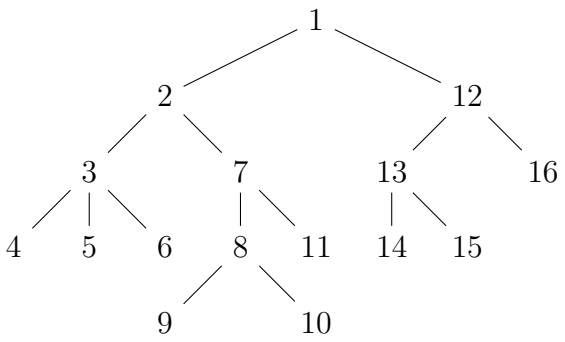


Abbildung 7.5.: Travesierungsreihenfolge eines Spannbaums mittels Tiefensuche. Die Knotennummer entsprechen der Ablaufsreihenfolge.

7.8. Zusammenhang in Graphen

7.36 Definition (Separator, Trenner)**.** Seien G ein Graph, $A, B \subseteq V(G)$, $S \subseteq V(G) \cup E(G)$.

(1) S trennt A von B, wenn jeder Pfad P mit einem Endpunkt in A und dem anderen Endpunkt in B mindestens einen Knoten aus S enthält.

(2) Einen $A-B$-*Trenner*, oder $A-B$-*Separator* ist eine Menge $S \subseteq V(G)$, die A von B trennt.

(3) Ein Knoten $v \in V(G)$, der zwei Knoten $x, y \in V(G)$ trennt, die in G zusammenhängen, nennt man *Schnittknoten* oder auch *cut-vertex*.

(4) Eine Kante $e \in E(G)$, die zwei Knoten $x, y \in V(G)$ trennt, die in G zusammenhängen, nennt man *Brücke*.

7.37 Beispiel. In Abbildung 7.6 ist v_4 ein Schnittknoten, der die Knoten v_1 und v_{11} trennt. Gibt es auch andere Schnittknoten, die diese beiden Knoten trennen?

7.38 Definition. Sei G ein Graph und $k \in \mathbb{N}$. G ist *k-zusammenhängend*, wenn $|V(G)| > k$ und $G - X$ ist zusammenhängend für alle $X \subseteq V(G)$ mit $|X| < k$.

Der Tiefensuchbaum kann benutzt werden, um Schnittknoten zu finden.

7.39 Lemma. *Sei G ein Graph. Sei T ein Tiefensuchbaum von G mit Wurzel $w \in V(G)$.*

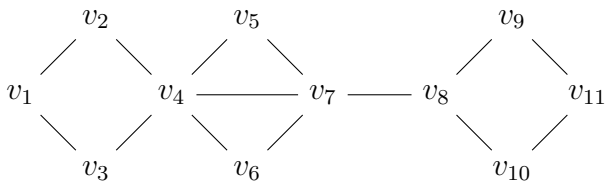
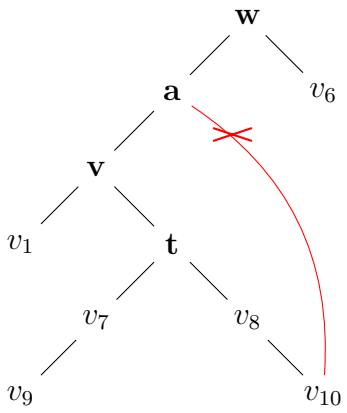


Abbildung 7.6.: Der Knoten v_4 ist ein Schnittknoten von v_1 und v_{11}. Die Kante $\{ v_7, v_8 \}$ ist eine Brücke zwischen diese Knoten.

(1) *w ist ein Schnittknoten in G gdw. w mindestens zwei Nachfolger hat.*

(2) *Ein anderer Knoten $v \in V(T)$ mit $v \neq w$ ist ein Schnittknoten in G, gdw. es existiert ein Nachfolger t von v und* keine *Kante in G von einem Knoten $u \in V(T_t)$ zu einem Knoten a mit $a \neq v$, der auf dem Pfad von w zu v liegt.*



7.9. Der Satz von Menger

7.40 Definition. Seien G ein Graph, $A, B \subseteq V(G)$. Zwei Pfade P, P' heißen *disjunkt*, wenn $V(P) \cap V(P') = \varnothing$.

Eine Menge der disjunkten Pfade von A nach B ist eine Menge M von Pfaden $P_i \subseteq G$ mit jeweils einen Endpunkt in A und dem anderen Endpunkt in B so, dass die Pfade in M paarweise disjunkt sind.

7.41 Beispiel. In Abbildung 7.7 sind die Pfade $P_1 := (v_1, v_2, v_{15}, v_4, v_5, v_6)$, $P_2 := (v_{13}, v_{14}, v_{17}, v_7)$, $P_3 := (v_{12}, v_{11}, v_{10}, v_9, v_8)$ paarweise disjunkt. Der Pfad

$P_4 := (v_{12}, v_{16}, v_7)$ und Pfad P_3 sind nicht disjunkt, da die Endpunkte der beiden Pfade gleich sind und somit $V(P_3) \cap V(P_4) = \{ v_{12}, v_7 \} \neq \varnothing$.

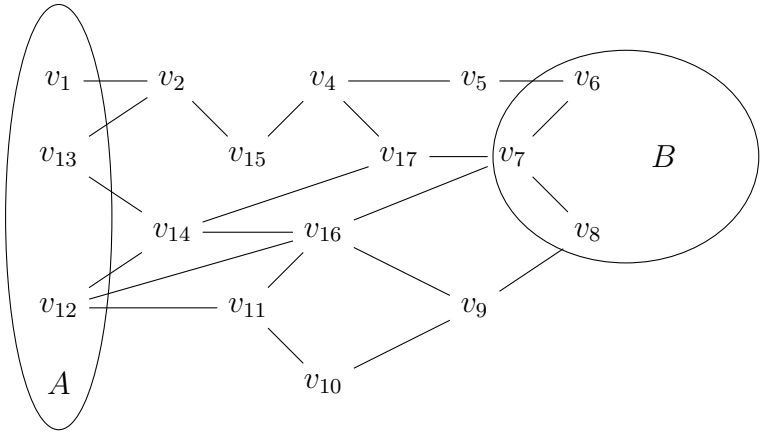


Abbildung 7.7.: Disjunkte Pfade von A nach B

7.42 Satz. *Sei G ein Graph und $A, B \subseteq V(G)$. Entweder gibt es k paarweise disjunkte Pfade von A nach B in G, oder einen Trenner $S \subseteq V(G)$ von A und B der Größe k. D.h. die maximale Zahl disjunkter $A-B$ Pfade ist gleich der minimalen Größe eines $A-B$ Trenners.*

7.43 Bemerkung. Der Satz von Menger kann in anderen Anwendungskontexte übertragen werden:

(1) Der Satz kann leicht auf gerichtete Graphen (siehe Kapitel 7.10.1) erweitert werden.

(2) Hier betrachten wir knotendisjunkte Pfade. Man kann den Satz aber auch für kantendisjunkte Pfade und Kantentrenner formulieren.

7.10. Alternative Graphmodelle

Neben den ungerichteten, einfachen Graphen, die wir bisher betrachtet haben, gibt es noch verschiedene andere Varianten von Graphen. Das wichtigste Graphenmodell neben ungerichteten sind gerichtete Graphen. Wir werden dies als Nächstes betrachten und danach dann noch kurz auf andere Varianten eingehen.

7.10.1. Gerichtete Graphen

7.44 Definition. Ein *gerichteter Graph* G besteht aus einer Menge $V(G)$ von *Knoten* und einer Menge $E(G) \subseteq V(G) \times V(G)$ von *Kanten*. G heißt *einfach*, wenn es keine Kante (u, u) für ein $u \in V(G)$ gibt. Die Zahl $|V(G)|$ heißt die *Ordnung* von G, die Zahl $|E(G)|$ heißt die *Größe*.

7.45 Beispiel. Abbildung 7.8 zeigt einen gerichteten Graphen der Ordnung 11.

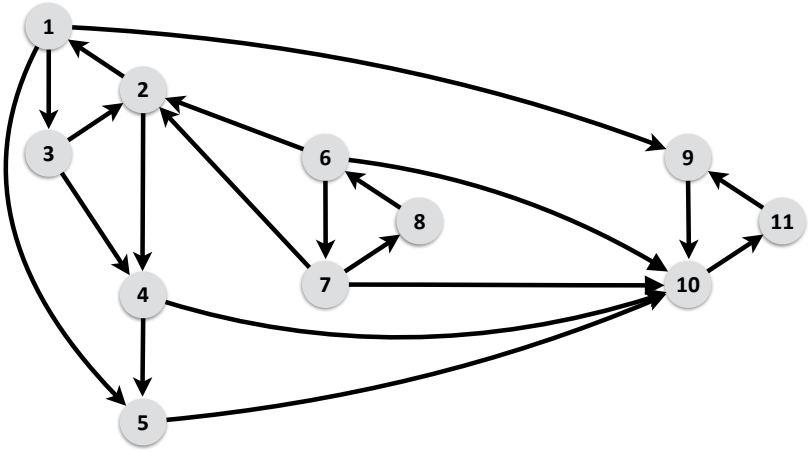


Abbildung 7.8.: Ein gerichteter Graph

Ein gerichteter Graph ist also das gleiche wie ein ungerichteter Graph mit dem Unterschied, dass eben jede Kante eine Richtung hat. Daher übertragen sich auch die meisten Begriffe wie *Adjazenz*, *Inzidenz*, *Untergraphen* und *induzierte* bzw. *spannende Untergraphen* usw. direkt von ungerichteten Graphen. Wie zuvor schreiben wir $G[U]$ für den durch eine Menge $U \subseteq V(G)$ induzierten Untergraphen von G, d.h. den Untergraphen von G mit Knotenmenge U und Kantenmenge $E(G) \cap U \times U$.

Wir gehen daher hier vor allem auf die Begriffe ein, die sich etwas unterscheiden. Sei G ein gerichteter, einfacher Graph.

- Wenn $e = (u, v) \in E(G)$ für einen gerichteten Graph G ist, dann nennen wir u den *Startknoten* und v den *Endknoten* von e.
- Sei $v \in V(G)$. Die *ausgehende Nachbarschaft* von v, geschrieben $N_G^+(v)$, ist definiert als

$$N_G^+(v) := \{u \in V(G) : (v, u) \in E(G)\}.$$

Die *eingehende Nachbarschaft* von v, geschrieben $N_G^-(v)$, ist entsprechend definiert als

$$N_G^-(v) := \{u \in V(G) : (u, v) \in E(G)\}.$$

- Entsprechend unterscheiden wir zwischen dem *Eingangsgrad* $\delta_G^-(v) := |N_G^-(v)|$ und dem *Ausgangsgrad* $\delta_G^+(v) := |N_G^+(v)|$.
- Ein *gerichteter Pfad* ist ein nicht-leerer Graph P der Form $V(P) := \{v_1, \dots, v_n\}$ und $E(G) := \{(v_i, v_{i+1}) : 1 \leqslant i < n\}$. Die *Länge* von P ist $n-1$, also die Zahl der Kanten in P. Wir sagen, dass P ein Pfad von v_1 nach v_n ist.
- Ein gerichteter *Zyklus* oder *Kreis* ist ein gerichteter Graph $C \subseteq G$, der aus einem gerichteten Pfad $P = (v_1, \dots, v_n)$ zusammen mit der Kante (v_n, v_1) besteht.

7.46 Beispiel. Betrachten wir noch einmal den Graph in Abbildung 7.8. Dann ist die eingehende Nachbarschaft des Knotens 6 die Menge $\{8\}$, die ausgehende die Menge $\{2, 7, 10\}$. Der durch die Knoten $1, 3, 4, 10, 11$ induzierte Untergraph von G ist ein gerichteter Pfad von 1 nach 11.

Etwas größere Unterschiede zu ungerichteten Graphen gibt es in Bezug auf Zusammenhang von Graphen.

7.47 Definition (Starker Zusammenhang und Zusammenhangskomponenten)**.** Sei G ein gerichteter Graph.

(1) Eine Menge $U \subseteq V(G)$ ist *stark zusammenhängend*, wenn es zu je zwei Knoten $u, v \in U$ einen gerichteten Pfad von u nach v und einen gerichteten Pfad von v nach u gibt.

(2) G heißt *stark zusammenhängend*, wenn $V(G)$ stark zusammenhängend ist.

(3) Die *starken Zusammenhangskomponenten* von G sind die maximalen stark zusammenhängenden Untergraphen von G. D.h. ein induzierter Untergraph $C \subseteq G$ ist eine starke Zusammenhangskomponente von G, wenn C stark zusammenhängend ist, aber kein $C' \subseteq G$ mit $V(C) \subseteq V(C')$ stark zusammenhängend ist.

7.48 Beispiel. Betrachten wir noch einmal den Graph in Abbildung 7.8. Die starken Zusammenhangskomponenten sind die durch die Mengen $V_1 := \{1, 2, 3\}$, $V_2 := \{4\}$, $V_3 := \{5\}$, $V_4 := \{6, 7, 8\}$ sowie $V_5 := \{9, 10, 11\}$ induzierten Untergraphen von G.

Wir können auf gerichteten Graphen die gleichen Suchverfahren, Breitensuche und Tiefensuche, wie auf ungerichteten Graphen definieren. Anstelle der bei der DFS oder BFS Suche auf ungerichteten Graphen verwendeten Nachbarschaft betrachtet man auf gerichteten Graphen nur die ausgehende Nachbarschaft, folgt also immer der Kantenrichtung.

7.49 Beispiel. Betrachten wir noch einmal den Graph in Abbildung 7.8. Abbildung 7.9 zeigt einen möglichen Tiefensuchbaum des Graphen. Zur besseren Lesbarkeit ist der Graph aus Abbildung 7.8 noch einmal abgebildet (um 90 Grad gedreht).

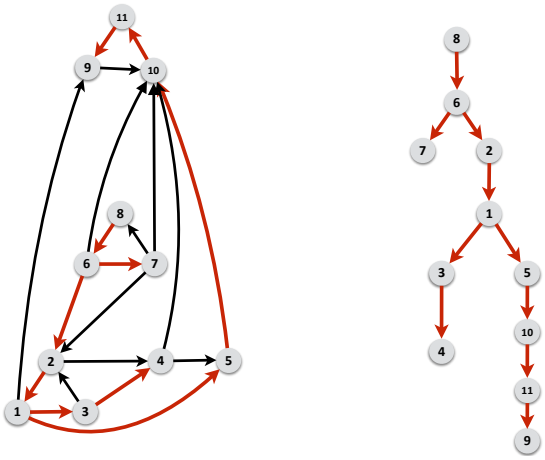


Abbildung 7.9.: Ein gerichteter Graph mit Tiefensuchbaum

Die Tiefensuche ist eine sehr effiziente Methode um starke Zusammenhangskomponenten eines gerichteten Graphen auszurechnen.

Bisweilen spricht man im Zusammenhang mit gerichteten Graphen auch vom *schwachen Zusammenhang*. Gemeint ist damit Zusammenhang im ungerichteten Graphen, den man erhält, indem man die Kantenrichtung ignoriert.

7.50 Definition. Sei G ein gerichteter Graph. Der *zugrunde liegende ungerichtete Graph* $u(G)$ ist definert als ungerichteter Graph $u(G)$ mit Knotenmenge $V(u(G)) := V(G)$ und einer Kante $\{u, v\}$ in $u(G)$ wenn (u, v) oder (v, u) eine Kante in G ist.

Ein gerichteter Graph ist *schwach zusammenhängend*, wenn $u(G)$ zusammenhängend ist.

7.10.2. Azyklische gerichtete Graphen

7.51 Definition. Ein gerichteter Graph G ist azyklisch, wenn er keinen Kreis enthält. Wir nennen die Knoten vom Eingangsgrad 0 in G *Wurzeln* oder *Quellen* und die Knoten vom Ausgangsgrad 0 *Senken.*

7.52 Beispiel. Die Abbildung 7.10 zeigt einen gerichteten azyklischen Graph. Der Graph hat eine Quelle, den Knoten 0 und eine Senke, den Knoten 11.

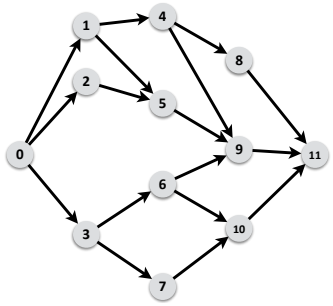


Abbildung 7.10.: Ein gerichteter, azyklischer Graph

Folgende Beobachtung folgt leicht aus der Definition azyklischer gerichteter Graphen.

7.53 Lemma. *Sei G ein azyklischer gerichteter Graph und sei R der reflexive, transitive Abschluss der Kantenrelation $E(G)$ (vgl. Definition 5.24). Dann ist R eine partielle Ordnung auf $V(G)$.*

7.54 Definition. Sei G ein azyklischer gerichteter Graph und sei R der reflexive, transitive Abschluss von $E(G)$. Eine *topologische Ordnung* auf G, oder eine *topologische Sortierung* von G, ist eine lineare Ordnung $\leqslant$ auf $V(G)$ die R enthält, d.h. es gilt $R \subseteq \leqslant$.

Eine topologische Sortierung eines azyklischen gerichteten Graphen ist also eine Reihenfolge, in der die Knoten durchlaufen werden können, so dass wenn für zwei Knoten $u, v \in V(G)$, u von v aus durch einen Pfad erreicht werden kann, dann ist $u \leqslant v$. Topologische Sortierungen können leicht durch Breitensuche gefunden werden. Dazu initialisiert man die Warteschlange im Algorithmus mit den Quellen und führt dann eine einfache Breitensuche aus.

7.55 Beispiel. Betrachten wir noch einmal den azyklischen, gerichteten Graphen aus Abbildung 7.10. Eine topologische Sortierung ist z.B. die Ordnung $0 > 1 > 2 > 3 > 4 > 5 > 6 > 7 > 8 > 9 > 10 > 11$.

7.11. Multigraphen und Hypergraphen

In gerichteten und ungerichteten Graphen kann es zwischen zwei Knoten nur höchstens eine Kante geben (in jede Richtung). Man kann auch mehrere parallele Kanten erlauben, was dann zum Begriff der Multigraphen führt. Die allermeisten Begriffe übertragen sich kanonisch auf Multigraphen.

Wichtiger als Multigraphen sind sogenannte Hypergraphen.

7.56 Definition. Ein *Hypergraph* H besteht aus einer Menge $V(H)$ von Knoten und einer Menge $E(H) \subseteq V(H)$ von *Hyperkanten*.

Hypergraphen sind also Graphen, bei denen Kanten mehr als zwei Endpunkte haben. Hypergraphen spielen in vierschiedenen Gebieten der Informatik eine Rolle, z.B. im Bereich der Datenbanken und der Auswertung konjunktiver Anfragen.

8. Algebraische Strukturen

8.1. Verbände

8.1.1. Partielle Ordnungen und Hasse Diagramme

Wir erinnern an den Begriff der partiellen Ordnung, oder Halbordnung, aus Definition 5.2, sowie minimale, maximale, kleinste und größte Elemente in solchen Ordnungen. Eine Halbordnung ist eine Ordnung, also eine reflexive, transitive und antisymmetrische Relation, in der aber nicht alle Paare von Elementen vergleichbar sein müssen.

Partielle Ordnungen lassen sich elegant durch sogenannte *Hasse Diagramme* darstellen, siehe Abbildung 8.1.

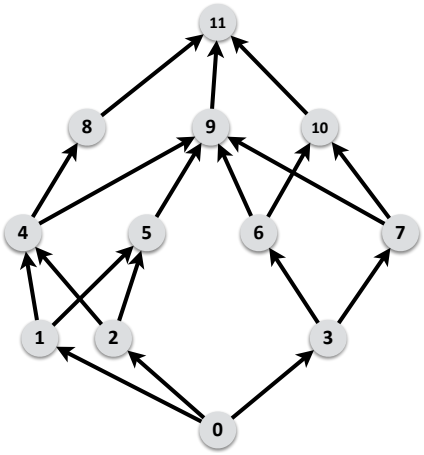


Abbildung 8.1.: Hasse Diagramm

In einem Hasse Diagramm werden die Elemente einer partiellen Ordnung $\leqslant$ auf einer Menge M als azyklischer gerichteter Graph dargestellt, der als Knotenmenge M hat und eine Kante (u, v), wenn $u < v$ und es kein $z \in M$ gibt, mit $u < z < v$. Üblicherweise werden die größeren Elemente bzgl. der Ordnung weiter oben gezeichnet.

Wir haben gesehen, dass zwar jede endliche Halbordnung minimale und maximale Elemente haben muss, diese aber nicht eindeutig sein müssen. Wir werden nun spezielle Halbordnungen kennen lernen, bei denen diese Elemente immer eindeutig existieren.

Dazu zunächst noch etwas Vorbereitung.

8.1.2. Infima, Suprema und Definition von Verbänden

8.1 Definition (Schranken)**.** Sei $\leqslant\colon (M, M)$ eine partielle Ordnung auf einer Menge M. Sei $A \subseteq M$.

(1) Ein Element $u \in M$ heißt *untere Schranke* von A (bzgl. M und $\leqslant$), wenn für alle $a \in A$ gilt:

$$u \leqslant a.$$

Eine *größte untere Schranke von A* (bzgl. X und $\leqslant$), oder auch ein *Infimum von A*, ist eine untere Schranke u von A, so dass $u' \leqslant u$ für alle unteren Schranken u' von A gilt.

(2) Ein Element $o \in M$ heißt *obere Schranke* von A (bzgl. M und $\leqslant$), wenn für alle $a \in A$ gilt:

$$a \leqslant o.$$

Eine *kleinste obere Schranke von A* (bzgl. X und $\leqslant$), oder auch ein *Supremum von A*, ist eine obere Schranke o von A, so dass $o \leqslant o'$ für alle oberen Schranken o' von A gilt.

8.2 Beispiel. Wir betrachten noch einmal die partielle Ordnung, die in Abbildung 8.1 abgebildet ist.

(1) Sei $A := \{4, 5\}$. Dann sind $1, 2, 0$ untere Schranken für A. Die Menge hat aber kein Infimum, da es kein größtes Element in $\{0, 1, 2\}$ gibt (1 und 2 sind unvergleichbar).

(2) Sei $A := \{6, 7\}$. Dann sind $9, 10, 11$ obere Schranken, aber es gibt kein Supremum.

(3) Sei $A := \{8, 9, 10\}$. Dann ist das Supremum von A der Knoten 11 und das Infimum der Knoten 0.

8.3 Bemerkung. Man beachte, dass die Schranken in Definition 8.1 aus der gesamten Menge M gewählt werden und daher nicht unbedingt in der Menge A selbst liegen.

8.4 Bemerkung. Sei $(M, <)$ eine partiell geordnete Menge und $A \subseteq M$. Wenn A ein Supremum (oder Infimum) hat, dann ist dieses immer eindeutig. Wir schreiben dann $\inf(A)$ bzw. $\sup(A)$ für das Infimum bzw. Supremum.

Wir können nun Verbände formal definieren.

8.5 Definition. Ein *Verband* ist eine partiell geordnete Menge $(M, \leqslant)$ in der jede Menge $\{a, b\} \subseteq M$ mit zwei Elementen sowohl ein Supremum als auch ein Infimum hat.

8.6 Beispiel.

- Die partielle Ordnung aus Abbildung 8.1 ist, wie wir gesehen haben, kein Verband.

- Ein Beispiel für einen (unendlichen) Verband ist folgende partiell geordnete Menge. Sei $M := \mathcal{P}(\mathbb{N})$ die Potenzmenge der natürlichen Zahlen. Wir haben bereits gesehen, dass M zusammen mit den Teilmengenbeziehung $\subseteq$ eine partielle Ordnung ist.

  Wir behaupten, dass $(M, \leqslant)$ ein Verband ist.

  Denn seien $m, n \in M$. Dann ist $n \cup m$ das Supremum und $n \cap m$ das Infimum.

  Wir beweisen hier nur die Aussage für das Supremum. Sei $s := n \cup m$. Offensichtlich gilt $n, m \subseteq s$, d.h. s ist eine obere Schranke.

  Es bleibt also noch zu zeigen, dass s die kleinste obere Schranke ist. Sei also z eine andere obere Schranke von n und m, d.h. $n \subseteq z$ und $m \subseteq z$. Wir müssen zeigen, dass $s \subseteq z$. Sei dazu $a \in s$ ein Element. Nach Konstruktion von s gilt $a \in n$ oder $a \in m$. Da $n, m \subseteq z$, gilt ferner $a \in z$. Also gilt $s \subseteq z$ und s ist ein Supremum.

Oft werden Verbände auch als algebraische Strukturen aufgefasst.

8.7 Definition. Sei $(M, \leqslant)$ ein Verband. Wir definieren Funktionen $\sqcup, \sqcap : M \times M \to M$ wie folgt: Für alle $a, b \in M$ definieren wir

$$a \sqcap b := \inf(\{a, b\})$$

als deren Infimum und

$$a \sqcup b := \sup(\{a, b\})$$

als deren Supremum. Dann können wir die Menge M zusammen mit $\sqcup$ und $\sqcap$ als algebraische Struktur $(M, \sqcap, \sqcup)$ auffassen.

8.1.3. Grundlegende Eigenschaften von Verbänden

Wir beweisen als nächstes einige grundlegende Eigenschaften von Verbänden. Das folgende Lemma folgt sofort aus der Definition eines Verbandes

8.8 Lemma (Idempotenzgesetze). *Sei $(M, \leqslant)$ ein Verband. Dann gilt für alle $u \in M$:*

(1) $u \sqcap u = u$ *und*

(2) $u \sqcup u = u$.

8.9 Lemma (Absorptionsgesetze). *Sei $(M, \leqslant)$ ein Verband. Dann gilt für alle $a, b \in M$:*

(1) $(a \sqcup b) \sqcap a = a$

(2) $(a \sqcap b) \sqcup a = a$.

Beweis: Wir zeigen hier den ersten Teil. Der zweite wird zur Übung empfohlen. Für alle $x, y \in M$ so dass $x \leqslant y$ gilt offenbar $x = x \sqcap y = y \sqcap x$. Denn sicherlich ist x eine untere Schranke von $\{x, y\}$. Es muss aber auch die größte sein, da ja jede untere Schranke u von $\{x, y\}$ auch $u \leqslant x$ erfüllen muss.

Da $a \sqcup b = \sup(\{a, b\})$ gilt $a \leqslant a \sqcup b$. D.h., $\inf(\{a \sqcup b, a\}) = (a \sqcup b) \sqcap a = a$. □

Das nächsten beiden Lemmata folgen ebenso leicht aus der Definition von Infima und Suprema.

8.10 Lemma (Kommutativitätsgesetze). *Sei $(M, \leqslant)$ ein Verband. Dann gilt für alle $a, b \in M$:*

(1) $a \sqcap b = b \sqcap a$.

(2) $a \sqcup b = b \sqcup a$.

8.11 Lemma (Assoziativitätsgesetze). *Sei $(M, \leqslant)$ ein Verband. Dann gilt für alle $a, b, c \in M$:*

(1) $\big((a \sqcap b) \sqcap c\big) = \big(a \sqcap (b \sqcap c)\big)$.

(2) $\big((a \sqcup b) \sqcup c\big) = \big(a \sqcup (b \sqcup c)\big)$.

Beweis: Wir beweisen hier nur den ersten Teil. Der zweite sei zur Übung empfohlen.

Sei $u := \inf(\{a, b\})$ und sei $u' := \inf(\{u, c\})$. Also gilt $u' = \big((a \sqcap b) \sqcap c\big)$. Wir müssen also zeigen, dass $u' = \big(a \sqcap (b \sqcap c)\big)$. Da $u' = \inf(\{u, c\})$ gilt also $u' \leqslant c$ und $u' \leqslant u$ und somit $u' \leqslant a, b, c$. Also gilt auch $u' \leqslant b \sqcap c$, da ja $b \sqcap c$ die größte untere Schranke von $\{b, c\}$ ist.

Es folgt daher, dass u' eine untere Schranke von $\{a, b \sqcap c\}$ ist. Wir müssen noch zeigen, dass es die größte ist. Sei also z eine andere untere Schranke von $\{a, b \sqcap c\}$. Wie zuvor gilt $z \leqslant a, b, c$ und $z \leqslant a \sqcap b$. Also ist z untere Schranke von $\big((a \sqcap b) \sqcap c\big)$. Da u' die größte untere Schranke von $\big((a \sqcap b) \sqcap c\big)$ ist, folgt also $z \leqslant u'$. □

Die Lemmata zusammen ergeben also folgenden Satz.

8.12 Satz. *Sei $(M, \leqslant)$ ein Verband. Dann definieren $\sqcap, \sqcup$ zwei kommutative und assoziative Verknüpfungen auf M, die die Idempotenz- und Absorptionsgesetze erfüllen.*

Umgekehrt kann man zeigen, dass jede Menge M zusammen mit zwei Verknüpfungen $\sqcap, \sqcup$, die kommutativ und assoziativ sind sowie die Idempotenz- und Absorptionsgesetze erfüllen, ein Verband definieren, in dem wir die partielle Ordnung $\leqslant$ definieren als $a \leqslant b$ genau dann, wenn $a = a \sqcap b$. Die liefert eine algebraische Definition von Verbänden.

8.1.4. Spezielle Verbände

Wir haben beim Beweis des Assoziativgesetzes für Verbände, Lemma 8.11, gezeigt, dass in einem Verband $(M, \leqslant)$ nicht nur für jede zweielementige Menge $U = \{a, b\}$ das Infimum sowie das Supremum existieren, sondern dass dies auch für dreielementige Mengen gilt. Ebenso kann man leicht per Induktion zeigen, dass jede *endliche* Teilmenge $U \subseteq M$ das Infimum und das Supremum existieren müssen.

Für unendliche Teilmengen muss das aber nicht gelten.

8.13 Definition. Ein *vollständiger Verband* ist ein Verband $(M, \leqslant)$, in dem jede Teilmenge $U \subseteq M$ ein Infimum und ein Supremum besitzt.

8.2. Halbgruppen, Monoide, Ringe und Körper

8.14 Definition (Halbgruppe)**.** Sei M eine nicht-leere Menge und sei $\circ : M \times M \to M$ eine zweistellige Funktion auf M. Das Paar $(M, \circ)$ heißt *Halbgruppe*, wenn $\circ$ assoziativ ist, d.h. für alle $x, y, z \in M$ gilt

$$(x \circ y) \circ z = x \circ (y \circ z).$$

Die Halbgruppe $(M, \circ)$ heißt *abelsch* oder *kommutativ*, wenn $\circ$ kommutativ ist, d.h. $x \circ y = y \circ x$ für alle $x, y \in M$.

Im Zusammenhang mit Halbgruppen wird die Funktion $\circ$ meistens als *Operation* bezeichnet. Wir werden in konkreten Halbgruppen meistens statt $\circ$ ein anderes Symbol verwenden, etwa $\sqcup$, $+$, ...

8.15 Beispiel. Ein Beispiel einer Halbgruppe ist $\mathbb{N}$ mit der natürlichen Addition.

8.16 Definition. Sei $(M, \circ)$ eine Halbgruppe.

(1) Ein Element $m \in M$ heißt *idempotent*, wenn $m \circ m = m$.

(2) Ein Element $e_l \in M$ heißt *linksneutral* (bzgl. $(M, \circ)$), wenn für alle $m \in M$ gilt: $e_l \circ m = m$.

(3) Ein Element $e_l \in M$ heißt *rechtsneutral* (bzgl. $(M, \circ)$), wenn für alle $m \in M$ gilt: $m \circ e_r = m$.

(4) Ein Element $e \in M$ heißt *neutral*, wenn es links- und rechtsneutral ist.

Mit Hilfe neutraler Elemente können wir nun den nächsten wichtigen Begriff einführen, die Monoide.

8.17 Definition. Ein *Monoid* ist ein Triple $(M, \circ, e)$, wobei $(M, \circ)$ eine Halbgruppe ist und e ein neutrales Element von $(M, \circ)$. Ist $\circ$ kommutativ, so heißt $(M, \circ, e)$ ein kommutativer Monoid.

8.18 Beispiel. Die natürlichen Zahlen $\mathbb{N}$ zusammen mit der Addition $\circ := +$ und der 0 als neutrales Element bilden ein Monoid. Ebenso $\mathbb{N}$ zusammen mit der Multiplikation $\circ := \cdot$ und der 1 als neutralem Element.

Eine besonders wichtige Klasse von Monoiden sind die sogenannten Gruppen. Das besondere an Gruppen ist, dass in einer Gruppe jedes Element ein inverses hat.

8.19 Definition (Gruppe)**.** Eine *Gruppe* ist ein Monoid $(M, \circ, e)$ in dem es für jedes Element $a \in M$ ein Element $a^{-1} \in M$ gibt, so dass

$$a \circ a^{-1} \quad = \quad a^{-1} \circ a \quad = \quad e.$$

Die Gruppe heißt *abelsch* oder *kommutativ*, wenn $\circ$ kommutativ ist.

Oft ist es nützlich, in Gruppen explizit $\cdot^{-1}$ als Abbildung $\cdot^{-1} : M \to M$ aufzufassen, die jedem Element $a \in M$ das inverse Element a^{-1} zuordnet.

8.20 Beispiel. Ein Beispiel für eine Gruppe ist $(\mathbb{Z}, +, 0)$, da $+$ assoziativ ist, 0 ein neutrales Element und für jedes $n \in \mathbb{Z}$ das Element $-n$ das inverse Element ist.

Gruppen treten in vielen verschiedenen Anwendungsgebieten und Teilbereichen der Informatik und Mathematik auf und es gibt eine sehr umfangreiche Literatur zur Gruppentheorie.

Zum Schluss behandeln wir noch kurz zwei weitere wichtige algebraische Strukturen.

8.21 Definition. Ein *Ring* ist ein Tupel $\mathcal{R} := (M, \cdot, +, 0, 1)$, wobei

- M eine Menge ist und $0, 1 \in M$ und
- $+, \cdot : M \times M \to M$ binäre Operationen auf M sind,

so dass gilt:

(1) $(M, +, 0)$ ist eine kommutative Gruppe.

(2) $(M, \circ, 1)$ ist ein Monoid.

(3) Es gelten folgende Distributivgesetze:

- $a \cdot (b + c) = a \cdot b + a \cdot c$ für alle $a, b, c \in M$.
- $(a + b) \cdot c = a \cdot c + b \cdot c$ für alle $a, b, c \in M$.

Ist $(M, \circ, 1)$ eine Gruppe, d.h. existiert für jedes $m \in M$ ein multiplikatives Inverses m^{-1} mit $m^{-1} \cdot m = m \cdot m^{-1} = 1$, dann heißt $\mathcal{R}$ ein *Schiefkörper*. Ist $(M, \cdot, 1)$ sogar kommutativ, dann heißt $\mathcal{R}$ ein *Körper*.

Anhang

A. Mathematische Notation

A.1. Standardnotationen

Die folgende Tabelle listet einige öfters verwendete Notationen auf.

Symbol	Bedeutung
$:=$	Definition eines Wertes, z.B. $x := 5$, $M := \{1, 2, 3\}$
$:\Leftrightarrow$	Definition einer Eigenschaft oder einer Schreibweise z.B. $m \in M :\Leftrightarrow m$ 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"
$\Rightarrow$	Abkürzung für "impliziert" z.B.: Regen $\Rightarrow$ nasse Straße
$\Leftrightarrow$	Abkürzung für "genau dann, wenn" z.B.: Klausur bestanden $\Leftrightarrow$ die erreichte Prozentzahl z ist $> 50\%$
$\square$	markiert das Ende eines Beweises
$\dashv$	markiert das Ende eines Beispiels oder Zwischenschritts

B. Griechische Symbole

Anbei eine Liste einiger häufig benutzter griechischer Symbole, teilweise in Klein- und Großschreibweise, sortiert nach Verwendungsarten.

α	alpha
β	beta
γ, Γ	gamma
δ, Δ	delta
ε	epsilon
φ, Φ	phi
ψ, Ψ	psi
ϑ, Θ	theta
χ	chi
ξ, Ξ	xi
λ, Λ	lambda
ω, Ω	omega
μ	mü
ν	nü