Diskrete Strukturen

Wintersemester 2024-25 Universität Leipzig

Inhaltsverzeichnis

Vorwort

Dieses Skript enthält die wesentlichen Inhalte der Vorlesung mit einigen zusätzlichen Informationen. Es wurde für Ihre Vor- und Nachbereitung von mehreren Personen in laufe mehrerer Jahre entwickelt, darunter (in chronologischer Reihenfolge) Mirko Schulze, Andrea Maletti, und Łukasz Grabowski.

Kapitel 1

Logik

Wir beschäftigen uns zunächst mit den Grundlagen der mathematischen Sprache und den Regeln, die gültigen Beweisen zugrunde liegen.

Bemerkung 1.0.1. Die Geschichte der Logik reicht Tausende von Jahren zurück. Doch erst zu Beginn des 20. Jahrhunderts wurde die Logik zu einem vollwertigen Teilgebiet der Mathematik. Die Motivation für diese Entwicklung war das Studium der Mathematik selbst, insbesondere um besser zu verstehen, was mathematische Beweise sind und was bewiesen werden kann und was nicht. Diese Entwicklungen wurden später zu Grundpfeilern der Informatik.

In diesem Kapitel versuchen wir nicht, eine vollständig formale Behandlung der Logik in diesem Sinne zu geben, sondern wir verwenden die Intuitionen aus dem täglichen Leben, um bestimmte Definitionen zu motivieren. Dies sollte uns ein gutes Verständnis für die Motivation hinter den klassischen Logiken vermitteln: der Aussagen- und Prädikatenlogik.

Allgemein liefert "eine Logik" die "gültigen" Beweistechniken und daraus abgeleitet die "gültigen" Folgerungen. Für die klassische Aussagen- und Prädikatenlogik werden wir Ihnen diese Beweistechniken in diesem Kapitel vorstellen - diese sind durch die alltäglichen Regeln motiviert, die wir verwenden, um Regeln, Gesetze usw. zu verstehen.

Wie oben erwähnt, einige der Definitionen, die wir einführen, sind nicht ganz formal, da das uns erlaubt die uns zur Verfügung stehenden Alltagsbegriffe besser nutzen zu können. Eine formale Einführung in verschiedene Logiken und automatische Schlussfolgerungssysteme liefert das Modul "Logik" (2. Semester B.Sc. Informatik).

Betrachten wir zunächst den folgenden Gesetzestext.

StGB § 211 — Mord

(1) Der Mörder wird mit lebenslanger Freiheitsstrafe bestraft.
(2) Mörder ist, wer

- aus Mordlust, zur Befriedigung des Geschlechtstriebs,
  aus Habgier oder sonst aus niedrigen Beweggründen,
- heimtückisch oder grausam oder mit gemeingefährlichen Mitteln oder
- um eine andere Straftat zu ermöglichen oder zu verdecken,

einen Menschen tötet.

Beziehen wir uns auf eine konkrete Person Alice, so beobachten wir:

1. Mit Hilfe der im Gesetz genannten Begriffe können wir Aussagen formulieren.

   Alice-ist-Mörder Alice-tötet-aus-Habgier
   Alice-bekommt-lebenslang Alice-tötet-heimtückisch

2. Aussagen können zur Beschreibung eines Sachverhalts kombiniert werden.

   Alice-tötet-aus-Habgier oder Alice-tötet-heimtückisch

3. Teile des Gesetzes können jetzt als folgende Folgerungen formuliert werden.

   wenn Alice-tötet-aus-Habgier dann Alice-ist-Mörder
   wenn Alice-ist-Mörder dann Alice-bekommt-lebenslang

Definition 1.0.2 (Aussage)**.** Eine Aussage ist eine Repräsentation eines Satzes, der entweder wahr (kurz 1) oder falsch (kurz 0) ist.

Eine Aussage hat also genau einen Wahrheitswert, dieser kann jedoch unbekannt oder auch nicht feststellbar sein. Dies muss von den alltäglichen Äußerungen unterschieden werden, denen man keinen einzelnen Wahrheitswert zuordnen kann; derartige Äußerungen sind keine Aussagen im Sinne der obigen Definition.

Beispiele 1.0.3.

- *"L befördert gerade frische Milch"*
  — ist eine Aussage für einen gegebenen Lastkraftwagen L.
  (Der Wahrheitswert dieser Aussage mag vom aktuellen Zeitpunkt abhängen, aber zu jedem Zeitpunkt ist dieser Satz entweder wahr oder falsch und damit eine Aussage.)
- *"2 ist eine Primzahl" — ist eine wahre Aussage.*
- *"$2 + 2 = 5$" — ist eine falsche Aussage.*
- *"Hallo Welt!" — ist keine Aussage.*
- *"Jede gerade natürliche Zahl $n > 2$ ist die Summe zweier Primzahlen"*
  *— ist eine Aussage mit unbekanntem Wahrheitswert ("*Goldbachs Vermutung*").*

Gegenstand der Aussagenlogik ist nicht die Wahrheitsbestimmung von Basis-Aussagen, sondern die Bewertung von Aussagenverknüpfungen anhand ihrer Struktur. Für logische Untersuchungen reduzieren wir Aussagen daher auf ihre logische Form (Formalisierung). Außerdem beschränken wir uns auf einige wenige Verknüpungsweisen. Aussagen F und G können über die folgenden Junktoren verknüpft werden:

Negation	$\neg F$	nicht F
Konjunktion	$F \wedge G$	F und G
Disjunktion	$F \vee G$	F oder G
Implikation	$F \to G$	wenn F, dann G
beidseitige Implikation	$F \leftrightarrow G$	F genau dann, wenn G

Wir nennen Aussagenvariablen wie A, B, ... aussagenlogische Atome und beliebige Verknüpfungen von Atomen mit Hilfe der obigen Junktoren aussagenlogische Formeln. Bei verschachtelten Formeln ist die Verknüpfungsreihenfolge durch Klammerung kenntlich zu machen. Dabei vereinbaren wir, dass die Negation stärker bindet als die übrigen Junktoren.

Beispiele 1.0.4.

- $\big((A \wedge B) \wedge C\big) \to (B \vee D)$
  (wenn A und B und C, dann B oder D)
- $\neg A \vee B$ — *die Negation bezieht sich hier auf A*
- B — *auch Atome selbst sind Formeln*

Die Wahrheit von Atomen ist abhängig von der fachlichen Aussage, mit der wir sie interpretieren. Hingegen ist die Wahrheit einer Formel nur abhängig von der Wahrheit ihrer Atome und der Interpretation der Junktoren. Letztere legen wir gemäß der folgenden Tabelle unmissverständlich fest.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \to B$	$A \leftrightarrow B$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Die meisten Verständnisschwierigkeiten gehen von der Implikation aus. Eine implikative Aussage $A \to B$ besteht aus Vorbedingung A und Folgerung B. Wie kann eine solche Aussage wahr sein, wenn schon ihre Vorbedingung falsch ist? Betrachten wir das Beispiel: "Wenn es regnet, dann bleibe ich zu Hause." Wenn es nicht regnet, können wir keine Konsequenzen daraus ziehen, ob wir zu Hause bleiben. Das bedeutet dass die Aussage

"Wenn es regnet, dann bleibe ich zu Hause." möglicherweise wahr ist, auch wenn z.B. die beiden Aussagen "Es regnet" und "Ich bleibe zu Hause" falsch sind.

Abschließend sei angemerkt, dass die Einführung weiterer Junktoren denkbar ist. Exemplarisch überlege man sich die Interpretation von "entweder A oder B" (exklusive Disjunktion). Es ist jedoch möglich alle anderen Junktoren durch die oben genannten vier auszudrücken, wie wir später sehen werden.

1.1 Wahrheitstabellen

Die einfachste Methode, eine gegebene Aussageformel zu untersuchen, ist anhand ihrer "Wahrheitstabelle". Hier sind die notwendige Schritte zur Erstellung so einer Wahrheitstabelle.

1. Identifikation aller vorkommenden Atome $A_1, \ldots, A_n$
2. Auflistung aller 2^n Wahrheitswertbelegungen für $A_1, \ldots, A_n$ (sortiert)

A_1	A_2	$\cdots$	A_{n-1}	A_n	$\cdots$
0	0	$\cdots$	0	0	$\cdots$
0	0	$\cdots$	0	1	$\cdots$
0	0	$\cdots$	1	0	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
1	1	$\cdots$	1	1	$\cdots$

3. Berechnung der Wahrheitswerte der Teilformeln

Beispiel 1.1.1. *Die Wahrheitstabelle der Aussageformel* $(A \wedge B) \to A$.

A	B	$A \wedge B$	$(A \wedge B) \to A$
0	*0*	*0*	*1*
0	*1*	*0*	*1*
1	*0*	*0*	*1*
1	*1*	*1*	*1*

In diesem Fall sehen wir dass die Aussageformel immer wahr ist, unabhängig davon was die Werte von A und B sind. Natürlich ist das nicht der Fall für alle Aussageformeln.

Beispiel 1.1.2. *Betrachten wir die folgende Aussage:*

Eine natürliche Zahl, die nicht ungerade ist, ist gerade. (1.1)

Wir bezezeichnet mit U die Aussage "die Zahl n ist ungerade" und mit G die Aussage "die Zahl n is gerade", wobei n ist eine beliebige, aber feste, Zahl. Also die Formaliesirung der Aussage (1.1) ist $\neg U \to G$. Hier ist die Wahrheitstabelle davon:

U	G	$\neg U$	$\neg U \to G$
0	0	1	0
0	1	1	1
1	0	0	1
1	1	0	1

Es ist vielleicht etwas überraschend, dass, obwohl wir mit einer offensichtlich wahren Aussage (1.1) begonnen haben, die logische Formalisierung die wir geschrieben haben nicht immer wahr ist. Dies geschieht, weil es Abhängigkeiten zwischen den Atomen bestehen, die bei der Formalisierung nicht erfasst wurden.

In diesem Fall betrachten wir noch die folgende wahre Aussage:

Jede natürliche Zahl ist gerade oder ungerade. (1.2)

Das bedeutet dass in unserer Situation die Aussage $U \vee G$ immer wahr ist. Intuitiv soll es klar sein dass der Grund warum die Aussage (1.1) wahr ist, ist genau dass die Aussage (1.2) wahr ist. Diese Intuition kann wie folgt formalisiert werden: $(U \vee G) \to (\neg U \to G)$. Wir schreiben die Wahrheitstabelle davon:

U	G	$U \vee G$	$\neg U$	$\neg U \to G$	$(U \vee G) \to (\neg U \to G)$
0	0	0	1	0	1
0	1	1	1	1	1
1	0	1	0	1	1
1	1	1	0	1	1

Also sehen wir dass die Aussageformel $(U \vee G) \to (\neg U \to G)$ immer wahr ist, unabhängig davon wass die Werte von U und G sind.

1.2 Äquivalenz von Formeln

Wir behandeln Formeln im weitesten Sinne als Zeichenketten. Als solche sind Formeln nur dann gleich, wenn sie auf Zeichenebene übereinstimmen. Unwesentlich sind nur die

„überflüssige“ Klammern. Beispielsweise gilt

$$(A \wedge B) \wedge C \neq A \wedge (B \wedge C),$$
$$(A \wedge B) \wedge C = ((A \wedge B) \wedge C).$$

Trotz ihrer Ungleichheit verhalten sich die Formeln aus der oberen Zeile logisch gleich. Wir nennen diesen Zusammenhang logische Äquivalenz. Zwei Formeln sind äquivalent genau dann, wenn deren Wahrheitswerte für alle Belegungen der Atome übereinstimmen. Ob zwei Formeln äquivalent sind, lässt sich natürlich aus ihren Wahrheitstabellen ablesen.

Beispiele 1.2.1.

- *Die Formeln* $(A \wedge B) \wedge C$ *und* $A \wedge (B \wedge C)$ *sind äquivalent.*
- *Die Formeln* $(A \to B) \to C$ *und* $A \to (B \to C)$ *sind nicht äquivalent.*

A	B	C	$(A \to B) \to C$	$A \to (B \to C)$
0	*0*	*0*	*0*	*1*

Wenn wir eine große Formel F haben und darin eine Unterformel U sehen, können wir U durch eine äquivalente Unterformel U' ersetzen und erhalten so eine neue formel F' die zu F äquivalent ist. Dieses Substitutionsprinzip eröffnet uns die Möglichkeit die Formeln zu vereinfachen, und zu zeigen dass zwei Formelm äquivalent sind, durch Äquivalenzketten.

Die folgenden Formel-Äquivalenzen können mit Wahrheitstabellen überprüft werden.

Äquivalente Formeln		Bezeichnung
$A \wedge B$	$B \wedge A$	Kommutativität von $\wedge$
$A \vee B$	$B \vee A$	Kommutativität von $\vee$
$(A \wedge B) \wedge C$	$A \wedge (B \wedge C)$	Assoziativität von $\wedge$
$(A \vee B) \vee C$	$A \vee (B \vee C)$	Assoziativität von $\vee$
$A \wedge (B \vee C)$	$(A \wedge B) \vee (A \wedge C)$	Distributivität von $\wedge$
$A \vee (B \wedge C)$	$(A \vee B) \wedge (A \vee C)$	Distributivität von $\vee$
$A \wedge A$	A	Idempotenz von $\wedge$
$A \vee A$	A	Idempotenz von $\vee$
$\neg\neg A$	A	Involution $\neg$
$\neg(A \wedge B)$	$(\neg A) \vee (\neg B)$	De-Morgan-Gesetz für $\wedge$
$\neg(A \vee B)$	$(\neg A) \wedge (\neg B)$	De-Morgan-Gesetz für $\vee$
$A \wedge (A \vee B)$	A	Absorptionsgesetz für $\wedge$
$A \vee (A \wedge B)$	A	Absorptionsgesetz für $\vee$
$A \to B$	$\neg A \vee B$	Elimination von $\to$
$A \leftrightarrow B$	$(A \to B) \wedge (B \to A)$	Elimination von $\leftrightarrow$

Wir verwenden diese oft, um Äquivalenzketten zu bilden, wie im folgenden Beispiel.

Beispiel 1.2.2 (Äquivalenzkette)**.**

$$
\begin{array}{lll}
 & ((A \wedge B) \vee (A \wedge C)) \wedge A & \\
\textit{ist äquivalent zu} & (A \wedge (B \vee C)) \wedge A & \text{(Distributivität } \wedge\text{)} \\
\textit{ist äquivalent zu} & A \wedge (A \wedge (B \vee C)) & \text{(Kommutativität } \wedge\text{)} \\
\textit{ist äquivalent zu} & (A \wedge A) \wedge (B \vee C) & \text{(Assoziativität } \wedge\text{)} \\
\textit{ist äquivalent zu} & A \wedge (B \vee C) & \text{(Idempotenz } \wedge\text{)}
\end{array}
$$

1.3 Formel-Äquivalenzen als Beweisprinzipien

Viele mathematische Aussagen sind Wenn-dann-Aussagen, haben also eine implikative Struktur. Gemäß der Eliminationsregel (siehe Übersicht) lassen sich Beweise für Aussagen der Form $A \leftrightarrow B$ auf Beweise für $A \to B$ und $B \to A$ reduzieren.

Beispiel 1.3.1. *Betrachten wir den Satz "Eine natürliche Zahl n ist nur dann durch 3 teilbar, wenn die Summe ihrer Dezimalziffern durch 3 teilbar ist". Da die Formeln $A \iff B$ und $(A \to B) \wedge (B \to A)$ äquivalent sind, ist dieser Satz äquivalent dem Satz "Wenn n durch 3 teilbar ist, dann ist die Summe seiner Dezimalstellen durch 3 teilbar. Und wenn die Summe seiner Dezimalziffern durch 3 teilbar ist, dann ist n durch 3 teilbar".*

Die erste Formulierung ist natürlich kürzer und wird daher normalerweise bei der Darstellung des Ergebnisses verwendet. Bei der eigentlichen Beweisführung wäre es jedoch bequemer, mit der zweiten Formulierung zu arbeiten. Den Studenten wird im Allgemeinen geraten, beim Beweis von Äquivalenzen immer beide Implikationen zu beweisen.

Konzentrieren wir uns auf Beweisprinzipien für die Implikation. Ein solches sehr häufig verwendetes Beweisprinzip ist die Kontraposition. Anstelle des Beweises einer Aussage $A \to B$ kann ein Beweis für die Aussage $\neg B \to \neg A$ geführt werden, da beide Aussagen äquivalent sind.

Satz 1.3.2 (Kontraposition)**.** *Die Formeln $A \to B$ und $\neg B \to \neg A$ sind äquivalent.*

Beweis.

$$
\begin{array}{lll}
 & A \to B & \\
\text{ist äquivalent zu} & \neg A \vee B & \text{(Elimination } \to\text{)} \\
\text{ist äquivalent zu} & \neg A \vee \neg\neg B & \text{(Involution } \neg\text{)} \\
\text{ist äquivalent zu} & \neg\neg B \vee \neg A & \text{(Kommutativität } \vee\text{)} \\
\text{ist äquivalent zu} & \neg B \to \neg A & \square \quad \text{(Elimination } \to\text{)}
\end{array}
$$

Beispiel 1.3.3. *Sei n eine beliebige ganze Zahl. Falls n^2 gerade ist, so ist auch n gerade.*

Beweis. (Kontraposition) Anstelle von

$$\text{QuadratGerade} \to \text{ZahlGerade}$$

beweisen wir die Kontraposition

$$\neg\text{ZahlGerade} \to \neg\text{QuadratGerade}$$

Sei n eine Ganzzahl, die nicht gerade, also ungerade, ist. Dann gilt $n = 2k + 1$ für eine ganze Zahl k (die geraden Zahlen sind die Vielfachen von 2 und jede ungerade Zahl ist Nachfolger einer geraden Zahl) und

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1,$$

womit n^2 wieder ungerade (nicht gerade) ist (da Nachfolger einer geraden Zahl). Damit ist die Kontraposition nachgewiesen und da die Ursprungsaussage äquivalent ist, ist diese ebenso bewiesen. □

1.4 Tautologien

Wir haben bereits Beispiele für Formeln gesehen, die immer wahr sind, unabhängig von den Werten der Atome. Wir werden gleich sehen, wie solche Formeln als Beweistechniken verwendet werden können. In der Tat sind alle Beweisprinzipien derartige universell wahre Formeln.

Definition 1.4.1 (Tautologie, unerfüllbar, erfüllbar, widerlegbar)**.** Eine Formel ist

- eine Tautologie (oder tautologisch), falls sie unabhängig von der Belegung der Atome wahr ist, (Tautologien sind immer wahr)
- unerfüllbar (oder Kontradiktion), falls sie unabhängig von der Belegung der

Atome falsch ist, (unerfüllbare Formeln sind immer falsch)

- erfüllbar, falls sie nicht unerfüllbar ist,
  (d. h. es gibt eine Belegung der Atome, so dass die Formel wahr ist),
- widerlegbar, falls sie keine Tautologie ist.
  (d. h. es gibt eine Belegung der Atome, so dass die Formel falsch ist)

Beispiel 1.4.2. *Wenn wir zwei Formeln F and F' haben die äquivalent sind dann ist die Formel $F \iff F'$ eine Tautologie. Auch umgekehrt, wenn $F \iff F'$ eine Tautologie ist, dann sind Fund F' equivalent zu einander. Anders gesagt die zwei Aussagen "F and F' sind äquivalent" und "$F \iff F'$ is eine Tautologie" sind äquivalent.*

Beispiele 1.4.3.

- *Die Formel $(A \wedge A) \leftrightarrow A$ ist eine Tautologie.*

  Tatsächlich ist für alle äquivalenten Aussagen A und B die Aussage $A \leftrightarrow B$ stets eine Tautologie und umgekehrt.

- *Die Formel Gerade $\leftrightarrow \neg$Ungerade ist erfüllbar, aber auch widerlegbar, obwohl die Hintergrundaussage mit Fachwissen wahr ist.*

Wir haben eine Übersicht von wichtigen Tautologien zusammengestellt. Diese dienen der Rechtfertigung weiterer Beweisprinzipien.

Klassische Tautologien	Bezeichnung
$A \vee \neg A$	Ausgeschlossenes Drittes
$((A \vee B) \wedge (A \to C) \wedge (B \to C)) \to C$	Fallunterscheidung
$(A \wedge (A \to B)) \to B$	Modus ponens
$((A \to B) \wedge (B \to C)) \to (A \to C)$	Transitivität von $\to$
$(A \to B) \leftrightarrow (\neg B \to \neg A)$	Kontraposition
$((\neg A \to B) \wedge (\neg A \to \neg B)) \to A$	Reductio ad absurdum (Indirekter Beweis)
$(A \wedge B) \to A$	Abschwächung für $\wedge$
$A \to (A \vee B)$	Abschwächung für $\vee$

Als Beispiele beweisen wir zwei von diesen Tautologien, die sehr häufig als Beweistechnike verwendet werden.

Satz 1.4.4 (Modus Ponens)**.** *Die Formel* $(A \wedge (A \to B)) \to B$ *ist eine Tautologie.*

Beweis. Wir beweisen es mit Hilfe der Wahrheitstabelle. Anstatt sie explizit aufzuschreiben, ist es praktisch, die folgenden Fälle zu betrachten.

- Falls B wahr ist, dann ist $F = \cdots \to B$ wahr.
- Falls B falsch ist, dann ist entweder (weitere Fallunterscheidung)
  - A wahr, womit $A \wedge (A \to B)$ falsch ist oder
  - A falsch, womit $A \wedge (A \to B)$ auch falsch ist.

  In beiden Fällen ist also $F' = A \wedge (A \to B)$ falsch und damit $F = F' \to B$ wahr.

In beiden Fällen ist also, wie gewünscht, F wahr. Da es keine weiteren Fälle gibt, ist die Aussage bewiesen. □

Nun rechtfertigen wir das Prinzip der Schlusskette; d.h. die mehrfache Anwendung von Schlussregeln wie dem Modus Ponens, um eine Behauptung zu beweisen. Ein solches Vorgehen nennen wir direkten Beweis.

Satz 1.4.5 (Schlusskette)**.** *Die Formel* $((A \to B) \wedge (B \to C)) \to (A \to C)$ *ist eine Tautologie.*

Beweis. Wir zeigen die Kontraposition $F = \neg(A \to C) \to \underbrace{\neg((A \to B) \wedge (B \to C))}_{F'}$.

Fallunterscheidung:

- Falls $\neg(A \to C)$ falsch ist, dann ist F wahr.
- Falls $\neg(A \to C)$ wahr ist, dann ist $A \to C$ falsch, woraus A wahr und C falsch folgen.
  - Sei B falsch. Dann ist $A \to B$ falsch und damit F' wahr.
  - Sei B wahr. Dann ist $B \to C$ falsch und damit F' wahr.

  Da F' wahr ist, ist auch F wahr. □

Bemerkung 1.4.6. Für die Beweise oben nutzten wir ein weiteres Beweisprinzip: die Fallunterscheidung. Wir haben gesehen, dass man sich innerhalb eines Beweises in einem von mehreren möglichen Fällen befinden kann. Genauer: Dass man von der Gültigkeit von einer aus endlich vielen zusätzlichen Annahmen weiß. Zur Ausnutzung

dieses Umstandes sind zwei Schritte zu erfüllen:

1. Vollständige Aufstellung der möglichen Fälle
2. Einzelbetrachtung eines jeden Falls mit Angabe eines Beweises unter Ausnutzung der zusätzlichen Annahme

1.5 Indirekte Beweise - „Beweis durch Widerspruch“

Für manche Aussagen ist ein direkter Beweis nicht oder nur unter erschwerten Bedingungen möglich. Eine Alternative bietet das Prinzip der Reductio ad absurdum: Eine Behauptung gilt als bewiesen, wenn aus ihrer Negation ein Widerspruch hergeleitet werden kann. Ein solcher Beweis wird indirekt oder auch Widerspruchsbeweis oder Beweise durch Widerspruch genannt .

Satz 1.5.1 (indirekter Beweis)**.** *Die Formel* $((\neg A \to B) \wedge (\neg A \to \neg B)) \to A$ *ist eine Tautologie.*

Anstelle des einfachen Beweises betrachten wir ein Beispiel.

Beispiel 1.5.2. *Es gibt keine rationale Zahl* x *mit* $x^2 = 2$.

Beweis. (indirekt) Angenommen es gäbe eine rationale Zahl x, so dass $x^2 = 2$.

Dann existieren teilerfremde ganze Zahlen m und n mit $n \neq 0$ und $x = \frac{m}{n}$. Also auch

$$2 = x^2 = (\tfrac{m}{n})^2 = \tfrac{m^2}{n^2}$$

und damit $2n^2 = m^2$, womit m^2 gerade ist. Somit ist auch m, also existiert eine ganze Zahl k mit $m = 2k$. Es gilt

$$2n^2 = m^2 = (2k)^2 = 4k^2 \implies n^2 = 2k^2.$$

Also ist auch n^2 gerade und damit auch n.

Da m und n gerade sind, sind sie nicht teilerfremd. Es gibt also eine teilerfremde Darstellung und gleichzeitig kann es diese nicht geben. Widerspruch. Folglich gilt die Behauptung. □

Zur Analyse der Beweisstruktur betrachten wir die folgenden Aussagen:

- $\underbrace{\text{Es existiert eine rationale Zahl } x \text{ mit } x^2 = 2.}_{\neg A}$
- $\underbrace{\text{Es existieren teilerfremde ganze Zahlen } m \text{ und } n \text{ mit } n \neq 0 \text{ und } (\frac{m}{n})^2 = 2.}_{B}$

Wir zeigten nacheinander die Aussagen $\neg A \to B$ und $\neg A \to \neg B$ durch direkte Beweise und konnten so schließlich das Prinzip der Reductio ad absurdum anwenden. Beachten Sie jedoch, dass bei realer Beweisführung eine passende Aussage B erst gefunden werden muss, auch wenn man dem fertigen Beweis diese Tatsache nicht mehr ansehen mag. Aufgrund des nicht-konstruktiven Charakters indirekter Beweise bieten diese oft weniger tiefe Einblicke in den mathematischen Sachverhalt als direkte Beweise.

1.6 Die Sprache der Prädikatenlogik

Betrachten wir die bisherigen Beispiele erneut, so fallen einige Beschränkungen der Aussagenlogik ins Auge. Versuchen wir, eine Beispielaussage zu formalisieren.

Beispiel 1.6.1. *Sei n eine beliebige ganze Zahl. Falls n^2 gerade ist, so ist auch n gerade.*

- *Formalisierung: QuadratGerade $\to$ ZahlGerade*

  Hier sind weder die Beschränkung auf ganze Zahlen, noch die Abhängigkeit der beiden Zahlen untereinander modelliert. Außerdem ist die Aussage nur für eine Zahl modelliert.

- *Formalisierung:* $\Big(1gerade \to (1gerade \wedge \text{-}1gerade)\Big) \wedge \Big(4gerade \to (\cdots)\Big) \wedge \cdots$

  Hier liegt eine ineffiziente, unendliche Auflistung von Formeln vor. Dabei benötigen wir unendlich viele Atome. Dies ist auch nicht reparierbar, denn Formeln sind stets endlich.

Obwohl eine Aussage vorliegt, können wir ihre interne Struktur nicht geeignet formalisieren. Deshalb erweitern wir die Aussagenlogik um neue „Features“. Unsere im Beispiel gemachten Beobachtungen motivieren die Einführung von

- Variablen und Prädikaten, die als “Aussagenschablonen” betrachtet werden können.
- Quantoren zur Modellierung der Beschränkung bzw. Wahl der Variablen.

Intuitiv sind Prädikaten abstrakte Aussagen, in denen Variablen zugelassen sind, so dass für jede Belegung der Variablen eine konkrete Aussage entsteht.

Beispiel 1.6.2 (Fortsetzung)**.** *Wir identifizieren*

- *QuadratGerade(n) als Aussagenschablone mit*

  “Das Quadrat der Zahl n ist gerade.”

- *Gerade(n) als Aussagenschablone mit*

"Die Zahl n ist gerade."

Durch Einsetzen eines konkreten Objektes oder Quantifizierung aller Variablen erhält man eine Aussage. Die Quantifizierung durch Quantoren erlaubt die Formalisierung von gewissen Variablenbelegungen, für die eine Aussagenschablone gelten soll:

- Der Allquantor $\forall$ fordert die Gültigkeit der Aussagenschablone für alle möglichen Belegungen einer Variable,
- der Existenzquantor $\exists$ fordert die Gültigkeit der Aussagenschablone für mindestens eine Belegung einer Variable.

Dabei nehmen wir entweder implizit ein Universum aller Objekte an, so dass jedes denkbare Objekt Belegung einer Variable sein kann oder wir geben im Kontext der Formeln explizit einen Grundbereich für die Variablenbelegung an.

Beispiel 1.6.3 (Fortsetzung)**.** *Mithilfe der neuen Ausdrucksmittel erreichen wir die Formalisierung*

$$\forall n\Big(\mathit{GanzeZahl}(n) \to \big(\mathit{QuadratGerade}(n) \to \mathit{Gerade}(n)\big)\Big).$$

Betrachten wir explizit den Bereich der ganzen Zahlen, so reduziert sich die Formel auf

$$\forall n\Big(\mathit{QuadratGerade}(n) \to \mathit{Gerade}(n)\Big).$$

Beispiel 1.6.4 (Existenzquantor)**.** *Wir formalisieren die Aussage*

"Es gibt keine rationale Zahl x mit $x^2 = 2$"

als

$$\neg\exists x\big(\mathit{Rat}(x) \wedge \mathit{Quadrat{=}2}(x)\big),$$

wobei $\mathit{Rat}(x)$ das Prädikat "x is eine Rationale Zahl" ist, und $\mathit{quadrat{=}2}(x)$ die Prädikat "$x^2 = 2$" ist.

1.7 Beweisstrategien für Sätze mit Prädikaten

Die Gesetze der Aussagenlogik gelten fort, so dass sich prädikatenlogische Formeln entsprechend umformen lassen. Es ergeben sich jedoch zusätzliche Umformungs- und Schlussregeln, die beim Beweisen angewendet werden können. Alle diese Regeln sind Teil der sogenannten Prädikatenlogi, die wir in dieser Modul nur sehr informell diskutieren.

Beispielsweise lässt sich die Negation einer quantifizierten Formel eliminieren, indem man das Negationszeichen „nach innen zieht" und den Quantor „tauscht". Diese sind unendliche Verallgemeinerungen von den De-Morgan-Gesetzen.

Weitere äquivalente Formeln		Bezeichnung
$\neg\forall x\, F$	$\exists x\, \neg F$	Negation Allquantor
$\neg\exists x\, F$	$\forall x\, \neg F$	Negation Existenzquantor

Beispiel 1.7.1. *Die Aussage "Es gibt eine natürliche Zahl n, die nicht durch 7 teilbar ist" und die Aussage "Es ist nicht wahr, dass jede natürliche Zahl durch 7 teilbar ist" sind äquivalent. Die Formalisierungen lauten jeweils $\exists n P(n)$ und $\neg\forall n P(n)$, wobei $P(n)$ die Aussage $7 \mid n$ ist.*

Außerdem benötigen wir Strategien zum Beweisen quantifizierter Formeln, die wir kurz zusammenfassen und anschließend an konkreten Beispielen illustrieren:

- Strategie für den Allquantor $\forall x\, F$
  1. Man nehme ein beliebiges abstraktes Element u des Universums an. Als Variable hat u genau die Eigenschaften, die alle Elemente des Universums gemein haben.
  2. Man zeige F für u als Belegung von x.
- Strategie für den Existenzquantor $\exists x\, F$
  1. Man wähle ein geeignetes konkretes Element u des Universums. Da u konkret ist, können Eigenschaften von u genutzt werden.
  2. Man zeige F für u als Belegung von x.

Beispiel 1.7.2. *Für jede natürliche Zahl existiert eine echt größere gerade natürliche Zahl.*

Formalisierung für das Universum natürlicher Zahlen:

$$\forall n\, \exists m \Big(\mathit{Gerade}(m) \wedge (m > n) \Big)$$

> *Beweisversuch.* Sei n eine beliebige natürliche Zahl. (Elimination Allquantor)
>
> Wir wählen $m = 2n$. (Elimination Existenzquantor)
>
> Dann ist m offenbar durch 2 teilbar und damit gerade. (Eigenschaft m)
>
> Weiterhin sei $n > 0$, woraus $m - n = 2n - n = n > 0$ und damit $m > n$ folgen. □

Der Beweis ist falsch, denn die Annahme einer zusätzlichen Eigenschaft von n, d.h. $n > 0$, ist nicht zulässig. Wir geben zwei korrekte Beweisvarianten an.

Beweis. Sei n eine beliebige natürliche Zahl.

Wir wählen $m = 2(n + 1)$.

Dann ist m offenbar durch 2 teilbar und damit gerade.

Weiterhin gilt $m - n = 2(n + 1) - n = n + 2 > 0$ und damit ist $m > n$. □

Beweis. Sei n eine beliebige natürliche Zahl. (Elimination Allquantor)

Dann ist n entweder gerade oder ungerade. (Eigenschaft aller natürlichen Zahlen)

- Sei n gerade. Wir wählen $m = n + 2$. (Elimination Existenzquantor)
  Dann ist m offenbar auch gerade und es gilt $m > n$.
- Sei n ungerade. Wir wählen $m = n + 1$. (Elimination Existenzquantor)
  Dann ist m gerade und $m > n$.

Wir haben die Aussage in beiden Fällen gezeigt. □

Kapitel 2

Naive Mengenlehre

Wir beginnen mit einer "naiven"Definition des Begriffs 'Menge'. Diese Definition erfasst sehr gut unsere Intuition was Mengen sein sollen, und wir werden sie als Ausgangspunkt nutzen. Es ist allerdings zu beachten, dass diese Definition präzisiert werden müsste, um den Normen der modernen Mathematik zu genügen.

Definition 2.0.1 (Georg Cantor 1895)**.** Eine Menge M ist eine Zusammenfassung von unterscheidbaren Objekten zu einem Ganzen. Die zusammengefassten Objekte heißen Elemente von M.

Die folgenden Eigenschaften sind zu beobachten. .

(a) Für eine Menge M ist jedes Objekt x entweder ein Element von M (kurz $x \in M$) oder nicht (kurz $x \notin M$).

(b) Insbesondere kann ein Element nicht mehrfach in einer Menge enthalten sein.

(c) Die Elemente einer Menge können unterschiedlichen Typs und sogar selbst wieder Mengen sein.

(d) Die Element einer Menge haben keine Anordnung; ihre Reihenfolge ist irrelevant.

(e) Außerdem gilt: Jede Menge ist unterscheidbar von jedem ihrer Elemente, auch wenn Sie genau ein Element enthält (in mathematischer Notation z.B. $\{3\} \neq 3$).

Beispiele 2.0.2.

- *Lkw sei die Menge aller Lastkraftwagen.*
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *bezeichnen jeweils die Mengen aller natürlichen Zahlen, aller ganzen Zahlen, aller rationalen Zahlen und aller reellen Zahlen. In diesem Modul wird angenommen, dass* $0 \in \mathbb{N}$.
- *Vollständige oder unvollständige Aufzählung:* $\{1, 2, 3\}$ *bzw.* $\{0, 1, 2, \ldots\}$

  Das Muster muss klar erkennbar sein.

- $\{1, 2, 3\} = \{1, 2, 3, 2\} = \{2, 3, 1\}$,
- *Leere Menge:* $\emptyset$ *enthält keine Elemente.*
- $\{\emptyset\}$ *ist die Menge mit genau einem Element. Dieses Element is die leere Menge.*

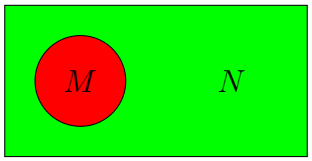
Wir verkürzen "$x \in M$ und $y \in M$" einfach zu "$x, y \in M$". Man beachte, dass wenn wir $x, y, z \in \{1, 2, 3\}$ schreiben, durchaus $x = y = z$ gelten kann!

Zwei Mengen M und N sind gleich, kurz $M = N$, wenn sie genau die gleichen Elemente enthalten.

Bemerkung 2.0.3. Insbesondere gibt es genau eine Menge die enthält keine Elemente, mämlich $\emptyset$.

Eine Menge M ist eine Teilmenge von der Menge N, kurz $M \subseteq N$, falls jedes Element von M auch Element von N ist. Formal:

$$M = N \text{ gdw. } \forall m\big((m \in M) \to (m \in N)\big) \wedge \forall n\big((n \in N) \to (n \in M)\big),$$
$$M \subseteq N \text{ gdw. } \forall m\big((m \in M) \to (m \in N)\big).$$



Man schreibt gelegentlich auch $N \supseteq M$ (anstelle $M \subseteq N$) und nennt N Obermenge von M. Wir sprechen von einer echten Teilmenge und schreiben $M \subsetneq N$, falls $M \subseteq N$ und $M \neq N$. Alternativ nennt man Gleichheits- und Teilmengenbeziehung auch Identität und Inklusion. Es gilt der folgende naheliegende Zusammenhang.

Satz 2.0.4. *Für alle Mengen M und N gilt: $M = N$ gdw. $M \subseteq N$ und $N \subseteq M$.*

Beweis. Durch Einsetzen der Definitionen:

$$\begin{aligned} & M = N \\ \text{ist äq. zu} \quad & \forall m\big((m \in M) \to (m \in N)\big) \wedge \forall n\big((n \in N) \to (n \in M)\big) \\ \text{ist äq. zu} \quad & (M \subseteq N) \wedge \forall n\big((n \in N) \to (n \in M)\big) \\ \text{ist äq. zu} \quad & (M \subseteq N) \wedge (N \subseteq M) \end{aligned}$$

□

2.1 Mengen und einstellige Prädikaten

Die einstelligen Prädikaten sind die Prädikaten der Form $P(x)$, die sagen ob eine spezielle Eigenschaft P für ein geg. Objekt x vorliegt. Derartige Atome (z.B. GanzeZahl(x), Gerade(x), Rat(x)) haben wir bereits intensiv in Kapitel 1 verwendet.

Die Verbindung zwischen Mengen und einstelligen Prädikaten ist einfach hergestellt. Ein Prädikat P legt für jedes Objekt x fest, ob das Atom $P(x)$ wahr oder falsch ist. Wir können die Objekte, für die $P(x)$ wahr ist, in einer Menge zusammenfassen.

Beispiele 2.1.1.

- $\{L \in \mathit{Lkw} \mid \mathit{hatFisch}(L)\}$

  Die Menge enthält genau die Elemente L von Lkw, für die hatFisch(L) wahr ist.

- $\{n \in \mathbb{N} \mid \mathit{Gerade}(n)\} = \{n \in \mathbb{N} \mid n \textit{ durch 2 teilbar}\} = \{n \in \mathbb{N} \mid \exists h(h \in \mathbb{N} \wedge n = 2h)\}$

  und $\{n \in \mathbb{N} \mid \mathit{Gerade}(n)\} \subseteq \{n \in \mathbb{N} \mid n \textit{ ist durch 2 teilbar}\}$,

- $\{n \in \mathbb{N} \mid n \textit{ ist durch 4 teilbar}\} \subseteq \{n \in \mathbb{N} \mid \mathit{Gerade}(n)\}$,

- $\emptyset \subseteq M$ *und* $M \subseteq M$ *für jede Menge* M,

- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

Bemerkung 2.1.2. Manchmal verwenden wir informell andere Methoden zur Definition von Mengen, die der obigen Methode mit Prädikaten ähneln, aber bei näherer Betrachtung anders sind. Hier sind zwei Beispiele:

(a) $\mathbb{Q} = \{\frac{m}{n} \mid m \in \mathbb{Z},\ n \in \mathbb{N},\ n \neq 0,\ m \text{ und } n \text{ teilerfremd}\}$

Bei der Mengennotation bedeutet das Zeichen ',' immer "und".

(b) $\{a + b \in \mathbb{R} \colon a \in \mathbb{Q}, b \in \{\sqrt{2}, \sqrt{3}\}\}$. Wenn wir es ganz formal schreiben wollen, würden wir schreiben $\{x \in \mathbb{R} \colon \exists a \in \mathbb{Q}, b \in \{\sqrt{2}, \sqrt{3}\}$ so dass $x = a + b\}$.

2.2 Operationen auf Mengen

Mit Hilfe der Junktoren der Logik lassen sich Operationen definieren, die aus zwei gegebenen Mengen eine neue Menge bilden. Seien M und N Mengen. Die Vereinigung von M und N besteht aus den Elementen, die Element von M oder Element von N sind:

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

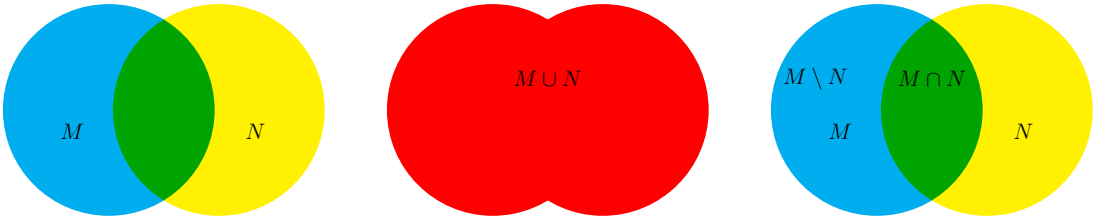
Der Schnitt von M und N besteht aus den Elementen, die Element von M und von N sind:

$$M \cap N = \{x \mid x \in M,\ x \in N\} = \{x \in M \mid x \in N\}.$$

Die Differenz von M ohne N besteht aus den Elementen, die Element von M, aber nicht Element von N sind:

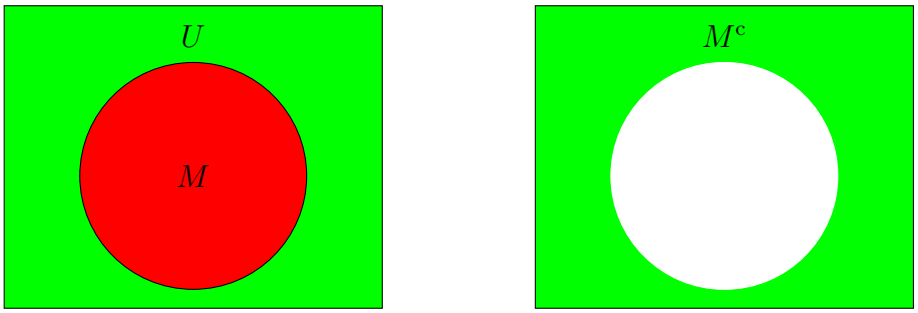
$$M \setminus N = \{x \mid x \in M,\ x \notin N\} = \{x \in M \mid x \notin N\}.$$

Venn-Diagramme illustrieren diesen Sachverhalt.



Im Kontext von Mengenoperationen gehen wir oft von einer Grundmenge U aus, in der alle betrachteten Mengen enthalten sind. Jede Menge M teilt U implizit in zwei Teile. Das Komplement von $M \subseteq U$ beinhaltet genau die Elemente von U, die nicht Elemente von M sind:

$$M^{\mathrm{c}} = \{u \in U \mid u \notin M\} = U \setminus M.$$



Basierend auf den Mengenoperationen ergeben sich viele verschiedene Möglichkeiten, komplexe Mengen aus einfacheren Mengen zu konstruieren. Gleichzeitig ergeben sich zahlreiche Rechenregeln (siehe Tabelle), die stark an die Regeln der Logik erinnern. So rechtfertigt das Assoziativgesetz beispielsweise das Weglassen von Klammern in mehrstelligen Vereinigungen und Schnitten wie $A \cup (B \cup C)$, so dass wir einfach $A \cup B \cup C$ schreiben.

Gleiche Mengen		Bezeichnung
$A \cap B$	$B \cap A$	Kommutativität von $\cap$
$A \cup B$	$B \cup A$	Kommutativität von $\cup$
$(A \cap B) \cap C$	$A \cap (B \cap C)$	Assoziativität von $\cap$
$(A \cup B) \cup C$	$A \cup (B \cup C)$	Assoziativität von $\cup$
$A \cap (B \cup C)$	$(A \cap B) \cup (A \cap C)$	Distributivität von $\cap$
$A \cup (B \cap C)$	$(A \cup B) \cap (A \cup C)$	Distributivität von $\cup$
$A \cap A$	A	Idempotenz von $\cap$
$A \cup A$	A	Idempotenz von $\cup$
$(A^{\mathrm{c}})^{\mathrm{c}}$	A	Involution $\cdot^{\mathrm{c}}$
$(A \cap B)^{\mathrm{c}}$	$A^{\mathrm{c}} \cup B^{\mathrm{c}}$	De-Morgan-Gesetz für $\cap$
$(A \cup B)^{\mathrm{c}}$	$A^{\mathrm{c}} \cap B^{\mathrm{c}}$	De-Morgan-Gesetz für $\cup$

Zur Verdeutlichung der Beweistechniken zeigen wir zunächst die Distributivität von $\cup$ und führen im Anschluss einen weiteren Identitätsbeweis, bei dem wir bereits auf die neu etablierten Rechenregeln zurückgreifen.

Beweis (Distributivität). Durch Anwendung der Definitionen erhalten wir:

$$\begin{aligned}
M \cup (N \cap P) &= \{x \mid (x \in M) \vee (x \in N \cap P)\} \\
&= \{x \mid (x \in M) \vee (x \in \{y \mid (y \in N) \wedge (y \in P)\})\} \\
&= \{x \mid \underbrace{(x \in M)}_{A} \vee (\underbrace{(x \in N)}_{B} \wedge \underbrace{(x \in P)}_{C})\} \\
&= \{x \mid (\underbrace{(x \in M)}_{A} \vee \underbrace{(x \in N)}_{B}) \wedge (\underbrace{(x \in M)}_{A} \vee \underbrace{(x \in P)}_{C})\} \\
&= \{x \mid (x \in M \cup N) \wedge (x \in M \cup P)\} \\
&= (M \cup N) \cap (M \cup P)
\end{aligned}$$

□

Bemerkung 2.2.1. Ein aufmerksamer Leser wird feststellen, dass wir die Tautologie $(A \wedge (B \vee C) = (A \vee B) \wedge (A \vee C)$ auf Prädikate und nicht auf atomare Formeln angewendet haben, d.h. $\forall x P(x) \wedge (Q(x) \vee R(x)) = \forall x (P(x) \vee Q(x)) \wedge P(x) \vee R(x))$. Dies ist zumindest intuitiv klar, denn es entspricht der Anwendung der aussagelogischen Tautologie "für jedes x", um die entsprechende prädikatenlogische Tautologie zu erhalten. In diesem Kurs rechtfertigen wir diesen Übergang nicht weiter und begnügen uns mit dieser informellen Rechtfertigung (sonst müsste man mehr formal die Prädikatlogik einführen).

Entsprechende Aussagen gelten für alle anderen Tautologien der Aussagenlogik.

Beispiel 2.2.2. *Seien M, N und U Mengen, so dass $M \subseteq U$ und $N \subseteq U$. Dann gilt*

$$M \setminus N = (M^c \cup N)^c.$$

Beweis.

$$\begin{aligned}
(M^{\mathrm{c}} \cup N)^{\mathrm{c}} &= (M^{\mathrm{c}})^{\mathrm{c}} \cap N^{\mathrm{c}} && \text{(De Morgan)} \\
&= M \cap N^{\mathrm{c}} && \text{(Involution)} \\
&= \{x \mid (x \in M) \wedge (x \in N^{\mathrm{c}})\} \\
&= \{x \mid (x \in M) \wedge (x \notin N)\} \\
&= M \setminus N.
\end{aligned}$$

□

Die Übersicht der wichtigen Tautologien aus Kapitel 1 liefert uns weitere Eigenschaften von Mengen. Unter Annahme einer Grundmenge U gilt:

Eigenschaft	Bezeichnung
$A \cup A^c = U$	Ausgeschlossenes Drittes
$((A \subseteq B) \wedge (B \subseteq C)) \to (A \subseteq C)$	Transitivität von $\subseteq$
$(A \subseteq B)$ gdw. $(B^c \subseteq A^c)$	Kontraposition
$(A \cap B) \subseteq A$	Abschwächung für $\cap$
$A \subseteq (A \cup B)$	Abschwächung für $\cup$

Beispiel 2.2.3. *Um die Eigenschaft* $((A \subseteq B) \wedge (B \subseteq C)) \to (A \subseteq C)$ *zu beweisen, definieren wir 3 Prädikate* $P(X) : x \in A$, $Q(x) : x \in B$, $R(x) : x \in C$. *Dann ist die Aussage* $A \subseteq B$ *äquivalent der Aussage* $\forall x P(x) \to Q(x)$ *usw, also die zubeweisende Eienschaft lautet*

$$\forall x((P(x) \to Q(x)) \wedge Q(x) \to R(x))) \to (P(x) \to R(x)).$$

Diese Eigenschaft stimmt, da es ist die prädikatlogische Variante der Tautologie $((X \to Y) \wedge (Y \to Z)) \to (X \to Z)$.

2.3 Eigenschaften der Teilmengenbeziehung

Wir sind an Zusammenhängen zwischen der Teilmengenbeziehung und den Mengenoperationen interessiert. Vom Bereich der Zahlen kennen wir folgende Monotonieeigenschaft: Zwei gleichsinnige Ungleichungen lassen sich miteinander addieren, ohne die Ungleichheit zu verlieren. Ein ganz analoger Zusammenhang gilt auch für Mengen.

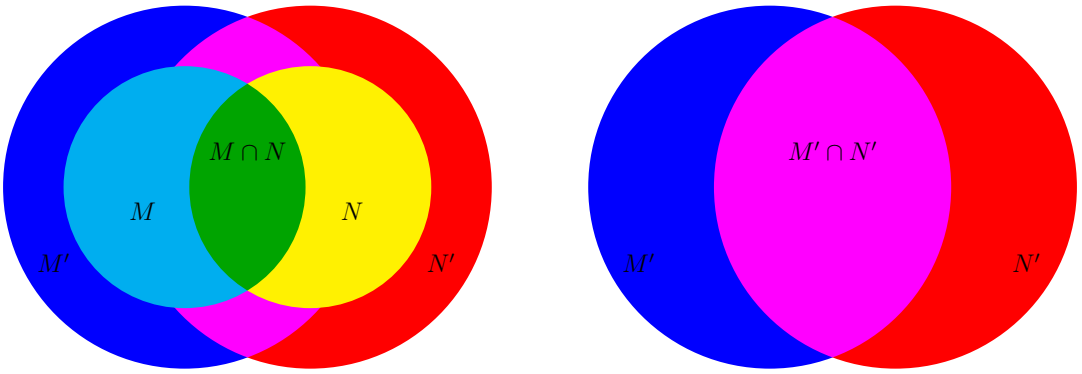
Satz 2.3.1 (Monotonie von $\subseteq$)**.** *Seien* $M \subseteq M'$ *und* $N \subseteq N'$. *Dann gelten*

$$(M \cap N) \subseteq (M' \cap N') \qquad \textit{und} \qquad (M \cup N) \subseteq (M' \cup N')$$

Beweis. Wir beweisen beide Inklusionen.

Zu $(M \cap N) \subseteq (M' \cap N')$: Sei $x \in (M \cap N)$. Dann $x \in M$ und $x \in N$.
Da $M \subseteq M'$ und $N \subseteq N'$ folgen $x \in M'$ und $x \in N'$. Folglich $x \in (M' \cap N')$.

Zu $(M \cup N) \subseteq (M' \cup N')$: Sei $x \in (M \cup N)$. Dann $x \in M$ oder $x \in N$.
Da $M \subseteq M'$ und $N \subseteq N'$ folgt $x \in M'$ oder $x \in N'$. Folglich $x \in (M' \cup N')$. □



Eine weitere Form des Zusammenhangs besteht in der Charakterisierung ein und desselben Sachverhalts aus verschiedenen Perspektiven. So lässt sich die Teilmengenbeziehung auch operational beschreiben.

Satz 2.3.2. *Für alle Mengen M und N sind folgende Aussagen äquivalent:*

1. $M \subseteq N$
2. $M \cap N = M$
3. $M \cup N = N$

Beweis. Wir zeigen die Äquivalenz von (2) und (3) zu (1). Die Äquivalenz von (2) und (3) folgt!

Zu (1) → (2) und (1) → (3): Da $M \subseteq N$ folgt durch Monotonie

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

Trivialerweise gelten $M \cap N \subseteq M$ und $N \subseteq M \cup N$.

Zu (2) → (1) und (3) → (1): Mit Abschwächung gelten

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

2.4 Verallgemeinerung von Vereinigung und Schnitt

Wir haben Vereinigung und Schnitt bisher zweistellig definiert. Analog zum Summenzeichen $\sum$ verallgemeinern wir die Definition auf beliebig viele Argumente. Sei I eine Menge und M_i eine Menge für jedes $i \in I$. Wir definieren

$$\begin{aligned}\bigcup_{i\in I} M_i &= \{x \mid \text{es existiert } i \in I, \text{ so dass } x \in M_i\} \\ &= \big\{x \mid \exists i\big((i \in I) \wedge (x \in M_i)\big)\big\} \text{ und}\end{aligned}$$

$$\begin{aligned}\bigcap_{i\in I} M_i &= \{x \mid \text{für alle } i \in I \text{ gilt } x \in M_i\} \\ &= \big\{x \mid \forall i\big((i \in I) \to (x \in M_i)\big)\big\}\end{aligned}$$

und fixieren für die Sonderfälle (für $I = \emptyset$)

$$\bigcup_{i\in\emptyset} M_i = \emptyset,$$
$$\bigcap_{i\in\emptyset} M_i = U \text{ für Grundmenge } U, \text{ sonst undefiniert.}$$

Beispiele 2.4.1.

- *Für jede Menge M gilt $M = \bigcup_{m\in M}\{m\}$.*
- *Das geschlossene Interval $[u, o]$ für $u, o \in \mathbb{R}$ mit $u \leq o$ ist definiert durch*

$$[u, o] = \{r \in \mathbb{R} \mid u \leq r \leq o\}.$$

- *Sei $r \in \mathbb{R}_{\geq 0}$ eine reelle Zahl. Dann ist*

$$\bigcap_{\substack{x\in\mathbb{R}_{\geq 0}\\ r\in[-x,x]}} [-x, x] = [-r, r].$$

- *Es gilt $\mathbb{R} = \bigcup_{n\in\mathbb{N}}[-n, n] = \bigcup_{r\in\mathbb{R}_{\geq 0}}[-r, r]$.*

Wir beweisen das letzte Beispiel zur Illustration des Beweisprinzips Ringinklusion.

Beweis. Wir zeigen $\mathbb{R} \subseteq \bigcup_{n\in\mathbb{N}}[-n, n] \subseteq \bigcup_{r\in\mathbb{R}_{\geq 0}}[-r, r] \subseteq \mathbb{R}$.

Zu $\mathbb{R} \subseteq \bigcup_{n\in\mathbb{N}}[-n, n]$: Sei $r \in \mathbb{R}$ und $n = \lceil |r| \rceil$ (aufrunden). Dann gilt $-n \leq r \leq n$ und damit $r \in [-n, n]$. Also auch $r \in \bigcup_{n\in\mathbb{N}}[-n, n]$.

Zu $\bigcup_{n\in\mathbb{N}}[-n, n] \subseteq \bigcup_{r\in\mathbb{R}_{\geq 0}}[-r, r]$: Trivial, da $\mathbb{N} \subseteq \mathbb{R}_{\geq 0}$.

Zu $\bigcup_{r\in\mathbb{R}_{\geq 0}}[-r,r]\subseteq\mathbb{R}$: Es ist $[-r,r]\subseteq\mathbb{R}$ für alle $r\in\mathbb{R}_{\geq 0}$. □

Schließlich machen wir auf die folgenden Notationsvarianten aufmerksam.
Für $I=\{u,u+1,\ldots,o\}\subseteq\mathbb{N}$ schreiben wir auch

$$\bigcup_{i=u}^{o} M_i=\bigcup_{i\in I} M_i \qquad \text{und} \qquad \bigcap_{i=u}^{o} M_i=\bigcap_{i\in I} M_i.$$

Liegt eine Menge von Mengen vor, so lassen wir die Laufvariable auch ganz weg:

$$\bigcup\{M_i\mid i\in I\}=\bigcup_{i\in I} M_i \qquad \text{und} \qquad \bigcap\{M_i\mid i\in I\}=\bigcap_{i\in I} M_i.$$

Beispiele 2.4.2.

$$\bigcup\big\{\{1,3,5\},\{1,2,3\},\{2,3,5\}\big\}=\{1,2,3,5\}$$

$$\bigcap\big\{\{1,3,5\},\{1,2,3\},\{2,3,5\}\big\}=\{3\}$$

Die Rechenregeln für Mengen übertragen sich in naheliegender Weise auf die verallgemeinerten Operationen, wie die folgende Tabelle exemplarisch darstellt.

gleiche Mengen		Bezeichnung
$M\cap\left(\bigcup_{i\in I} M_i\right)$	$\bigcup_{i\in I}(M\cap M_i)$	Distributivität von $\cap$
$M\cup\left(\bigcap_{i\in I} M_i\right)$	$\bigcap_{i\in I}(M\cup M_i)$	Distributivität von $\cup$
$\bigcap_{i\in I} A$	A	Idempotenz von $\bigcap$; $I\neq\emptyset$
$\bigcup_{i\in I} A$	A	Idempotenz von $\bigcup$; $I\neq\emptyset$
$\left(\bigcap_{i\in I} M_i\right)^{\mathrm{c}}$	$\bigcup_{i\in I} M_i^{\mathrm{c}}$	De-Morgan-Gesetz für $\bigcap$
$\left(\bigcup_{i\in I} M_i\right)^{\mathrm{c}}$	$\bigcap_{i\in I} M_i^{\mathrm{c}}$	De-Morgan-Gesetz für $\bigcup$

2.5 Potenzmenge

Für eine Menge M ist die Potenzmenge $\mathcal{P}(M)$ die Menge

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

aller Teilmengen von M.

Beispiel 2.5.1. *Es gelten* $\mathcal{P}(\emptyset)=\{\emptyset\}$, $\mathcal{P}(\{\emptyset\})=\{\emptyset,\{\emptyset\}\}$ *und*

$$\mathcal{P}(\{1,2,3\})=\big\{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\big\}.$$

2.6 Naive Kardinalität

Intuitiv unterscheiden wir zwischen endlichen und unendlichen Mengen. Für endliche Mengen M bezeichnen wir mit $|M|$ die Anzahl ihrer Elemente. Ist M unendlich, so schreiben wir auch $|M| \geq \infty$.

Wie bestimmt sich die Anzahl der Elemente von Mengenverknüpfungen? Exemplarisch betrachten wir die Vereinigung.

Satz 2.6.1. *Für alle endlichen Mengen M und N gilt*

$$\max(|M|, |N|) \leq |M \cup N| \leq |M| + |N|.$$

Eine genauere Angabe können wir im Allgemeinen nicht treffen, da die Mengen M und N eine echte gemeinsame Schnittmenge haben könnten. Gilt aber

$$M \cap N = \emptyset,$$

so nennen wir M und N disjunkt und die Abschätzung wandelt sich zu

$$|M \cup N| = |M| + |N|.$$

Beispiele 2.6.2.

- *Die Mengen $\{1, 2, 3\}$ und $\{2, 4, 6\}$ sind nicht disjunkt und es gilt*

$$|\{1, 2, 3\} \cup \{2, 4, 6\}| = 5 < 6 = 3 + 3 = |\{1, 2, 3\}| + |\{2, 4, 6\}|.$$

- *Die Mengen $\{1, 2, 3\}$ und $\{4, 5, 6\}$ sind disjunkt und es gilt*

$$|\{1, 2, 3\} \cup \{4, 5, 6\}| = 6 = 3 + 3 = |\{1, 2, 3\}| + |\{4, 5, 6\}|.$$

Bemerkung 2.6.3. Wie viele Elemente enthält die Potenzmenge einer endlichen Menge M? Durch systematisches Probieren gelangt man zu der Hypothese

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

Der Grund dafür ist informell, dass die Definition einer Teilmenge S von M gleichbedeutend damit ist, für jedes x inM zu entscheiden, ob es in S enthalten ist oder nicht. Da es $2^{|M|}$ solche Auswahlmöglichkeiten gibt, ist dies auch die Anzahl der Teilmengen von M.

Für den präzisen Beweis benötigen wir jedoch eine neue Beweistechnik, “Induktion”, mit der wir uns in Kapitel 3 beschäftigen.

∎

Kapitel 3

Vollständige Induktion und Induktionsbeweise

Wir betrachten die folgende Aussage.

Beispiel 3.0.1. *Für alle $n \in \mathbb{N}$ gilt*

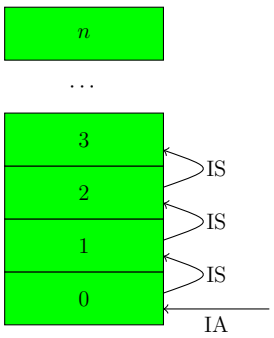
$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Obwohl der Beweis dieser Aussage für eine konkrete Zahl n unproblematisch ist, stellt der Beweis für alle $n \in \mathbb{N}$ eine Hürde dar, da wir nicht unendlich viele Beweise angeben können. Das folgende Prinzip liefert uns eine Strategie für dieses Problem.

Satz 3.0.2 (Prinzip der vollständigen Induktion)**.** *Sei $F(x)$ eine Aussagenschablone mit einer Variable x. Gelten die Aussagen*

- *Induktionsanfang (IA):* $F(0)$ *und*
- *Induktionsschritt (IS):* $F(n) \to F(n+1)$ *für alle* $n \in \mathbb{N}$,

dann gilt $F(x)$ für alle $x \in \mathbb{N}$.



Bemerkung 3.0.3. Obwohl wir das Prinzip der vollständigen Induktion oben als SSatz"beschrieben haben, wird dieses Prinzip normalerweise nicht bewiesen - es wird als eine der grundlegenden Eigenschaften der natürlichen Zahlen betrachtet und als Axiom als wahr angenommen.

Ein Induktionsbeweis funktioniert wie folgt. Zunächst zeigen wir die Behauptung für den Fall $n = 0$ (Induktionsanfang). Anschließend wählen wir eine beliebige natürliche Zahl n und setzen voraus, dass die Behauptung für n bereits gezeigt ist (Induktionshypothese). Dann zeigen wir die Behauptung für den Nachfolger $n + 1$ unter Rückgriff auf die Induktionshypothese (Induktionsschritt). So „erreichen“ wir alle natürlichen Zahlen durch einen einzigen Beweis.

Beweis. (Gaußsche Summenformel)

Induktionsanfang: Es gilt $\sum_{i=1}^{0} i = 0 = \frac{0 \cdot 1}{2}$.

Induktionshypothese: Sei $n \in \mathbb{N}$ und gelte $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Induktionsschritt: Zu zeigen: $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$. Es gilt

$$\begin{aligned}\sum_{i=1}^{n+1} i &= \sum_{i=1}^{n} i + (n+1) \\ &\overset{\text{IH}}{=} \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2} \quad .\end{aligned}$$

Nach dem Prinzip der vollständigen Induktion folgt die Behauptung. □

Kehren wir nun zu unserer Hypothese bezüglich der Potenzmenge aus Kapitel 2 zurück.

Satz 3.0.4. *Sei M eine endliche Menge. Dann gilt $|\mathcal{P}(M)| = 2^{|M|}$.*

Zunächst stellen wir fest, dass es bei dieser Aussage lediglich auf die Anzahl der Elemente von M ankommt und nicht auf das Wesen der Elemente. In diesem Sinne handelt es sich um eine universelle Aussage über die natürlichen Zahlen:

$$\forall n \forall M \left(|M| = n \to |\mathcal{P}(M)| = 2^n \right).$$

Beweis. (Vollständige Induktion über $n = |M|$)

IA: Sei Menge M beliebig mit $|M| = 0$. Die einzige solche Menge ist $M = \emptyset$. Zusätzlich $\mathcal{P}(\emptyset) = \{\emptyset\}$, also gilt $|\mathcal{P}(\emptyset)| = |\{\emptyset\}| = 1 = 2^0 = 2^{|\emptyset|}$.

IH: Sei $n \in \mathbb{N}$ und $|\mathcal{P}(N)| = 2^n$ für alle Mengen N mit $|N| = n$.

IS: Sei M Menge mit $|M| = n + 1$. Wähle $x \in M$ beliebig und sei $N = M \setminus \{x\}$.

Dann ist

$$\mathcal{P}(M) = \mathcal{P}(N) \cup \big\{S \cup \{x\} \mid S \in \mathcal{P}(N)\big\}.$$

(Aufteilung in Teilmengen $\mathcal{P}(N)$, die x nicht enthalten, und die Teilmengen, die x enthalten) Unter Beachtung der Disjunktheit gilt

$$|\mathcal{P}(M)| = |\mathcal{P}(N)| + |\mathcal{P}(N)| = 2 \cdot |\mathcal{P}(N)| \overset{\text{IH}}{=} 2 \cdot 2^n = 2^{n+1} = 2^{|M|} \ ,$$

wobei $|\mathcal{P}(N)| = 2^n$ per Induktionshypothese gilt. □

Bemerkung 3.0.5. Der Beginn der Induktion muss nicht bei $n = 0$ liegen. Betrachten wir zum Beispiel die Aussage, dass für alle $n \in NN$ mit $n > 2$ gilt: $n^2 > n + 5$.

Beweis. Induktionsanfang. Für $n = 3$ haben wir $n^2 = 9 > 9 = n + 5$.

Induktionshypothese. Sei $n > 2$ beliebig. Wir nehmen an, dass $n^2 > n + 5$.

Induktionsschritt. Wir haben $(n+1)^2 = n^2+2n+1 \overset{\text{IH}}{>} n+5+2n+1 > (n+1)+5$.
Nach dem Prinzip der vollständigen Induktion folgt die Behauptung. □

□

Kapitel 4

Relationen

Im letzten Kapitel haben wir unsere grundlegende Einführung in die Mengenlehre abgeschlossen. Alle mathematischen Strukturen können mit Hilfe von Mengen definiert werden.

> **Bemerkung 4.0.1.** Es sollte betont werden, dass wir, wenn wir über Strukturen wie Zahlen, Graphen von Funktionen usw. nachdenken, fast nie bis zu den Mengen zurückgehen. Dies ist sehr analog zu der Situation mit modernen Computern: Einerseits stimmt es, dass jeder Computer in seinem Kern 0/1-Variablen mit den Grundoperationen $\wedge$, $\vee$ und $\neg$ manipuliert. Wir brauchen uns damit aber nicht zu befassen wenn wir ein Dokument bearbeiten, im Internet surfen oder Musik auf dem Computer hören.

Die erste Struktur, die wir in diesem Kapitel einführen, ist ein geordnetes Paar: Gegeben zwei Objekte A und B, können wir das Paar (A, B) betrachten. Wir betonen die folgenden Unterschiede im Vergleich zur Menge $\{A, B\}$. 1) Wenn $A \neq B$, dann spielt die Reihenfolge eine Rolle, d.h. $(A, B) \neq (B, A)$, und 2) Wenn $A = B$, dann ist $\{A, B\} = \{A\}$, während nichts dergleichen für ein geordnetes Paar geschieht, z.B. können wir geordnete Paare $(2, 2)$, $(3, 3)$, $(\mathbb{R}, \mathbb{R})$, usw. betrachten.

> **Bemerkung 4.0.2.** Es gibt viele Möglichkeiten, geordnete Paare mit Hilfe von Mengen als Bausteinen zu definieren. Die populärste Definition ist das "Kuratowskis geordnetes Paar": Bei gegebenen Objekten A und B definieren wir das geordnete Paar (A, B) als die Menge $(A, B) := \{A, \{A, B\}$. Der Leser wird leicht feststellen, dass diese Definition die folgende Schlüsseleigenschaft erfüllt: $(A, B) = (C, D)$, genau dann, wenn $A = C$ und $B = D$. Es gibt auch andere mögliche mengentheoretische Definitionen, die diese Eigenschaft erfüllen. Wie in der letzten Bemerkung erläutert wurde, werden wir nie wieder die eigentliche Definition des geordneten Paares verwenden, nur diese Schlüsseleigenschaft ist wichtig. Die Analogie zur Informatik ist: Wenn wir im Internet surfen, ist es uns ziemlich egal, welchen Webbrowser wir benutzen und wie genau sein Quellcode aussieht, solange er uns den Zugriff auf die für uns wichtigen

Webdienste ermöglicht.

Da wir nun über geordnete Paare verfügen, können wir die karthesischen Produkte wie folgt definieren. Für alle Mengen M und N ist das kartesische Produkt $M \times N$ definiert durch

$$M \times N := \{(m,n) \mid m \in M,\, n \in N\} \ .$$

Also $M \times N$ ist die Menge aller geordneten Paare von einem Element m aus M gefolgt von einem Element n aus N. Wir betonen dass wenn $M \neq N$ dann auch $M \times N \neq N \times M$.

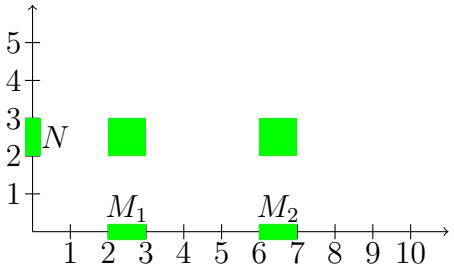
Beispiele 4.0.3.

- *Für* $M = \{1, 2, 3\}$ *und* $N = \{1, 3\}$ *ist*

$$M \times N = \{(1,1), (1,3), (2,1), (2,3), (3,1), (3,3)\}.$$

- *Seien* $M_1 = [2,3]$, $M_2 = [6,7]$ *und* $N = [2,3]$. *Dann ist*

$(M_1 \cup M_2) \times N =$



Die letzten Strukturen, die wir in diesem Kapitel betrachten, sind Relationen. Wir werden bald sehen, dass Relationen äußerst nützlich sind, um andere mathematische Strukturen zu definieren, sowie die Strukturen in der Welt um uns herum zu modellieren.

Eine Relation R von M nach N ist eine Teilmenge $R \subseteq M \times N$. Ist $M = N$, so heißt R auch Relation auf M. Zum Umgang mit Relationen sind verschiedene Schreibweisen gebräuchlich. Statt $(m,n) \in R$ schreiben wir auch $m \ R \ n$ oder $R(m,n)$ oder $m \sim_R n$. Analog $m \not R \ n$. Dabei legen wir fest, dass Relationszeichen stärker binden als die logischen Junktoren:

$$(x \sim y \ \wedge \ y \sim x) \ \rightarrow \ x = y \quad \text{heißt} \quad \big((x \sim y) \wedge (y \sim x)\big) \rightarrow (x = y).$$

Beispiele 4.0.4.

- *Die leere Relation* $\emptyset$ *und* $M \times N$ *selbst sind Relationen von* M *nach* N.
- *Sei* B *die Menge der Bundesbürger. Die Menge*

$$\{(p,n) \in B \times \mathbb{N} \mid p \text{ hat Identifikationsnummer } n\}$$

ist eine Relation von B nach $\mathbb{N}$.

- *Die Menge $\{(n, n') \in \mathbb{N} \times \mathbb{N} \mid n \leq n'\}$ ist eine Relation auf $\mathbb{N}$.*
- *Die Teilmengerelation $\subseteq$ ist eine Relation auf $\mathcal{P}(M)$.*
- *Die Freund-Relation auf der Menge F der Facebook-Nutzer*

$$\big\{(x, y) \in F \times F \mid x \text{ ist Facebook-Freund von } y\big\}$$

ist eine Relation.

- *Für jede Menge M ist die Identität $\mathrm{id}_M = \{(m, m) \mid m \in M\}$ eine Relation auf M. Gewöhnlich schreibt man $x = y$ statt $x \,\mathrm{id}_M\, y$.*

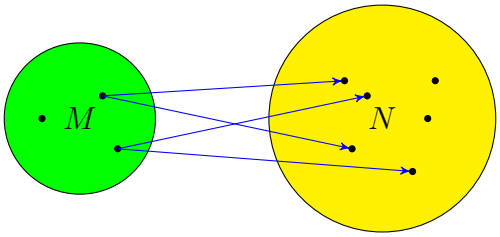


Abbildung 4.1: Relation von M nach N

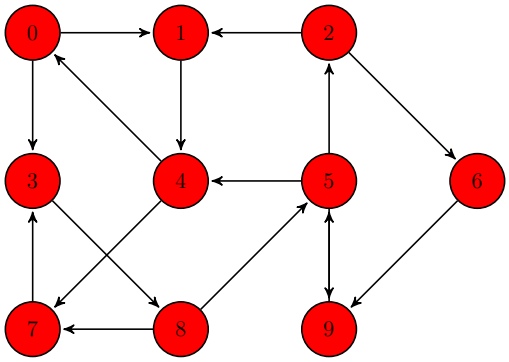


Abbildung 4.2: Relation auf $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Bemerkung 4.0.5. Wie wir in Beispielen oben sehen, häufig benutzen wir zweistelligen Prädikaten um Relationen zu definieren. Wir fassen die Paare, die in Beziehung stehen (also die Eigenschaft erfüllen), zu einer Menge zusammen und nennen diese Menge "Relation".

4.1 Eigenschaften von Relationen

Eine Relation $R \subseteq M \times M$ auf M heißt

- reflexiv, falls $\forall x(x \in M \to (x,x) \in R)$,
  (jedes Element x von M steht in Relation zu sich selbst)
  z. B. $=$ ist reflexiv, $<$ ist nicht reflexiv, $\subseteq$ ist reflexiv,

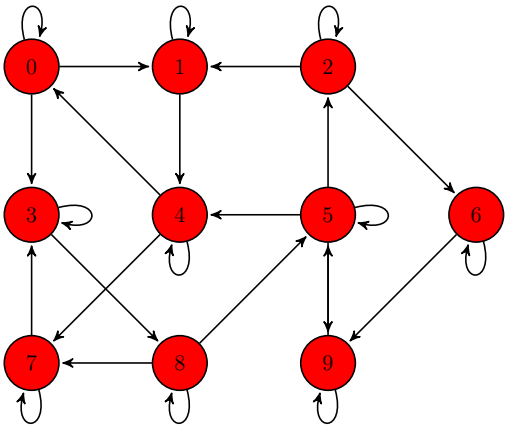
- irreflexiv, falls $\forall x(x \in M \to (x,x) \notin R)$,
  (kein Element x von M steht in Relation zu sich selbst)
  z.B. $<$ is irreflexiv

- symmetrisch, falls $\forall x, y\big((x,y) \in R \to (y,x) \in R\big)$,
  (falls x in Relation zu y steht, dann steht auch y in Relation zu x)
  z.B. $=$ is symmetrisch, Facebook-frenschaft ist symmetrisch.

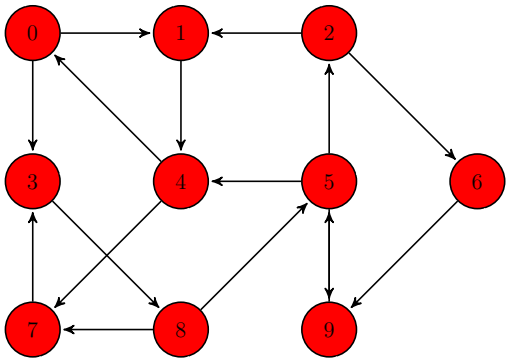
- antisymmetrisch, falls $\forall x, y\Big(\big((x,y) \in R \wedge (y,x) \in R\big) \to x = y\Big)$,
  (falls sowohl x zu y und y zu x in Relation stehen, dann sind x und y gleich)
  z.B. $\leq$ and $\subseteq$ sind antisymmetrisch.

- transitiv, falls $\forall x, y, z\Big(\big((x,y) \in R \wedge (y,z) \in R\big) \to (x,z) \in R\Big)$,
  (falls x zu y und y zu z in Relation stehen, dann steht auch x in Relation zu z)
  z.B.$<$ und $\leq$ sind tarnsitive

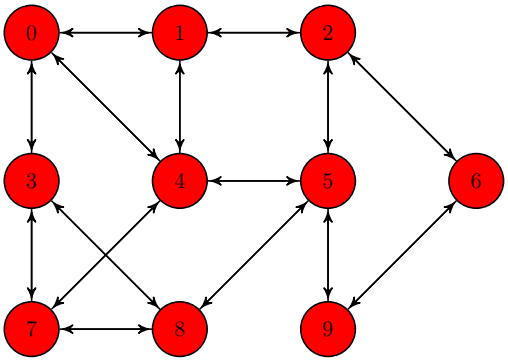
- vollständig, falls $\forall x, y\Big((x \in M \wedge y \in M) \to \big((x,y) \in R \vee (y,x) \in R\big)\Big)$.
  (für alle Elemente $x, y \in M$ steht x in Relation zu y oder y in Relation zu x)
  z.B. $\leq$ ist vollständig



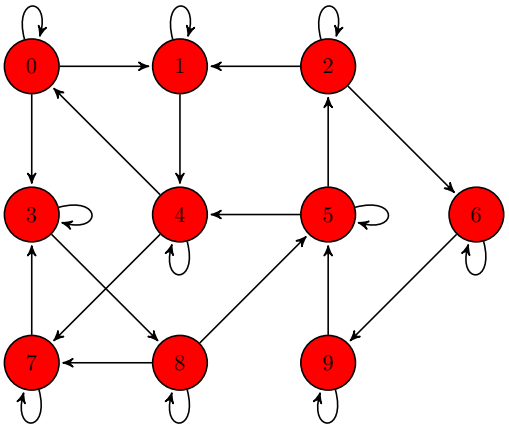
Reflexivität: Alle Elemente haben Schleifen.



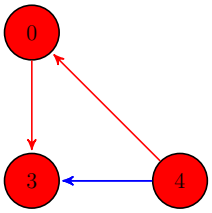
Irreflexivität: Kein Element hat Schleifen.



Symmetrie: Jeder Pfeil ist beidseitig.



Antisymmetrie: Kein Pfeil ist beidseitig, mit Ausnahme von Schleifen.



Transitivität: Für jeden Weg existiert auch der direkte Weg.

Eigenschaft \ Relation	$\emptyset$	$\leq$	$=$	$\subseteq$
reflexiv	✗	✓	✓	✓
irreflexiv	✓	✗	✗	✗
symmetrisch	✓	✗	✓	✗
antisymmetrisch	✓	✓	✓	✓
transitiv	✓	✓	✓	✓
vollständig	✗	✓	✗	✗

Bemerkung 4.1.1. In der obigen Tabelle haben wir markiert, dass die leere Relation nicht reflexiv ist. Das ist richtig, außer wenn die Menge, auf der wir die Relation definieren, leer ist. Dies ist ein nicht besonders interessanter Fall, und deshalb von nun an in diesem Kapitel wir nur noch Relationen auf nicht leeren Mengen betrachten, auch wenn wir dass nicht explizit schreiben.

4.2 Operationen auf Relationen

Wir haben Relationen augenscheinlich als spezielle Mengen definiert, also sind alle Mengenoperationen auch auf Relationen anwendbar. Darüber hinaus legt die speziellere Struktur von Relationen zusätzliche Operationen nahe. Sei $R \subseteq M \times N$ eine Relation. Die inverse Relation R^{-1} von R ist definiert durch

$$R^{-1} = \{(n, m) \in N \times M \mid (m, n) \in R\}.$$

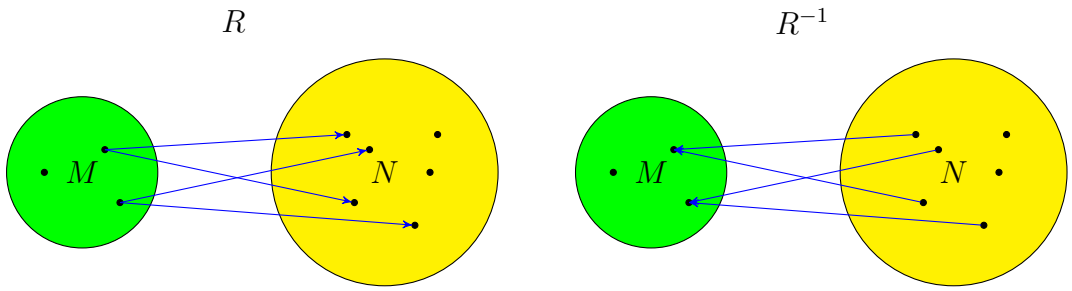
Die Inversion bewirkt also einen Tausch der Komponenten bzw. eine Umkehr der Pfeile.

Beispiele 4.2.1.

- *Sei* $R = \{(1,1), (1,3), (2,2), (2,4), (3,2)\}$. *Dann ist*

$$R^{-1} = \{(1,1), (3,1), (2,2), (4,2), (2,3)\}.$$

- *Die inverse Relation von $<$ ist $>$.*



Seien $R \subseteq M \times N$ und $R' \subseteq N \times P$ Relationen. Die Komposition von R gefolgt von R', geschrieben als $R\,;R'$, ist definiert durch

$$R\,;R' = \big\{(m,p) \in M \times P \mid \exists n\big(n \in N \wedge R(m,n) \wedge R'(n,p)\big)\big\}.$$

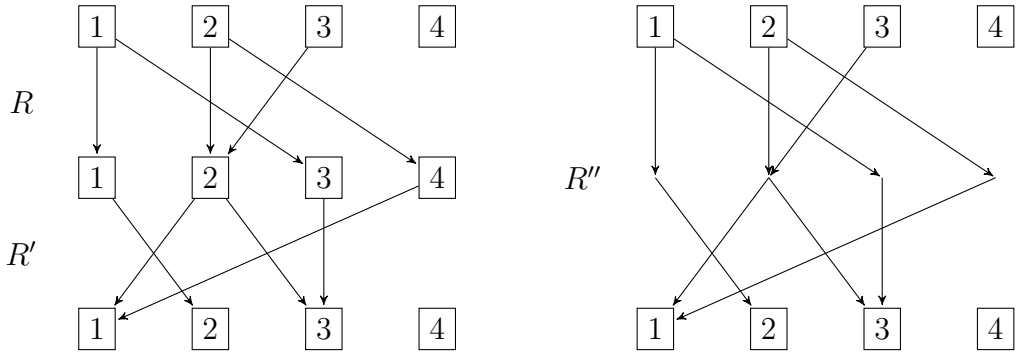
Die Komposition bewirkt die Verkettung und Auswahl von Paaren mit gleichem Mittelglied.

Beispiel 4.2.2. *Seien*

$$R = \{(1,1),\,(1,3),\,(2,2),\,(2,4),\,(3,2)\} \quad \textit{und} \quad R' = \{(1,2),\,(2,1),\,(2,3),\,(3,3),\,(4,1)\}.$$

Dann ist

$$R'' = R\,;R' = \{(1,2),\,(1,3),\,(2,1),\,(2,3),\,(3,1),\,(3,3)\}.$$



4.3 Äquivalenzrelationen

Oft ist es hilfreich eigentlich verschiedene Objekte nicht länger zu unterscheiden. In einer Zusammenfassung von Objekten mit verschiedenen Farben und Formen stellt man evtl. fest, dass die Farbe für die folgenden Betrachtungen irrelevant ist und man daher Objekte gleicher Form (aber potentiell verschiedener Farbe) nicht länger unterscheiden möchte. Derartige, potentiell ungleiche Objekte bezeichnet man dann als äquivalent bezüglich einer Äquivalenzrelation, die genau die Paare der neuerdings ununterscheidbaren Objekte enthält.

Tatsächlich haben wir diesen Ansatz bereits in der Logik verwendet und Formeln als äquivalent bezeichnet, falls sie die gleiche Aussage repräsentieren. Ob wir eine oder andere, doch äquivalente, Aussage wählen ist letztlich nicht entscheidend, denn wir sind typischerweise an Eigenschaften der Aussage (entscheidbar, tautologisch, etc.) und nicht an Eigenschaften der Formel (Anzahl der Negationen, etc.) interessiert. Insofern waren äquivalente Formeln beliebig füreinander austauschbar und ununterscheidbar.

Im Folgenden sind Eigenschaften aufgeführt, die wir unbedingt von Ununterscheidbaren Objekten verlangen.

- Jedes Objekt a ist ununterscheidbar von a selbst. (reflexiv)

- Wenn a ununterscheidbar von b ist, dann ist auch b ununterscheidbar von a. (symmetrisch)

- Wenn a ununterscheidbar von b und b wiederum ununterscheidbar von c ist, dann ist auch a ununterscheidbar von c. (transitiv)

Eine Relation $\equiv$ auf M ist eine Äquivalenzrelation, falls sie reflexiv, symmetrisch und transitiv ist. Für $m \in M$ beliebig ist

$$[m]_{\equiv} = \{x \in M \mid m \equiv x\}$$

die Äquivalenzklasse von m, (oder die $\equiv$-Äquivalenzklasse von m). Wir sagen auch dass m ein Vertreter oder Repräsentant von $[m]_{\equiv}$ ist. Sofern $\equiv$ sich aus dem Kontext ergibt, schreiben wir einfach $[m]$ statt $[m]_{\equiv}$.

Beispiele 4.3.1.

- *Die Identität ist stets eine Äquivalenzrelation. Keine Äquivalenzrelationen sind die natürliche Ordnung $\leq$ auf $\mathbb{N}$ und die Inklusion $\subseteq$ auf $\mathcal{P}(M)$ mit $M \neq \emptyset$.*

Eigenschaft \ *Relation*	$\emptyset$	$\leq$	$=$	$\subseteq$
reflexiv	✗	✓	✓	✓
irreflexiv	✓	✗	✗	✗
symmetrisch	✓	✗	✓	✗
antisymmetrisch	✓	✓	✓	✓
transitiv	✓	✓	✓	✓
vollständig	✗	✓	✗	✗

- *Die Relation $R_2 = \{(n, n') \in \mathbb{N}\times\mathbb{N} \mid n + n'$ ist gerade$\}$ ist eine Äquivalenzrelation.*

  Beweis.

  – Reflexivität: Für alle $x \in \mathbb{N}$ ist $x + x = 2x$ gerade, also $(x, x) \in R_2$.

  – Symmetrie: Seien $x, y \in \mathbb{N}$, so dass $(x, y) \in R_2$.
  Damit ist $x + y = y + x$ gerade, womit auch $(y, x) \in R_2$ gilt.

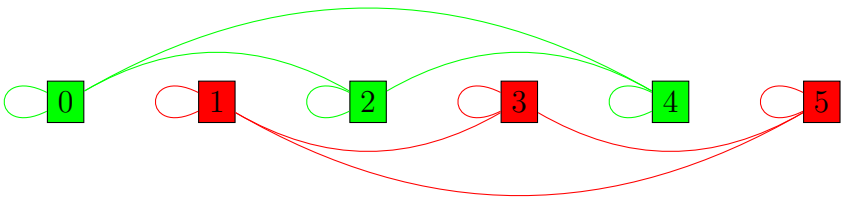
  – Transitivität: Seien $x, y, z \in \mathbb{N}$, so dass $(x, y) \in R_2$ und $(y, z) \in R_2$.
  Daher sind $x+y$ und $y+z$ gerade; d. h. es existieren $k, \ell \in \mathbb{N}$, so dass $x + y = 2k$ und $y + z = 2\ell$. Also

  $$x + z = (2k - y) + (2\ell - y) = 2k + 2\ell - 2y = 2(k + \ell - y),$$

  womit auch $x + z$ gerade ist und daher $(x, z) \in R_2$. □

Wie sieht R_2 aus? Die Zahl 0 steht zu allen geraden Zahlen in Relation und die Zahl 1 steht zu allen ungeraden Zahlen in Relation. Insgesamt ergibt sich:

$$[0]_{R_2} = \{0, 2, 4, 6, \ldots\} \quad \text{und} \quad [1]_{R_2} = \{1, 3, 5, 7, \ldots\}$$
$$[2]_{R_2} = \{0, 2, 4, 6, \ldots\} \quad \text{und} \quad [3]_{R_2} = \{1, 3, 5, 7, \ldots\}$$



Die Relation R_2 unterscheidet die Zahlen also in gerade und ungerade. Wir halten fest:

Für jede Äquivalenzrelation $\equiv$ auf einer Menge M und Elemente $x, y \in M$ gilt

$$x \equiv y \iff [x] = [y] \ .$$

Beweis.

($\to$) Sei $x \equiv y$. Zu zeigen $[x] = [y]$. Wir zeigen beidseitig die Teilmengenbeziehung.

($\subseteq$) Sei $z \in [x]$. Dann gilt $x \equiv z$. Mit Symmetrie folgt aus $x \equiv y$ auch $y \equiv x$ und vermittels Transitivität gilt damit $y \equiv z$. Folglich $z \in [y]$.

($\supseteq$) Sei $z \in [y]$. Dann gilt $y \equiv z$. Vermittels Transitivität gilt damit $x \equiv z$. Folglich $z \in [x]$.

($\leftarrow$) Sei $[x] = [y]$. Gemäß Reflexivität gilt $y \in [y] = [x]$, also $x \equiv y$. □

Sei $\equiv$ eine Äquivalenzrelation auf M. Die Menge

$$(M/\equiv) = \{[m]_\equiv \mid m \in M\}$$

aller Äquivalenzklassen von $\equiv$ wird auch Quotient von M via $\equiv$ genannt.

Beispiele 4.3.2.

$(\mathbb{N}/=) = \big\{\{0\}, \{1\}, \{2\}, \ldots\big\}$

$(\mathbb{N}/R_2) = \big\{\{0, 2, 4, 6, \ldots\}, \{1, 3, 5, 7, \ldots\}\big\}$

Wir beobachten: Die Äquivalenzrelationen $=$ und R_2 zerlegen die Menge $\mathbb{N}$ vollständig in Klassen. Unsere Beobachtung lässt sich auf alle Äquivalenzrelationen verallgemeinern. Sei M eine Menge. Eine Zerlegung von M ist eine Menge $\mathcal{N} \subseteq \mathcal{P}(M)$ mit den Eigenschaften

1. $\emptyset \notin \mathcal{N}$,
2. $M = \bigcup \mathcal{N}$,
3. $N \cap N' = \emptyset$ für alle $N, N' \in \mathcal{N}$ mit $N \neq N'$.

Satz 4.3.3. *Sei M eine nicht leere MEnge und sei $\equiv$ eine Äquivalenzrelation auf M. Dann ist $(M/\equiv)$ eine Zerlegung von M.*

Beweis. Sei $\mathcal{M} = (M/\equiv) = \{[m] \mid m \in M\}$. Offensichtlich ist $\mathcal{M} \subseteq \mathcal{P}(M)$.
Zu zeigen: Die Menge $\mathcal{M}$ erfüllt alle Eigenschaften einer Zerlegung.

1. Vermittels der Reflexivität von $\equiv$ gilt $m \in [m]$ und damit $[m] \neq \emptyset$ für jedes $m \in M$.
   Es folgt $\emptyset \notin \mathcal{M} = \{[m] \mid m \in M\}$.

2. Die Inklusion $\bigcup \mathcal{M} \subseteq M$ ist trivial.
   Umgekehrt gilt für jedes $m \in M$ auch $m \in [m] \subseteq \bigcup \mathcal{M}$, womit $M \subseteq \bigcup \mathcal{M}$.

3. (Kontraposition) Seien $M_1, M_2 \in \mathcal{M}$ mit $M_1 \cap M_2 \neq \emptyset$. Dann existiert $m \in M_1 \cap M_2$. Für jedes $x \in M_1$ gilt $m \equiv x$ und damit $x \in M_2$. Also $M_1 \subseteq M_2$. Ebenso $M_2 \subseteq M_1$ da $m \equiv y$ und $y \in M_1$ für alle $y \in M_2$. □

Tatsächlich erzeugt jede Zerlegung auch wieder eine Äquivalenzrelation. Es handelt sich also um stark korrespondierende Begriffe. Ihnen gemein ist der Aspekt der Klassifikation von Objekten.

Satz 4.3.4. *Sei M eine nicht leere Menge, und sei $\mathcal{N}$ eine Zerlegung von M. Dann ist*

$$\equiv = \left\{(x, y) \in M \times M \mid \exists N(N \in \mathcal{N} \wedge \{x, y\} \subseteq N)\right\}$$

eine Äquivalenzrelation auf M.

Beweis. Offensichtlich ist $\equiv$ eine Relation auf M.

- Reflexivität: Sei $x \in M$. Da $M = \bigcup \mathcal{N}$ gibt es eine Menge $N \in \mathcal{N}$ mit $x \in N$. Also $x \equiv x$.
- Symmetrie: Sei $x \equiv y$. Dann existiert $N \in \mathcal{N}$ mit $\{x, y\} \subseteq N$. Folglich auch $y \equiv x$.
- Transitivität: Seien $x \equiv y$ und $y \equiv z$. Also existieren $N, N' \in \mathcal{N}$ mit $\{x, y\} \subseteq N$ und $\{y, z\} \subseteq N'$. Da $y \in N \cap N'$ gilt $N = N'$, denn andernfalls wären N und N' disjunkt. Folglich $\{x, z\} \subseteq N$ und damit $x \equiv z$. □

4.4 Ordnungsrelationen

Eine Relation $\preceq$ auf M ist eine Ordnungsrelation gdw. sie reflexiv, antisymmetrisch und transitiv ist. Das Paar $(M, \preceq)$ heißt dann teilweise oder partiell geordnete Menge. Ist $\preceq$ auch vollständig, dann heißt $(M, \preceq)$ auch total geordnete Menge, linear geordnete Menge oder Kette. Die Schreibweise $(M, \preceq)$ mag etwas ungewohnt erscheinen, sie trägt jedoch der Tatsache Rechnung, dass wir uns die Menge M nun geordnet vorstellen.

Beispiele 4.4.1.

1. *Die Identität* $\mathrm{id}_{\mathbb{N}}$ *ist eine Ordnungsrelation, aber nicht vollständig.*
2. *Die Struktur* $(\mathbb{N}, \leq)$ *ist eine total geordnete Menge.*
3. *Für jede Menge* M *ist* $(\mathcal{P}(M), \subseteq)$ *eine teilweise geordnete Menge.*
4. *Die Teilbarkeitsrelation* $\mid = \{(n, n') \in \mathbb{N}_+ \times \mathbb{N}_+ \mid n \text{ teilt } n'\}$ *ist eine Ordnungsrelation.*

   Beweis. Reflexivität: Für alle $x \in \mathbb{N}_+$ teilt x sich selbst, also $x \mid x$.

   Antisymmetrie: Seien $x \mid y$ und $y \mid x$. Dann gelten $x \leq y$ und $y \leq x$, womit $x = y$ folgt (Antisymmetrie von $\leq$).

   Transitivität: Seien $x \mid y$ und $y \mid z$. D. h. es existieren $k, n \in \mathbb{N} \setminus \{0\}$, so dass $kx = y$ und $ny = z$. Also $z = ny = n(kx) = (nk)x$, womit auch $x \mid z$ gilt. □

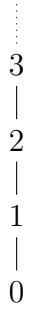


Abbildung 4.3: $(\mathbb{N}, \leq)$

Endliche teilweise geordnete Mengen lassen sich durch Hasse-Diagramme[1] visualisieren (siehe rechts). Alle Kanten sind per Konvention nach oben gerichtet. Kanten aus id_M (Schleifen) werden nicht dargestellt, ebenso Kanten, die sich vermittels Transitivität aus anderen Kanten ergeben. Dies trägt zur Übersichtlichkeit des Diagramms bei.

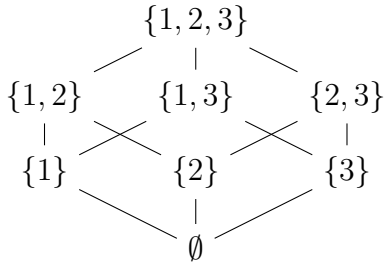


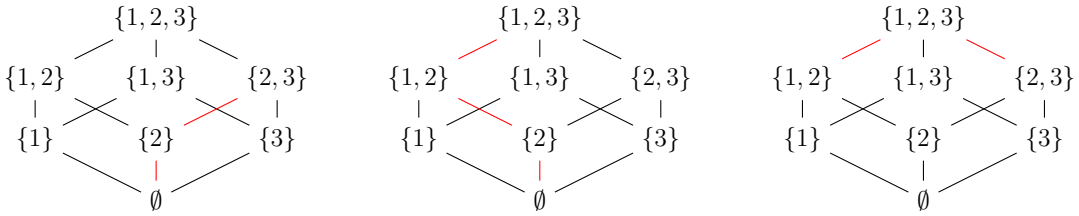
Abbildung 4.4: $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$

Sei $(M, \preceq)$ eine teilweise geordnete Menge. Eine Teilmenge $X \subseteq M$ ist Teilkette von $(M, \preceq)$ gdw. $x \preceq y$ oder $y \preceq x$ für alle $x, y \in X$.

Beispiele 4.4.2.

- *Die Menge* $\mathbb{N}$ *ist eine Teilkette von* $(\mathbb{Z}, \leq)$
- *Die Menge* $\{\emptyset, \{2\}, \{2, 3\}\}$ *ist eine Teilkette von* $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$
- *Die Menge* $\{\emptyset, \{2\}, \{1, 2\}, \{1, 2, 3\}\}$ *ist eine Teilkette von* $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$
- *Die Menge* $\{\{1, 2\}, \{1, 2, 3\}, \{2, 3\}\}$ *ist keine Teilkette von* $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$.

[1] Helmut Hasse (1898–1979)



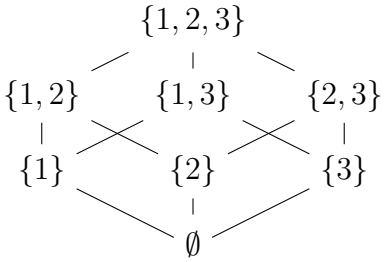
4.4.1 Schranken, Maxima und Minima

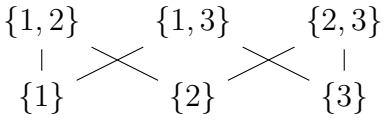
Im folgenden führen wir einige wichtige Begriffe für die Untersuchung geordneter Mengen ein. Sei $(M, \preceq)$ eine teilweise geordnete Menge. Ein Element $x \in M$ ist

- maximal gdw. $x \not\preceq m$ für alle $m \in M$ mit $m \neq x$;
  d. h. es gibt keine echt größeren Elemente,
- minimal gdw. $m \not\preceq x$ für alle $m \in M$ mit $m \neq x$;
  d. h. es gibt keine echt kleineren Elemente.

Beispiele 4.4.3.

- *In* $(\mathbb{N}, \leq)$ *haben wir* 0 *als einziges minimales Element und keine maximalen Elemente.*
- *In* $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$
  - *maximale Elemente:* $\{1, 2, 3\}$
  - *minimale Elemente:* $\emptyset$
- *In* $(\mathcal{P}(\{1, 2, 3\}) \setminus \{\emptyset, \{1, 2, 3\}\}, \subseteq)$
  - *maximale Elemente:* $\{1, 2\}$, $\{1, 3\}$ *und* $\{2, 3\}$
  - *minimale Elemente:* $\{1\}$, $\{2\}$ *und* $\{3\}$





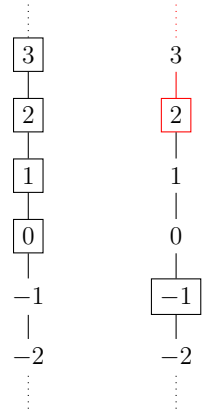
Sei $(M, \preceq)$ eine teilweise geordnete Menge und $X \subseteq M$. Ein Element $m \in M$ ist

- eine obere Schranke für X gdw. $x \preceq m$ für alle $x \in X$;
  d. h. größer als alle Elemente aus X,
- das größte Element von X gdw. $m \in X$ und m obere Schranke für X ist;
  d. h. obere Schranke von X, die in X liegt.

Es gibt höchstens ein größtes (bzw. kleinstes) Element von X. Wir bezeichnen mit $\uparrow X$ die Menge der oberen Schranken und mit $\max_{\preceq} X$ das größte Element von X. Die Begriffe untere Schranke und kleinstes Element werden analog definiert.

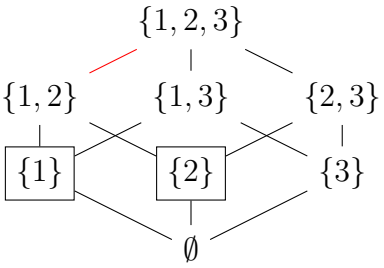
Beispiele 4.4.4.

- *In* $(\mathbb{Z}, \leq)$ *hat* $\mathbb{N}$
  - *obere Schranken: keine*
  - *größtes Element: keins*



- *In* $(\mathbb{Z}, \leq)$ *hat* $\{-1, 2\}$
  - *obere Schranken:* $\{z \in \mathbb{Z} \mid z \geq 2\}$
  - *größtes Element:* 2

- *In* $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$ *hat* $\{\{1\}, \{2\}\}$
  - *obere Schranken:* $\{1, 2\}$ *und* $\{1, 2, 3\}$
  - *größtes Element: keins*



Kapitel 5

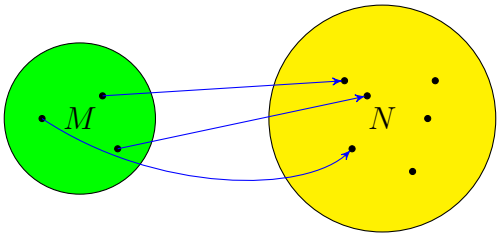
Funktionen

Die Summe zweier Zahlen und die Länge einer gegebenen Zeichenkette sind eindeutig bestimmt. Derartige eindeutige Zuordnungen sind hochgradig relevant in Theorie und Praxis. Der Aspekt der Eindeutigkeit motiviert den Funktionsbegriff.

Eine Relation $R \subseteq M \times N$ ist eine Funktion oder Abbildung gdw. für jedes $m \in M$ genau ein $n \in N$ existiert, so dass $(m, n) \in R$. Mit anderen Worten: Für jedes $m \in M$ gibt es mindestens ein $n \in N$ (Totalität oder Existenz) und höchstens ein $n \in N$ (Eindeutigkeit) mit $m\ R\ n$. Während sich die Existenzbedingung leicht mithilfe des Existenzquantors formulieren lässt, greift man bezüglich der Eindeutigkeit gewissermaßen zu einem Trick. Man formuliert: Falls ein Element $m \in M$ mit zwei Elementen $x, y \in N$ in Relation steht, so müssen diese übereinstimmen. Konkret:

$$\forall m \Big(m \in M \to \exists n \big(n \in N \wedge R(m, n) \big) \Big) \qquad \text{(Totalität)}$$

$$\forall m, x, y \Big(\big(m \in M \wedge x \in N \wedge y \in N \wedge R(m, x) \wedge R(m, y) \big) \to x = y \Big) \qquad \text{(Eindeutigkeit)}$$



Beispiele 5.0.1.

- *Sei B die Menge der Bundesbürger. Die Relation*

$$\big\{ (p, n) \in B \times \mathbb{N} \mid p \text{ hat Identifikationsnummer } n \big\}$$

  von B nach $\mathbb{N}$ ist eine Funktion.

- *Keine Funktion ist die Freund-Relation*

$$\big\{(x,y) \in F \times F \mid x \text{ ist Facebook-Freund von } y\big\}$$

  auf der Menge der Facebook-Nutzer F.

- *Die Relation $R = \big\{(n,n') \mid n \in \mathbb{N},\, n' = 2n\big\}$ ist eine Funktion.*

- *Die Identität id_M ist eine Funktion.*

Sei $f \subseteq M \times N$ eine Funktion von M nach N. Dann schreibt man üblicherweise $f\colon M \to N$. Für Elemente $m \in M$ und $n \in N$ mit $(m,n) \in f$ schreibt man entweder

$$n = f(m) \qquad \text{oder} \qquad m \overset{f}{\mapsto} n \ .$$

Man nennt n dann Bild von m und umgekehrt m Urbild von n. Die Menge M heißt Definitionsbereich und die Menge N Bildbereich oder Wertebereich von f. Für eine gegebene Teilmenge $M' \subseteq M$ bezeichnet

$$f(M') = \big\{f(m) \mid m \in M'\big\}$$

die Menge aller Bilder von Elementen aus M', die wir dementsprechend als Bild von M' unter f bezeichnen. Analog ist

$$f^{-1}(N') = \big\{m \in M \mid f(m) \in N'\big\}$$

die Menge aller Urbilder von Elementen aus N'.

Beispiele 5.0.2.

- *Die Funktion $\mathrm{id}_M\colon M \to M$ ist definiert durch*

$$\mathrm{id}_M(m) = m.$$

  Es gilt $\mathrm{id}_M(M') = M'$ und $\mathrm{id}_M^{-1}(M') = M'$ für alle $M' \subseteq M$.

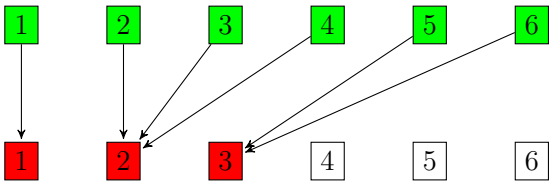
- *Sei verdoppeln$\colon \mathbb{N} \to \mathbb{N}$ die Funktion mit verdoppeln$(n) = 2n$ für alle $n \in \mathbb{N}$. Es gilt*

$$\textit{verdoppeln}(\mathbb{N}) = \{2x \mid x \in \mathbb{N}\} \quad \textit{und} \quad \textit{verdoppeln}^{-1}\big(\{2k+1 \mid k \in \mathbb{N}\}\big) = \emptyset \ .$$

- *Sei $M = \{1, 2, 3, 4, 5, 6\}$. Wir betrachten die Funktion $f\colon M \to M$ mit $m \mapsto \lceil \sqrt{m} \rceil$ für alle $m \in M$.*

Es gilt

$$f(M) = \{1, 2, 3\}$$
$$f(\{1, 2\}) = \{1, 2\}$$
$$f^{-1}(\{2\}) = \{2, 3, 4\}$$



5.1 Eigenschaften von Funktionen

Angenommen, jedem Telefonanschluss soll genau eine Telefonnummer zugeordnet werden. Bei der Zuordnung handelt es sich dementsprechend um eine Funktion. Darüber hinaus soll eine Telefonnummer aber auch nicht mehrfach vergeben werden. Es ist naheliegend, auch diesen anderen Aspekt der Eindeutigkeit zu formalisieren.

Eine Funktion $f\colon M \to N$ heißt injektiv gdw. alle verschiedenen Elemente von M auch verschiedene Bilder unter f haben und surjektiv gdw. $f(M) = N$, also jedes Element von N das Bild eines Elements von M ist. Sind beide Eigenschaften erfüllt, so heißt f bijektiv. Eine bijektive Funktion auf einer Menge M wird auch Permutation von M genannt. Formal:

$$\forall x, y\Big((x \in M \wedge y \in M \wedge x \neq y) \to f(x) \neq f(y)\Big), \qquad \text{(Injektivität)}$$
$$\forall n\Big(n \in N \to \exists m(m \in M \wedge f(m) = n)\Big). \qquad \text{(Surjektivität)}$$

Beispiele 5.1.1.

- *Die Identität* $\mathrm{id}_M\colon M \to M$ *ist eine Permutation.*
- *Die Funktion verdoppeln*: $\mathbb{N} \to \mathbb{N}$ *ist injektiv, aber nicht surjektiv, denn* 3 *ist nicht erreichbar.*
- *Die Funktion* $f\colon \mathbb{N} \to \mathbb{N}$ *mit* $f(n) = \lceil\sqrt{n}\rceil$ *ist surjektiv, aber nicht injektiv, denn es gilt* $f(2) = f(3)$.
- *Die Funktion quadrieren*: $\mathbb{R} \to \mathbb{R}$ *mit quadrieren*$(x) = x^2$ *ist weder injektiv noch surjektiv, denn die negativen Zahlen sind nicht erreichbar und es gilt* $(-2)^2 = 2^2$.

5.2 Komposition von Funktionen

Funktionen sind insbesondere Relationen, also wir können die Funktionen komponieren. Im Prinzip ist die Komposition von zwei Funktionen “nur” eine Relation. Der folgende Satz sagt jedoch dass die Komposition von Funktionen wieder eine Funktion ist.

Satz 5.2.1. *Die Komposition zweier Funktionen ist wieder eine Funktion.*

Beweis. Seien $f\colon M \to N$ und $g\colon N \to P$. Dann ist $(f\,;g)(m) = g(f(m))$ für alle $m \in M$. Also ist $(f\,;g)(m)$ insbesondere existent und eindeutig bestimmt. □

Satz 5.2.2 (Assoziativität der Komposition)**.** *Für Abbildungen $f\colon M \to N$, $g\colon N \to P$ und $h\colon P \to Q$ gilt*

$$(f\,;g)\,;h = f\,;(g\,;h)$$

Tatsächlich gilt diese Eigenschaft bereits für Relationen.

Beweis. Offensichtlich handelt es sich um Funktionen. Sei $m \in M$ beliebig.

$$\begin{aligned}\big((f\,;g)\,;h\big)(m) &= h\big((f\,;g)(m)\big) = h\big(g(f(m))\big)\\ &= \big(g\,;h\big)(f(m)) = \big(f\,;(g\,;h)\big)(m)\end{aligned}$$ □

Analog zur Funktionseigenschaft übertragen sich auch Injektivität und Surjektivität bei der Komposition.

Satz 5.2.3. *Seien $f\colon M \to N$ und $g\colon N \to P$.*

1. *$f\,;g$ ist injektiv, falls f und g injektiv sind.*
2. *$f\,;g$ ist surjektiv, falls f und g surjektiv sind.*
3. *$f\,;g$ ist bijektiv, falls f und g bijektiv sind.*

Beweis.

1. Seien $m, m' \in M$ mit $m \neq m'$. Da f injektiv ist, gilt $f(m) \neq f(m')$. Da auch g injektiv ist, gilt weiterhin

   $$(f\,;g)(m) = g(f(m)) \neq g(f(m')) = (f\,;g)(m')\ .$$

   Also ist $f\,;g$ injektiv.

2. Sei $p \in P$ beliebig. Da g surjektiv ist, existiert $n \in N$, so dass $g(n) = p$. Weiterhin ist auch f surjektiv, wodurch $m \in M$ existiert, so dass $f(m) = n$. Also ist

   $$(f\,;g)(m) = g(f(m)) = g(n) = p\ .$$

   Also ist $f\,;g$ auch surjektiv.

3. Dies ergibt sich direkt aus (1) und (2). □

5.3 Invertierung von Funktionen

Die „Gutartigkeit“ von Funktionen bezüglich der Komposition ist keineswegs selbstverständlich. So liefert die Bildung der inversen Relation einer Funktion im Allgemeinen keine Funktion (siehe Abbildung unten). Manchmal möchte man eine Funktionsanwendung jedoch rückgängig machen können, zum Beispiel bei der Verschlüsselung und Kompression von Daten. Eine Funktion $f\colon M \to N$ ist invertierbar gdw. eine Funktion $g\colon N \to M$ existiert, so dass

$$f\,;g = \mathrm{id}_M \qquad \text{und} \qquad g\,;f = \mathrm{id}_N \ .$$

Beispiele 5.3.1.

- *Die Identität* id_M *ist offensichtlich invertierbar.*
- *Die Funktion verdoppeln ist nicht invertierbar. Welchen Wert soll die inverse Funktion der Zahl* 3 *zuweisen?*
- *Die Funktion* f *mit* $f(n) = \lceil\sqrt{n}\rceil$ *ist nicht invertierbar. Welchen Wert soll die inverse Funktion der Zahl* 2 *zuweisen?*

Obwohl es sich bei f^{-1} nicht immer um eine Funktion handelt, ist f^{-1} dennoch ein guter Kandidat für die Invertierung einer dafür geeigneten Funktion $f\colon M \to N$. Dazu müssen wir nachweisen, dass Elemente $m \in M$ und $n \in N$ unter wechselseitiger „Anwendung“ von f und f^{-1} auf sich selbst abgebildet werden.

Lemma 5.3.2. *Sei* $f\colon M \to N$. *Für alle* $m \in M$ *und* $n \in N$ *gelten*

1. $m \in f^{-1}(\{f(m)\})$,
2. $f(f^{-1}(\{n\})) = \{n\}$, *falls* f *surjektiv ist.*

Beweis.

1. Wir setzen zunächst einfach die Definition ein:

$$\begin{aligned} f^{-1}\big(\{f(m)\}\big) &= \big\{x \in M \mid f(x) \in \{f(m)\}\big\} \\ &= \big\{x \in M \mid f(x) = f(m)\big\} \ni m \ . \end{aligned}$$

2. Sei $n \in N$. Dann gilt

$$\begin{aligned} f\big(f^{-1}(\{n\})\big) &= \big\{f(x) \mid x \in f^{-1}(\{n\})\big\} \\ &= \big\{f(x) \mid x \in \{y \in M \mid f(y) = n\}\big\} \\ &= \big\{f(x) \mid x \in M,\, f(x) = n\big\} \\ &= \{n\}. \qquad (f \text{ surjektiv}) \end{aligned}$$ □

Es besteht ferner die Frage, welche Funktionen für eine Invertierung geeignet sind. Der folgende Satz charakterisiert diese Funktionen.

Satz 5.3.3. *Eine Funktion $f\colon M \to N$ ist invertierbar gdw. sie bijektiv ist.*

Beweis.

($\to$) Sei f invertierbar. Dann existiert eine Funktion $g\colon N \to M$, so dass $f\,;g = \mathrm{id}_M$ und $g\,;f = \mathrm{id}_N$.

- Injektivität: Seien $x, y \in M$ mit $f(x) = f(y)$. Zu zeigen: $x = y$. Es gilt

$$\begin{aligned} x &= \mathrm{id}_M(x) = (f\,;g)(x) = g(f(x)) \\ &= g(f(y)) = (f\,;g)(y) = \mathrm{id}_M(y) = y. \end{aligned}$$

- Surjektivität: Sei $n \in N$ beliebig. Dann ist $f(g(n)) = (g;f)(n) = \mathrm{id}_N(n) = n$. Also existiert ein $m \in M$, so dass $g(n) = m$ und $f(m) = n$.

($\leftarrow$) Sei f bijektiv. Wir zeigen die Invertierbarkeit von f vermittels f^{-1}. Zunächst zeigen wir, dass f^{-1} eine Funktion ist.

- Totalität: Sei $n \in N$ beliebig. Da f surjektiv ist, existiert $m \in M$ mit $f(m) = n$. Also $(n, m) \in f^{-1}$.
- Eindeutigkeit: Seien $(n, x) \in f^{-1}$ und $(n, y) \in f^{-1}$. Folglich gilt $f(x) = n = f(y)$ und gemäß der Kontraposition der Injektivität von f folgt $x = y$.

Nun zeigen wir $f\,;f^{-1} = \mathrm{id}_M$ und $f^{-1}\,;f = \mathrm{id}_N$. Für jedes $m \in M$ und $n \in N$ gelten

$$\begin{aligned} (f\,;f^{-1})(m) &= f^{-1}(f(m)) = m \quad \text{und} \\ (f^{-1}\,;f)(n) &= f(f^{-1}(n)) = n, \end{aligned}$$

denn $m \in f^{-1}(\{f(m)\})$ und $f(f^{-1}(\{n\})) = \{n\}$ entsprechend Lemma 5.3.2. □

Wir zeigen noch, dass sich eine Funktion f vermittels höchstens einer Funktion invertieren lässt, nämlich ihrer inversen Funktion f^{-1}.

Satz 5.3.4 (Eindeutigkeit des Inversen)**.** *Sei* $f\colon M \to N$ *und seien* $g, g'\colon N \to M$ *mit*

$$f\,;g = \mathrm{id}_M, \qquad g\,;f = \mathrm{id}_N,$$
$$f\,;g' = \mathrm{id}_M, \qquad g'\,;f = \mathrm{id}_N.$$

Dann gilt $g = g'$.

Beweis. Wegen der Assoziativität der Komposition gilt

$$g = g\,;\mathrm{id}_M = g\,;(f\,;g') \qquad = (g\,;f)\,;g' = \mathrm{id}_N\,;g' = g' \ . \qquad \square$$

5.4 Einseitige Inversen und das Auswahlaxiom

5.4.1 Einseitige Inversen von injektiven Funktionen

In Anwendungen wie zum Beispiel die Verschlüsselung sind die Funktionen, mit denen wir arbeiten, häufig nicht bijektiv, sondern nur injektiv. In diesem Fall spricht man von einer einseitigen Inverse.

Satz 5.4.1. *Für jede injektive Funktion* $f\colon M \to N$ *existiert eine Funktion* $g\colon N \to M$*, so dass* $f; g = \mathrm{id}_M$.

Beweis. Die Relation f^{-1} ist eindeutig. Wir zeigen dass wie früher für bijektionen: Seien $(n, x) \in f^{-1}$ und $(n, y) \in f^{-1}$. Folglich gilt $f(x) = n = f(y)$ und gemäß der Kontraposition der Injektivität von f folgt $x = y$.

Sei $m_0 \in M$ beliebig. Wir definieren $g\colon N \to M$ wie folgt: wenn $n \in f(M)$ dann $g(n) := f^{-1}(n)$, und sonst $g(n) := m_0$.

Wir müssen zeigen dass wenn $m \in m$ dann gilt $f; g(m) = m$. Wir haben jedoch $f; g(m) = g(f(m))$, und da $f(m) \in f(M)$, folgt $g(f(m)) = f^{-1}(f(m)) = m$. $\square$

5.4.2 Einseitige Inversen von surjektiven Funktionen

Motiviert durch den vorangegangenen Abschnitt, und vielleicht auch durch unsere Intuition, geben wir auch den folgenden Satz an und beweisen ihn.

Satz 5.4.2. *Für jede surjektive Funktion* $f\colon M \to N$ *existiert eine Funktion* $g\colon N \to M$*, so dass* $g\,;f = \mathrm{id}_N$.

Da die Funktion f nicht notwendigerweise injektiv ist, ist unser Kandidat f^{-1} im Allgemeinen nicht eindeutig, also auch keine Funktion. Der Beweis folgt nun einer simplen Idee: Wir wählen für jedes Element $n \in N$ ein beliebiges Urbild $m_n \in f^{-1}(\{n\})$ aus und gewinnen so aus f^{-1} die gesuchte Funktion g.

Beweis (nutzt Auswahlaxiom). Sei $n \in N$ beliebig.

Da f surjektiv ist, existiert $m \in M$ mit $f(m) = n$. Also $f^{-1}(\{n\}) \neq \emptyset$.

Wähle ein $m_n \in f^{-1}(\{n\})$ für jedes $n \in N$.

Wir definieren die Funktion $g\colon N \to M$ durch $g(n) = m_n$.

Zu zeigen: $g\,;f = \mathrm{id}_N$. Für alle $n \in N$ gilt

$$(g\,;f)(n) = f(g(n)) = f(m_n) = n = \mathrm{id}_N(n),$$

denn $f(f^{-1}(\{n\})) = \{n\}$ nach Lemma 5.3.2. □

Die Kernidee des Beweises ist offensichtlich die Auswahl. Eine solche Auswahl erscheint auf den ersten Blick einfach; sie ist jedoch alles andere als trivial. Zur Untermauerung dieser These betrachten wir die Menge $\mathcal{P}(\mathbb{R})\setminus\{\emptyset\}$ aller nicht-leeren Teilmengen der reellen Zahlen. Gelingt es Ihnen eine konkrete Vorschrift anzugeben, die jeder Menge $X \subseteq \mathbb{R}$ mit $X \neq \emptyset$ genau eines ihrer Elemente $r \in X$ zuordnet? Um es vorwegzunehmen: bisher ist dies nicht gelungen. Es gibt jedoch auch keinen Grund zu der Annahme, dass eine solche Auswahl nicht existiert. Das folgende Auswahlaxiom (AC[1]) ist eine unbewiesene Grundannahme, ein sogenanntes Axiom. Man kann AC also annehmen oder eben nicht.

Axiom (Auswahlaxiom, Zermelo 1904)**.** Für jede Menge $\mathcal{X}$ von nicht-leeren Mengen gibt es eine Auswahlfunktion, d.h. Funktion $c\colon \mathcal{X} \to \bigcup \mathcal{X}$ mit $c(X) \in X$ für alle $X \in \mathcal{X}$.

Die Mathematik arbeitet entsprechend der axiomatischen Methode. Das bedeutet, dass man mathematische Erkenntnisse durch Beweise auf der Grundlage von Axiomen und bereits bewiesenen Aussagen gewinnt. Man kann Mathematik nun derart betreiben, dass man sich auf einen intuitiven Mengenbegriff, eine intuitive Konzeption der natürlichen Zahlen oder andere Grundsätze beruft. Dieser Ansatz wird in der Schule verfolgt und auch wir werden diesem Ansatz folgen, aber ab einem gewissen Punkt (siehe Kapitel 8) führt dies zu Schwierigkeiten (Widersprüchen). Daher begann man gegen Ende des 19. Jahrhunderts mit der Aufstellung von Axiomensystemen, also explizit formulierter Axiome.

Bekannte Axiomensysteme sind ZF (Zermelo-Fraenkel) und ZFC[2] (Zermelo-Fraenkel with Choice) für Mengen und die Peano-Axiome[3] der natürlichen Zahlen. Das Auswahlaxiom

[1] Axiom of choice
[2] nach Ernst Zermelo (1871–1953), Abraham Fraenkel (1891–1965) und Choice
[3] Guiseppe Peano (1858–1932)

ist heute allgemein akzeptiert, wobei die Nutzung jedoch gekennzeichnet werden sollte. Aufgrund der Komplexität von ZFC geben wir an dieser Stelle lediglich eine Variante der Peano-Axiome an.

Beispiel 5.4.3. *Die natürlichen Zahlen sind ein System (N, s, z), so dass*

1. *$z \in N$ und $s\colon N \to N$ injektiv,*
2. *$z \notin s(N)$,*
3. *jede Teilmenge $E \subseteq N$ mit*
   - *$z \in E$ und*
   - *$n \in E \to s(n) \in E$ für alle $n \in N$*

   erfüllt $E = N$.

Das „System“ $(\mathbb{N}, \text{nachfolger}, 0)$ mit $\text{nachfolger}(n) = n + 1$ für alle $n \in \mathbb{N}$ erfüllt die Peano-Axiome, wie man leicht zeigen kann.

5.5 Bemerkung über endlichen Mengen

Wir enden diesen Kapitel mit der folgenden Bemerkung.

Satz 5.5.1. *Eine Funktion $f\colon M \to M$ auf einer endlichen Menge M ist surjektiv genau dann, wenn sie injektiv ist.*

Beweis. Wir betrachten die Menge $\mathcal{M} = \{f^{-1}(\{m\}) \mid m \in f(M)\}$. Offenbar ist $\mathcal{M}$ eine Zerlegung von M. Sei $c_m = |f^{-1}(\{m\})|$ für alle $m \in f(M)$. Es gilt $c_m \geq 1$ und weiterhin $|M| = |\bigcup \mathcal{M}| = \sum_{m \in f(M)} c_m$.

($\to$) (indirekt) Sei f surjektiv, aber nicht injektiv. Dann ist $f(M) = M$ und $c_m \geq 2$ für ein $m \in M$. Es folgt jedoch $\sum_{m \in M} c_m > |M|$. Widerspruch.

($\leftarrow$) (indirekt) Sei f injektiv, aber nicht surjektiv. Dann ist $c_m = 1$ für alle $m \in f(M)$ und $|f(M)| < |M|$. Also auch $\sum_{m \in f(M)} c_m = |f(M)| < |M|$. Widerspruch. □

Dieses Resultat gilt nicht für unendliche Mengen. So ist die Funktion verdoppeln$\colon \mathbb{N} \to \mathbb{N}$ zwar injektiv, aber nicht surjektiv. Die Funktion $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(n) = \lceil \sqrt{n} \rceil$ für alle $n \in \mathbb{N}$ ist surjektiv, aber nicht injektiv.

Kapitel 6

Der Satz von Cantor-Schröder-Bernstein

6.1 Fixpunkte

Die Iteration ist ein wesentliches Prinzip in Rainer Mathematik und in der Programmierung. Ein wichtiger Aspekt der Iteration sind die sogenannte Fixpunkte. Sei $f\colon M \to M$ eine Funktion auf einer Menge M. Ein Fixpunkt von f ist ein Element $m \in M$, so dass $f(m) = m$.

Beispiele 6.1.1.

- *Die Funktion nachfolger*: $\mathbb{N} \to \mathbb{N}$ *hat keine Fixpunkte.*
- *Die Funktion* $f\colon \mathbb{N} \to \mathbb{N}$ *mit* $n \mapsto \lceil \sqrt{n} \rceil$ *hat die Fixpunkte* 0, 1 *und* 2.

In der Fixpunkttheorie ist man an Kriterien für die Existenz von Fixpunkten interessiert. Wir beweisen das Kriterium von Knaster-Tarski. Letztlich wird uns dieses Resultat bei Untersuchungen zur Größe von Mengen helfen.

Lemma 6.1.2. *Sei M eine Menge. Wir betrachten die teilweise geordnete Menge $(\mathcal{P}(M), \subseteq)$. Sei $\mathcal{X} \subseteq \mathcal{P}(M)$. Dann gilt*

$$\bigcup \mathcal{X} \subseteq U \quad \text{für alle } U \in {\uparrow}\mathcal{X},$$

d. h. $\bigcup \mathcal{X}$ ist die kleinste obere Schranke von $\mathcal{X}$.

Beweis. Seien $U \in {\uparrow}\mathcal{X}$ und $m \in \bigcup \mathcal{X}$. Dann existiert ein $N \in \mathcal{X}$, so dass $m \in N$.
Da U obere Schranke für $\mathcal{X}$ ist und $N \in \mathcal{X}$, gilt $N \subseteq U$.
Aus $N \subseteq U$ und $m \in N$ folgt $m \in U$. □

Satz 6.1.3 (Lemma von Knaster-Tarski[1])**.**
Sei $f\colon \mathcal{P}(M) \to \mathcal{P}(M)$ mit $f(X) \subseteq f(Y)$ für alle $X \subseteq Y \subseteq M$.
Dann hat f einen Fixpunkt.

Beweis. Seien

$$P = \big\{X \in \mathcal{P}(M) \mid X \subseteq f(X)\big\}$$

und $N = \bigcup P$. Für jede Menge $X \in P$ gilt offensichtlich $X \subseteq N$. Nach Annahme gilt

$$X \subseteq f(X) \subseteq f(N),$$

womit $f(N)$ eine obere Schranke von P ist. Nach Lemma 6.1.2 ist

$$N = \bigcup P \subseteq f(N),$$

also nach Annahme auch $f(N) \subseteq f(f(N))$, wodurch $f(N) \in P$. Demzufolge gilt auch

$$f(N) \subseteq \bigcup P = N$$

und wir erhalten $N = f(N)$ und damit den Fixpunkt N. □

Beispiele 6.1.4.

- *Für welche Teilmengen $X \subseteq \mathbb{N}$ gilt $\mathit{nachfolger}(X) = X$?* *Für $X = \emptyset$*
- *Sei nun $\mathit{nachfolger}'\colon \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$, so dass für alle $X \subseteq \mathbb{N}$*

  $$\mathit{nachfolger}'(X) = X \cup \mathit{nachfolger}(X).$$

  Für welche Teilmengen $X \subseteq \mathbb{N}$ gilt $\mathit{nachfolger}'(X) = X$?
  Sowohl für $X \in \{\emptyset, \mathbb{N}\}$ als auch für $X_k = \{n \in \mathbb{N} \mid n \geq k\}$ mit $k \in \mathbb{N}$.

6.2 Der Satz von Cantor-Schröder-Bernstein

Wir wollen das Kriterium von Knaster-Tarski nutzen, um ein äußerst hilfreiches Kriterium für die Existenz einer Bijektion zwischen zwei Mengen herauszuarbeiten. Zur Vorbereitung weisen wir auf einige einfache Tatsachen über Mengen und Funktionen hin.

Lemma 6.2.1. *Seien $f\colon M \to N$ und $X \subseteq Y \subseteq M$. Es gelten*

(i) $f(X) \subseteq f(Y)$, *(ii)* $M \setminus Y \subseteq M \setminus X$, *(iii)* $M \setminus (M \setminus X) = X$.

[1] Bronisław Knaster (1893–1980) und Alfred Tarski (1901–1983)

Satz 6.2.2 (Cantor-Schröder-Bernstein[2]). *Seien $f\colon M \to N$ und $g\colon N \to M$ injektive Funktionen. Dann existiert eine bijektive Funktion $B\colon M \to N$.*

Beweis. Wir definieren die Funktion

$$\begin{aligned} h\colon \mathcal{P}(M) &\to \mathcal{P}(M) \\ h(X) &= M \setminus g\big(N \setminus f(X)\big) \ . \end{aligned}$$

Für alle $X \subseteq Y \subseteq M$ gelten nach obigem Lemma

$$f(X) \subseteq f(Y), \quad \text{also} \quad N \setminus f(Y) \subseteq N \setminus f(X) \quad \text{und} \quad g\big(N \setminus f(Y)\big) \subseteq g\big(N \setminus f(X)\big)$$

und damit $h(X) \subseteq h(Y)$.
Nach dem Lemma von Knaster-Tarski existiert also ein Fixpunkt $F \subseteq M$ bezüglich h. Es gilt

$$M \setminus F = M \setminus h(F) = M \setminus \Big(M \setminus g\big(N \setminus f(F)\big)\Big) = g\big(N \setminus f(F)\big) \ .$$

Wir definieren die Relation $B \subseteq M \times N$ durch

$$B = \big\{(m,n) \in f \mid m \in F\big\} \cup \big\{(m,n) \in g^{-1} \mid m \in M \setminus F\big\}$$

und zeigen im Folgenden, dass B eine Bijektion ist.

Totalität: Sei $m \in M$. Falls $m \in F$, dann gilt $\big(m, f(m)\big) \in B$. Sonst ist

$$m \in M \setminus F = g\big(N \setminus f(F)\big),$$

also existiert $n \in N \setminus f(F)$, so dass $g(n) = m$ und damit $(m,n) \in B$.

Eindeutigkeit: Seien $(m,x) \in B$ und $(m,y) \in B$. Falls $m \in F$, dann gilt $x = f(m) = y$. Andernfalls gilt $g(x) = m = g(y)$ und aufgrund der Injektivität von g gilt dann auch $x = y$.

Surjektivität: Sei $n \in N$. Falls $n \in f(F)$, dann existiert $m \in F$, so dass $f(m) = n$. Damit gilt $B(m) = n$. Sonst ist $n \in N \setminus f(F)$ und damit

$$g(n) \in g\big(N \setminus f(F)\big) = M \setminus F.$$

Also ist $B\big(g(n)\big) = n$.

[2]Der Satz wurde 1887 von Georg Cantor formuliert, aber nicht bewiesen. Ernst Schröder (1841–1902) publizierte 1896 eine Beweisskizze, die sich jedoch als falsch herausstellte. Ein Jahr später bewies der 19-jährige Felix Bernstein (1878–1956) den Satz in einem von Georg Cantor geleiteten Seminar. Später wurde bekannt, dass Richard Dedekind (1831–1916) bereits 1887 einen Beweis gefunden hatte, den er jedoch weder publizierte, noch Cantor mitteilte.

Injektivität: Seien $x, y \in M$ mit $B(x) = B(y)$.

- Sei $B(x) \in f(F)$.
  Existiert ein $m \in \{x, y\}$ mit $m \in M \setminus F$, dann existiert wegen $M \setminus F = g\big(N \setminus f(F)\big)$ auch ein $n \in N \setminus f(F)$ mit $g(n) = m$. Damit gilt $B(m) = n \in N \setminus f(F)$, was jedoch $B(m) = B(x) \in f(F)$ widerspricht. Also gilt $x, y \in F$. Damit gilt jedoch auch $x = y$, da f injektiv ist.

- Sei $B(x) \notin f(F)$.
  Dann gilt $x, y \in M \setminus F$, also $x = g(B(x)) = g(B(y)) = y$. □

Kapitel 7

Mächtigkeit von Mengen

Wir haben in Kapitel 2 die Größe von Mengen auf intuitive Weise betrachtet. Die Schwachstelle dieses Kardinalitätskonzepts besteht in der großen Ungenauigkeit bezüglich unendlicher Mengen. So konnten wir im Hinblick auf $\mathbb{N}$ und $\mathbb{R}$ lediglich

$$|\mathbb{N}| \geq \infty \leq |\mathbb{R}|$$

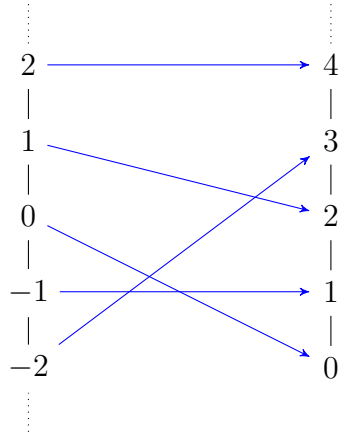
feststellen. In diesem Kapitel werden wir den Kardinalitätsbegriff präzisieren, und insbesondere werden wir sehen dass es verschiedene Typen von Unendlichkeiten gibt, die als "grössere" und "kleinere" Unendlichkeiten beschrieben werden können. Und in der Tat, es gibt unendlich viele Unendlichkeiten.

Zwei Mengen M und N sind gleichmächtig, kurz $|M| = |N|$, gdw. eine bijektive Funktion $f\colon M \to N$ existiert.

Beispiele 7.0.1.

- $|\emptyset| \neq |M|$ *für alle nicht-leeren Mengen* M
- $|\{1, 2, 3\}| = |\{6, 9, 11\}|$
  via $\{(1, 6), (2, 9), (3, 11)\}$
- $|\mathbb{Z}| = |\mathbb{N}|$ *vermittels* $f\colon \mathbb{Z} \to \mathbb{N}$ *mit*

$$f(z) = \begin{cases} 2z & \text{falls } z \geq 0 \\ -(2z+1) & \text{sonst} \end{cases}$$



Wenn wir irgendwwelche Universum $\mathcal{U}$ von Mengen haben, die Gleichmächtigkeit lässt sich als eine Äquivalenzrelation auf $\mathcal{U}$ auffassen. Ihre Äquivalenzklassen heißen Kardinalitäten.

Bemerkung 7.0.2. Wir könnten auch über Kardinalitäten sprechen, ohne ein Universum $\mathcal{U}$ festzulegen. Stattdessen könnte man von der so genannten Klasse $\mathcal{U}$ aller Mengen sprechen und die Äquivalenzklassen der Gleichmächtigkeit auf $\mathcal{U}$ betrachten.

Das kleine Problem dabei ist, dass die Klasse $\mathcal{U}$ aller Mengen selbst keine Menge ist - das lässt sich anhand eines Arguments von Bertrand Russell zeigen, das als Russell-Paradox bekannt ist.

Nehmen wir an, dass $\mathcal{U}$ eine Menge ist. Dann definieren wir $V := \{M \in \mathcal{U} \colon M \notin M\}$. Nun haben wir zwei Möglichkeiten: entweder $V \in V$ oder $V \notin V$. Wenn $V \in V$, dann leiten wir durch die Definition von V ab, dass $V \notin V$. Wenn wir $V \notin V$ annehmen, dann folgern wir, dass $V \in V$. Das ist ein Widerspruch der zeigt, dass V nicht existieren kann, und dass $\mathcal{U}$ keine Menge ist.

Tatsächlich könnten wir in der gebräuchlichsten Axiomatisierung der Mengenlehre, dem Zermelo-Fraenkel-Axiomensystem, direkt aus den Axiome ableiten, dass eine Menge kann nicht sich selbst als ein Element enthalten. Das gibt uns eine andere Möglichkeit zu sehen, dass die Klasse aller Mengen selbst keine Menge ist. Die Entwicklung des Zeremlo-Fraenkel-Axiomensystems wurde unmittelbar durch die Entdeckung des Russell-Paradox beeinflusst.

Für den besonderen Zweck der Betrachtung von Kardinalitäten ist es jedoch in Ordnung die Tatsache zu "ignorieren", dass die Klasse aller Mengen keine Menge ist, da wir immer in einem ausreichend großen Universum von Mengen arbeiten können, das trotzdem noch eine Menge ist (eine solche Menge von Mengen wird als Grothendieck-Universum bezeichnet).

7.1 Mächtigkeit der Zahlenbereiche

Die Kardinalitäten endlicher Mengen entsprechen den natürlichen Zahlen, an dieser Stelle also alter (d.h. "die Anzahl von Elementen") und neuer Kardinalitätsbegriff übereinstimmen. Daher wollen wir im Folgenden die Mächtigkeit unendlicher Mengen genauer erkunden.

Satz 7.1.1. $|\mathbb{Q}| = |\mathbb{Z}|$

Die Beweisidee ist die folgende. Zunächst suchen wir, gemäß CSB, statt einer Bijektion nach zwei Injektionen $\mathbb{Z} \to \mathbb{Q}$ und $\mathbb{Q} \to \mathbb{Z}$. Erstere Injektion ist trivial. Für die zweite Injektion überlegen wir uns zunächst, dass es genügt eine Injektion $f_+ \colon \mathbb{Q}_+ \to \mathbb{N}_+$ anzugeben, denn dann ist

$$
\begin{aligned}
f \colon \mathbb{Q} &\to \mathbb{Z} \\
x &\mapsto \begin{cases} f_+(x) & \text{falls } x > 0 \\ 0 & \text{falls } x = 0 \\ -f_+\big(|x|\big) & \text{falls } x < 0 \end{cases}
\end{aligned}
$$

unsere gesuchte Injektion.

Die positiven rationalen Zahlen entsprechen den nicht weiter kürzbaren Brüchen $\frac{m}{n}$ mit $m, n \in \mathbb{N}_+$. Wir suchen eine injektive Funktion $f_+ \colon \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{N}_+$. Die Kernidee ist nun, dass wir die Dezimaldarstellungen zweier Zahlen durch Zufügen von führenden Nullen auf die gleiche Länge bringen und anschließend durch abwechselndes Schreiben der Ziffern eine neue Zahl herstellen können.

- $[m_\ell m_{\ell-1} \cdots m_1 m_0]_{10}$ ist die Dezimaldarstellung von m der Länge $l+1$.

  Für $m = 4906$ und $\ell = 3$ erhalten wir beispielsweise $m_3 = 4$, $m_2 = 9$, $m_1 = 0$ und $m_0 = 6$ und für $n = 331$ erhalten wir $n_3 = 0$, $n_2 = 3$, $n_1 = 3$ und $n_0 = 1$.

- Dann ist $f_+(\frac{m}{n}) = [m_\ell n_\ell m_{\ell-1} n_{\ell-1} \cdots m_1 n_1 m_0 n_0]_{10}$.

  Entsprechend ist $f_+(\frac{4906}{331}) = 40\,930\,361$.

Beweis. Nach dem Satz von Cantor-Schröder-Bernstein reicht die Angabe zweier injektiver Funktionen $f \colon \mathbb{Q} \to \mathbb{Z}$ und $g \colon \mathbb{Z} \to \mathbb{Q}$. Sei $g(z) = z$ für alle $z \in \mathbb{Z}$. Dann ist g offensichtlich injektiv, aber nicht surjektiv.

Wir konstruieren $f \colon \mathbb{Q} \to \mathbb{Z}$ für alle teilerfremden $m \in \mathbb{Z}$ und $n \in \mathbb{N} \setminus \{0\}$:

$$f\left(\frac{m}{n}\right) = \begin{cases} \sum_{i=0}^{\ell} (m_i \cdot 10^{2i+1} + n_i \cdot 10^{2i}) & \text{falls } m \geq 0 \\ -\sum_{i=0}^{\ell} (m_i \cdot 10^{2i+1} + n_i \cdot 10^{2i}) & \text{sonst,} \end{cases}$$

wobei $m_0, \ldots, m_\ell, n_0, \ldots, n_\ell \in \{0, \ldots, 9\}$ und

$$m = \sum_{i=0}^{\ell} m_i \cdot 10^i \qquad \text{und} \qquad n = \sum_{i=0}^{\ell} n_i \cdot 10^i \ .$$

Dies ist ebenso injektiv, da m und n direkt aus $f(\frac{m}{n})$ ablesbar sind. □

Das folgende Theorem zeigt jedoch, dass es tatsächlich mindestens zwei verschiedene unendliche Kardinalitäten gibt. Der Beweis verwendet eine Idee, die als "diagonales Argument" bezeichnet wird und die an vielen anderen Stellen in der Mathematik und Informatik verwendet wird.

Satz 7.1.2. $|\mathbb{N}| \neq |\mathbb{R}|$

Beweis. (indirekt) Sei $|\mathbb{N}| = |\mathbb{R}|$. Dann existiert eine bijektive Funktion $b \colon \mathbb{N} \to \mathbb{R}$. Schreibe Bilder als Dezimalzahlen mit $a_i \in \mathbb{Z}$ und $d_{ij} \in \{0, 1, \ldots, 9\}$

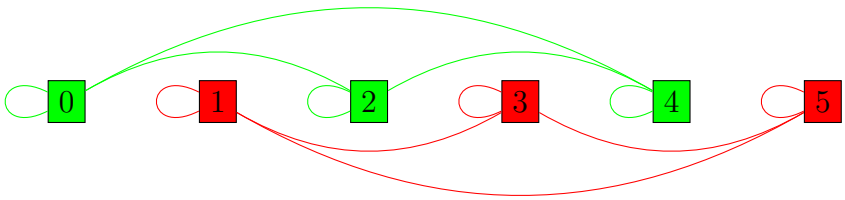
$$\begin{array}{rccccccccc}
b(0) = & a_0 & , & d_{00} & d_{01} & d_{02} & \cdots & d_{0n} & \cdots \\
b(1) = & a_1 & , & d_{10} & d_{11} & d_{12} & \cdots & d_{1n} & \cdots \\
b(2) = & a_2 & , & d_{20} & d_{21} & d_{22} & \cdots & d_{2n} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
b(n) = & a_n & , & d_{n0} & d_{n1} & d_{n2} & \cdots & d_{nn} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Für jedes $i \in \mathbb{N}$, wähle $d_i \in \{1, \ldots, 8\} \setminus \{d_{ii}\}$. Da b surjektiv ist, existiert ein $n \in \mathbb{N}$ mit $b(n) = 0, d_0 d_1 d_2 d_3 \ldots$. Es gilt $d_n = d_{nn} \neq d_{nn}$. Widerspruch! □

7.2 Ordnungsrelation auf Kardinalitäten

Wir haben bisher lediglich die Gleich- oder Ungleichmächtigkeit von Mengen definiert. Nun wollen wir die Mächtigkeiten untereinander ordnen. Wir wollen also eine Ordnungsrelation auf der Menge der Kardinalitäten definieren. Dies geschieht unter Zuhilfenahme der Repräsentanten, wobei man allerdings die Wohldefiniertheit der Konstruktion nachweisen muss. D.h. wir definieren $|M| \leq |N|$ ganau dann wenn es gibt eine Injektion $f\colon M \to N$, und wir möchten jetzt argumentieren dass diese Relation wohldefiniert ist.

Beispiel 7.2.1. *Wir betrachten erst ein Beispiel das zeigt warum man braucht die Wohldefinierthait zu beweisen. Dazu betrachten wir die durch das Bild veranschaulichte Äquivalenzrelation* $\equiv$.



1. *Die Konstruktion* $[i] \prec [j]$ *gdw.* $i < j$ *ist nicht wohldefiniert, denn* $[1] \prec [2]$ *aber* $[1] \not\prec [0] = [2]$.

2. *Die Konstruktion*

   $$[i] \prec [j] \quad \textit{gdw. es existiert eine ungerade Zahl } z \in \mathbb{Z} \textit{ mit } i = j + z$$

   ist wohldefiniert, denn sie ist unabhängig von den Repräsentanten.

Wir zeigen jetzt dass die Relation $\leq$ auf Kardinalitäten ist wohldefiniert.

Lemma 7.2.2. *Seien* M, X, N, Y *Mengen, so dass* $|M| = |X|$ *und* $|N| = |Y|$. *Es existiert eine injektive Funktion* $f\colon M \to N$ *(womit* $|M| \leq |N|$*)*

gdw. eine injektive Funktion $g\colon X \to Y$ existiert (womit $|X| \leq |Y|$).

Beweis.

($\to$) Sei $f\colon M \to N$ injektiv. Aufgrund der Annahme existieren $b\colon X \to M$ und $c\colon N \to Y$ bijektiv. Dann ist $(b\,;f\,;c)\colon X \to Y$ injektiv nach Satz 5.2.3.

($\leftarrow$) analog □

Wir sagen auch dass eine Menge N ist mächtiger als eine Menge M, gdw. $|M| \leq |N|$, also gdw. existiert eine injektive Funktion $f\colon M \to N$.

Beispiele 7.2.3.

- $|\mathbb{N}| \leq |\mathbb{Z}|$ *vermittels* $\mathrm{id}\colon \mathbb{N} \to \mathbb{Z}$ *mit* $\mathrm{id}(n) = n$ *für alle* $n \in \mathbb{N}$
- $|\emptyset| \leq |\mathbb{N}|$ *vermittels* $\emptyset$
- $|\{1, 2\}| \leq |\{2, 3, 4\}|$ *vermittels* $f = \{(1, 4), (2, 2)\}$

Zusammen mit der Teilmengenbeziehung haben wir nun zwei Konzepte zur Ordnung von Mengen vorliegen. Wie hängen diese zusammen?

Satz 7.2.4. *Sei $M \subseteq N$. Dann gilt $|M| \leq |N|$.*

Beweis. Sei $\mathrm{id}\colon M \to N$, so dass $\mathrm{id}(m) = m$ für alle $m \in M$. Offensichtlich ist 'id' injektiv. □

Der folgende Satz liefert uns eine alternative Charakterisierung der Mächtigkeitshierarchie, greift jedoch auf das Auswahlaxiom zurück.

Satz 7.2.5 (nutzt Auswahlaxiom)**.** *Sei $f\colon M \to N$ surjektiv. Dann gilt $|N| \leq |M|$.*

Beweis. Da f surjektiv ist, existiert gemäß Satz 5.4.2 (unter Nutzung des Auswahlaxioms) eine Funktion $g\colon N \to M$ mit $g\,;f = \mathrm{id}_N$. Wir zeigen per Kontraposition, dass g injektiv ist. Seien also $x, y \in N$ mit $g(x) = g(y)$. Dann gilt

$$\begin{aligned} x = \mathrm{id}_N(x) = (g\,;f)(x) = f(g(x)) \\ = f(g(y)) = (g\,;f)(y) = \mathrm{id}_N(y) = y \end{aligned}$$

Da g injektiv ist, gilt $|N| \leq |M|$. □

Der folgende Satz ist im Wesentichen eine Konsequenz des Satzes von Cantor-Schröder-Bernstein.

Satz 7.2.6. *Die Relation $\leq$ ist eine Ordnungsrelation auf Kardinalitäten.*

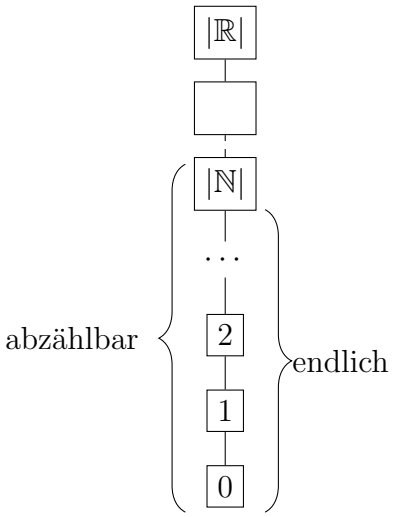
Beweis.

- Reflexivität: Für jede Menge M ist $\mathrm{id}_M \colon M \to M$ injektiv, also gilt $|M| \leq |M|$.
- Antisymmetrie: Seien $|M| \leq |N|$ und $|N| \leq |M|$. Also existieren injektive Funktionen $f \colon M \to N$ und $g \colon N \to M$. Dann existiert auch eine bijektive Funktion $h \colon M \to N$ nach CSB und damit $|M| = |N|$.
- Transitivität: Seien $|M| \leq |N|$ und $|N| \leq |P|$. Also existieren injektive Funktionen $f \colon M \to N$ und $g \colon N \to P$. Dann ist $(f \,;\, g) \colon M \to P$ injektiv nach Satz 5.2.3 und damit $|M| \leq |P|$. □

Es besteht jetzt eine natürliche Frage - ist die Relation $\leq$ auf Kardinalitäten total? D.h. wenn wir zwein Mengen M und N haben, gibt's immer eine Injektion $M \to N$ oder eine injektion $N \to M$?

Satz 7.2.7 (Satz von Hartogs, benutzt das Auswahlaxiom)**.** *Die Kardinalitäten $\mathcal{K}$ bilden eine total geordnete Menge $(\mathcal{K}, \leq)$*

Insbesondere man kann auch beweisen das $|\mathbb{N}|$ ist die kleinste unendliche Kardinalität, mnachmal auch $\aleph_0$ genannt. Wir sagen dass eine Menge M ist abzählbar gdw. $|M| \leq |\mathbb{N}|$; d. h. wenn sie höchstens die Kardinalität von $\mathbb{N}$ hat. Jede endliche Menge, $\mathbb{Z}$ und $\mathbb{Q}$ sind also abzählbar, aber $\mathbb{R}$ hingegen nicht. Echt mächtigere Mengen nennen wir auch überabzählbar.



Gibt es unendlich viele unendliche Kardinalitäten?

Satz 7.2.8 (Cantor)**.** *Für jede Menge M gelten $|M| \leq |\mathcal{P}(M)|$ und $|M| \neq |\mathcal{P}(M)|$.*

Beweis. Sei $f\colon M \to \mathcal{P}(M)$, so dass $f(m) = \{m\}$. Da f injektiv ist, gilt $|M| \leq |\mathcal{P}(M)|$.

Wir zeigen nun $|M| \neq |\mathcal{P}(M)|$ indirekt. Sei also $|M| = |\mathcal{P}(M)|$. Damit existiert eine bijektive Funktion $g\colon M \to \mathcal{P}(M)$. Ferner sei

$$X = \big\{x \in M \mid x \notin g(x)\big\} \ .$$

Da g surjektiv ist, existiert $m \in M$, so dass $g(m) = X$.
Es gilt folglich $m \in g(m) = X$ gdw. $m \notin g(m)$. Widerspruch! □

Es gibt also unendlich viele unendliche Kardinalitäten:

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \cdots{}^{1}$$

7.3 Kontinuum und Kontinuumshypothese

Die Kardinalität $|\mathbb{R}|$ nennt man auch Kontinuum und bezeichnet man sie mit dem Symbol $\mathfrak{c}$.

Gibt es Kardinalitäten zwischen $\aleph_0 = |\mathbb{N}|$ und $\mathfrak{c} = |\mathbb{R}|$? Ein Kandidat wäre das reelle Intervall $(0, 1)$.

Satz 7.3.1. *Es gilt $|(0,1)| = |\mathbb{R}|$ mit $(0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$.*

Beweis. Die Funktion $f\colon (0,1) \to \mathbb{R}$ mit $f(x) = \tan(\pi x - \frac{\pi}{2})$ für alle $x \in (0,1)$ ist bijektiv. Wir verzichten auf den Beweis der Bijektivität. □

Eine weiterer Kandidat wäre die Potenzmenge von $\mathbb{N}$.

Satz 7.3.2 (Cantor 1874)**.** *Es gilt $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.*

Wir kodieren reelle Zahlen wie $\frac{\pi}{10} = 0,31415927\cdots$ als

$$f(\tfrac{\pi}{10}) = \{3,\ 31,\ 314,\ 3.141,\ 31.415,\ 314.159,\ 3.141.592,\ 31.415.926, \dots\}.$$

Umgekehrt kodieren wir Mengen wie $G = \{0,\ 2,\ 4,\ 6,\ \dots\}$ als

$$g(G) = 0,15050505\cdots,$$

in der genau an den geraden Stellen hinter dem Komma die Ziffer 5 vorkommt.

[1] Dabei steht $m < m'$ für $m \leq m'$ und $m \neq m'$.

Beweis. Wir wissen bereits, dass $|\mathbb{R}| = |(0,1)|$. Wir konstruieren zwei injektive Funktionen $f\colon (0,1) \to \mathcal{P}(\mathbb{N})$ und $g\colon \mathcal{P}(\mathbb{N}) \to (0,1)$ und verwenden dann Cantor-Schröder-Bernstein.

- Jede reelle Zahl $x \in (0,1)$ lässt sich eindeutig als $x = [0, d_1 d_2 d_3 d_4 \cdots]_{10}$ mit den Ziffern $d_1, d_2, \ldots \in \{0, 1, \ldots, 9\}$ darstellen, so dass kein $n \in \mathbb{N}$ existiert mit $d_i = 9$ für alle $i \in \mathbb{N}$ mit $i \geq n$. Dann sei $f(x) := \{[d_1]_{10}, [d_1 d_2]_{10}, [d_1 d_2 d_3]_{10}, \ldots\}$. Diese Funktion f ist offenbar injektiv.
- Sei $X \subseteq \mathbb{N}$. Wir konstruieren die reelle Zahl $g(X) = [0, 1 b_0 b_1 b_2 \cdots]_{10}$ mit $b_i \in \{0, 5\}$, so dass $b_i = 5$ gdw. $i \in X$ für alle $i \in \mathbb{N}$. Offenbar ist auch diese Funktion g injektiv. □

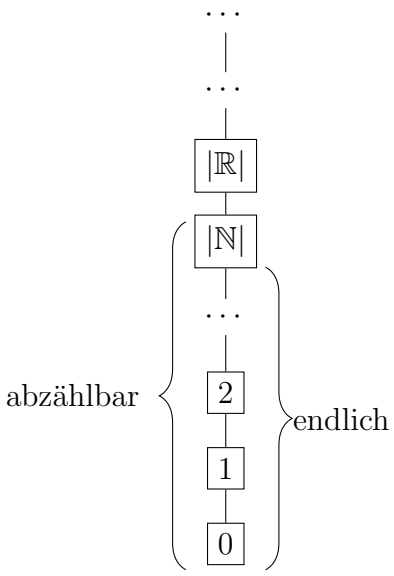
Es scheint schwer zu sein eine Menge M mit $|\mathbb{N}| < M < |\mathbb{R}|$ zu finden. Dies brachte Georg Cantor in 1878 dazu, die folgende Frage zu stellen, die als "Kontinu- umshypothese" bekannt ist: Ist es wahr, dass eine Menge A von reellen Zahlen entweder die gleiche Anzahl von Elementen hat wie die gesamte relle Linie R, oder die gleiche Anzahl von Elementen hat wie die natürlichen Zahlen N?

In den folgenden Jahrzehnten wurde diese Frage als eine der dringendsten mathematischen Fragen betrachtet. David Hilbert setzte sie im Jahr 1900 an die Spitze seiner Liste der wichtigsten offenen Probleme. Wie sich herausstellte, verfügte die Mathematik damals einfach nicht über die notwendigen Werkzeuge und das nötige Verständnis, um diese Frage zu beantworten. Auch heute noch wird die Antwort auf diese Frage häufig missverstanden.

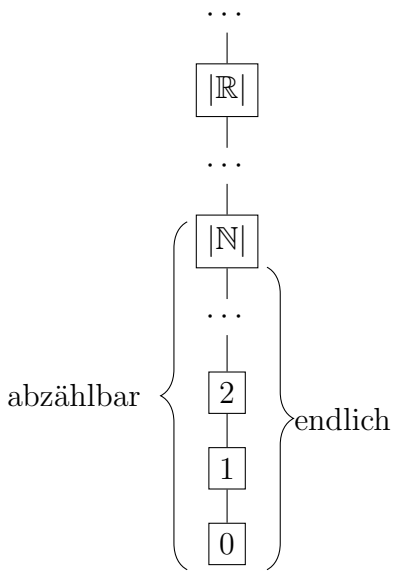
Heute wissen wir dank der gemeinsamen Arbeit von Kurt Gödel aus den 1940er Jahren und Paul Cohen aus den 1960er Jahren, dass diese Frage unmöglich zu beantworten ist. (man sagt dass CH "unabhängig von dem ZFC-Aziomssytem ist).

Der Grund dafürist, ganz informell gesprochen, dass es trotz der genauen mathematischen Definition der reellen Linie verschiedene Modelle der reellen Linie und ihrer Teilmengen gibt, in denen die Antwort auf die Kontinuumshypothese entweder wahr oder falsch ist. Es besteht die entfernte Möglichkeit (so gennante "Dream Solution"), dass es bessere mathematische Definitionen gibt, die genau beschreiben, woran (alle? die meisten?) Mathematiker denken, wenn sie an die reelle Linie und ihre Teilmengen denken. Dies scheint eine Überzeugung zu sein, die Kurt Gödel manchmal äußerte. In der Zwischenzeit fragen sich Mathematiker manchmal halb spaßhaft, ob sie "an die Kontinuumshypothese glauben".

Kontinuumshypothese gilt:



Kontinuumshypothese gilt nicht:



Kapitel 8

Verbände

8.1 Verbände

Wir betrachten in diesem Kapitel eine spezielle Form geodneter Mengen mit interessanten Eigenschaften. Sei $(M, \preceq)$ eine teilweise geordnete Menge und $X \subseteq M$. Das Supremum $\sup X$ von X ist das kleinste Element von $\uparrow X$, also die kleinste obere Schranke für X. Das Infimum $\inf X$ von X ist das größte Element von $\downarrow X$, also die größte untere Schranke für X. Sollten solche Schranken nicht existieren, dann existiert auch das entsprechende Supremum oder Infimum nicht.

Beispiel 8.1.1. *Wir betrachten* $\big(\mathcal{P}(\{1,2,3\}), \subseteq\big)$.

- *Das Supremum von* $\big\{\{2\}\big\}$ *ist* $\{2\}$, *es gilt* $\sup\big\{\{2\}\big\} = \{2\}$.
- *Es gilt* $\sup\big\{\{1\}, \{2\}\big\} = \{1, 2\}$.

Für eine Menge M ist $\mathcal{P}(M)$ die Menge aller Teilmengen von M. Eine Menge $\mathcal{M} \subseteq \mathcal{P}(M)$ enthält demnach einige Teilmengen von M. Wir nennen $\mathcal{M}$ Mengensystem über M. Jedes Mengensystem bildet anhand der üblichen Teilmengenbeziehung die teilweise geordnete Menge $(\mathcal{M}, \subseteq)$. Bildet man die Vereinigung von Elementen des Mengensystems $X \subseteq \mathcal{M}$, so erhält man eine Teilmenge $\bigcup X \in \mathcal{P}(M)$, die ihrerseits auch wieder ein Element von $\mathcal{M}$ sein kann, aber nicht muss. In jedem Fall liefert die Vereinigung das Supremum des Mengensystems.

Satz 8.1.2. *Wir betrachten die teilweise geordnete Menge* $(\mathcal{M}, \subseteq)$ *mit* $\mathcal{M} \subseteq \mathcal{P}(M)$ *für eine Menge* M. *Für jede Teilmenge* $X \subseteq \mathcal{M}$ *mit* $\bigcup X \in \mathcal{M}$ *gilt* $\bigcup X = \sup X$.

Beweis. Wir zeigen zunächst, dass $\bigcup X$ eine obere Schranke für X ist. Sei $Y \in X$ beliebig. Dann gilt $Y \subseteq \bigcup X$, womit $\bigcup X$ obere Schranke ist. Nach Lemma 6.1.2 ist

$\bigcup X$ die kleinste obere Schranke. Also ist $\bigcup X$ das Supremum von X. □

Die Verbindung von Supremum und Mengenvereinigung motiviert die folgende Schreibweise. Wir schreiben $m_1 \vee m_2$ statt $\sup\{m_1, m_2\}$ und $m_1 \wedge m_2$ statt $\inf\{m_1, m_2\}$. Eine teilweise geordnete Menge $(M, \preceq)$ heißt Verband gdw. für alle $m_1, m_2 \in M$ das Supremum von $\{m_1, m_2\}$ und das Infimum von $\{m_1, m_2\}$ existieren. Weiterhin heißt $(M, \preceq)$ vollständiger Verband gdw. sogar die Suprema und Infima beliebiger Teilmengen $X \subseteq M$ existieren. Jeder vollständige Verband enthält das größte Element $\inf \emptyset$ in M und das kleinste Element $\sup \emptyset$ in M.

Beispiele 8.1.3.

- *Die teilweise geordnete Menge* $\big(\{0, 1\}, R\big)$ *mit* $R = \big\{(0,0), (0,1), (1,1)\big\}$ *ist ein vollständiger Verband mit*
  - $\sup B = 1$ *gdw.* $1 \in B$,
  - $\inf B = 1$ *gdw.* $0 \notin B$,

  dem größten Element 1 *und dem kleinsten Element* 0.
- *Die teilweise geordnete Menge* $\big(\mathcal{P}(M), \subseteq\big)$ *ist für jede Menge* M *ein vollständiger Verband mit*
  - $\sup X = \bigcup X$,
  - $\inf X = \bigcap X$,

  dem größten Element M *und dem kleinsten Element* $\emptyset$.

Ein Verband $(M, \preceq)$ ist distributiv gdw. für alle $m_1, m_2, m_3 \in M$

$$m_1 \wedge (m_2 \vee m_3) = (m_1 \wedge m_2) \vee (m_1 \wedge m_3)$$
$$m_1 \vee (m_2 \wedge m_3) = (m_1 \vee m_2) \wedge (m_1 \vee m_3)$$

gelten.

Beispiele 8.1.4.

- *Die teilweise geordnete Menge* $\big(\{0, 1\}, R\big)$ *mit* $R = \big\{(0,0), (0,1), (1,1)\big\}$ *ist ein vollständiger und distributiver Verband.*
- *Die teilweise geordnete Menge* $\big(\mathcal{P}(M), \subseteq\big)$ *ist für jede Menge* M *ein vollständiger und distributiver Verband.*

Bekannte Beispiele geordneter Mengen sind außerdem $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ und $(\mathbb{R}, \leq)$. Es handelt sich nicht um vollständige Verbände, denn $\sup \mathbb{N}$ existiert nicht. Dennoch erlaubt ihre charakteristische Ordnungsstruktur eine Einordnung als Verbände.

Satz 8.1.5. *Jede total geordnete Menge $(M, \preceq)$ ist ein distributiver Verband.*

Beweis. Wir müssen die Eigenschaften eines Verbandes und die Distributivität beweisen.

- Supremum: Für alle $x, y \in M$ gilt entweder $x \preceq y$ oder $y \preceq x$ (Vollständigkeit). Ohne Beschränkung der Allgemeinheit (oBdA) sei $x \preceq y$. Dann ist y obere Schranke für $\{x, y\}$. Sei z eine beliebige obere Schranke für $\{x, y\}$. Dann gilt $y \preceq z$ und damit ist y die kleinste obere Schranke für $\{x, y\}$.
- Infimum: Analog.
- Distributivität: Seien $x, y, z \in M$. Seien $m = (x \wedge y) \vee (x \wedge z)$ und $m' = (x \vee y) \wedge (x \vee z)$.

Ordnung	$x \wedge (y \vee z)$	m	$x \vee (y \wedge z)$	m'
$x \preceq y \preceq z$	x	x	y	y
$x \preceq z \preceq y$	x	x	z	z
$y \preceq x \preceq z$	x	x	x	x
$y \preceq z \preceq x$	z	z	x	x
$z \preceq x \preceq y$	x	x	x	x
$z \preceq y \preceq x$	y	y	x	x

□

Wir beweisen jetzt die Tatsache, dass die Existenz der Suprema von je zwei Elementen auch die Existenz von Suprema endlich vieler Elemente (außer 0) bedeutet.

Satz 8.1.6. *Jeder endliche Verband ist vollständig.*

Beweis. Sei $(M, \preceq)$ ein Verband. Wir beweisen durch Induktion über $n = |X|$: Für jede endliche nicht-leere Teilmenge $X \subseteq M$ existiert $\sup X$. Der Beweis bezüglich $\inf X$ geht analog.

- Induktionsanfang: Sei $n = 1 = |X|$ und $x \in X$. Dann ist $x \preceq x$ und für alle oberen Schranken z von X gilt offenbar $x \preceq z$. Also ist $x = \sup X$.
- Induktionsschritt: Sei $n \in \mathbb{N}_+$ beliebig.
  - Induktionshypothese: Für jedes $X \subseteq M$ mit $|X| = n$ existiert $\sup X$.
  - Induktionsbehauptung: Für jedes $X \subseteq M$ mit $|X| = n+1$ existiert $\sup X$.

  Sei $X \subseteq M$ mit $|X| = n + 1$ und $z \in X$. Gemäß Induktionshypothese existiert

ein $y = \sup\big(X \setminus \{z\}\big)$. Wir zeigen, dass $z \vee y = \sup X$.

Es gilt $x \preceq z \vee y$ für alle $x \in X$ (da $z \preceq z \vee y$ und $x \preceq y \preceq z \vee y$ für alle $x \in X \setminus \{z\}$). Sei $m \in M$, so dass $x \preceq m$ für alle $x \in X$. Also auch $z \preceq m$ und $y \preceq m$. Damit allerdings auch $z \vee y \preceq m$. □

8.2 Charakterisierung von Verbänden mit Hilfe der Operationen $\vee$ und $\wedge$

In Verbänden kann man mit Suprema und Infima auf naheliegende Weise rechnen. Dabei gelten einige bekannte Rechengesetze.

Satz 8.2.1. *Für jeden Verband $(M, \preceq)$ und alle $x, y, z \in M$ gelten*

- $x \vee y = y \vee x$ *und* $x \wedge y = y \wedge x$ — *Kommutativität*
- $x \vee (y \vee z) = (x \vee y) \vee z$ *und* $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ — *Assoziativität*
- $x \vee (x \wedge y) = x$ *und* $x \wedge (x \vee y) = x$ — *Absorption*

Der Beweis bleibt dem Leser überlassen. Es ist ein klassischer Resultat, der wir jetzt besprechen, dass die obene Eigenschaften reichen um die Ordnungsrelationen wiederzuherstellen. Jetzt besprechen wir das im Detail.

Satz 8.2.2. *Sei $(M, \sqcup, \sqcap)$ eine Menge zusammen mit swei Funktionen $\sqcup, \sqcap\colon M \times M \to M$, so dass für alle $x, y, z \in M$ das Folgende gilt:*

- $x \sqcup y = y \sqcup x$ *und* $x \sqcap y = y \sqcap x$ — *(Kommutativität)*
- $x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$ *und* $x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z$ — *(Assoziativität)*
- $x \sqcup (x \sqcap y) = x$ *und* $x \sqcap (x \sqcup y) = x$ — *(Absorption)*

Dann ist $(M, \preceq)$ ein Verband, wobei wir definieren $x \preceq y$ gdw. $x = x \sqcap y$. Außerdem gilt in diesem Verband dass $x \vee y = x \sqcap y$ und $x \wedge y = x \sqcup y$.

Beweis. Für alle $x, y \in M$ ist also $x \preceq y$ gdw. $x = x \sqcap y$. Wir weisen zunächst die Eigenschaften einer Ordnungsrelation nach.

- Reflexivität: Für jedes $x \in M$ gilt nach zweimaligem Anwenden der Absorption

$$x = x \sqcap \big(x \sqcup (x \sqcap x)\big) = x \sqcap x \ ,$$

  also $x \preceq x$.

- Antisymmetrie: Seien $x \preceq y$ und $y \preceq x$. Es gelten $x = x \sqcap y$ und $y = y \sqcap x$. Mit

Hilfe der Kommutativität gilt dann

$$x = x \sqcap y = y \sqcap x = y \ .$$

- Transitivität: Seien $x \preceq y$ und $y \preceq z$. Es gelten $x = x \sqcap y$ und $y = y \sqcap z$. Unter Nutzung der Assoziativität erhalten wir

$$x = x \sqcap y = x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z = x \sqcap z$$

und damit $x \preceq z$.

Wir weisen nun noch die Existenz der Suprema (Infima analog) nach. Seien $x, y \in M$. Wir behaupten, dass $x \sqcup y$ das Supremum von $\{x, y\}$ ist.

- Obere Schranke: Es gilt $x = x \sqcap (x \sqcup y)$ und damit $x \preceq x \sqcup y$. Ebenso gilt $y = y \sqcap (y \sqcup x)$ und damit $y \preceq x \sqcup y$, da $y \sqcup x = x \sqcup y$.
- Kleinste obere Schranke: Sei $z \in M$ mit $x \preceq z$ und $y \preceq z$, also $x = x \sqcap z$ und $y = y \sqcap z$. Wir folgern zunächst mit Absorption und Kommutativität

$$\begin{aligned} x \sqcup z &= (x \sqcap z) \sqcup z = z \quad \text{und} \\ y \sqcup z &= (y \sqcap z) \sqcup z = z \ . \end{aligned}$$

Damit ergibt sich nun

$$\begin{aligned} (x \sqcup y) \sqcap z &= (x \sqcup y) \sqcap (x \sqcup z) \\ &= (x \sqcup y) \sqcap (x \sqcup (y \sqcup z)) \\ &= (x \sqcup y) \sqcap ((x \sqcup y) \sqcup z) = (x \sqcup y) \end{aligned}$$

und damit $(x \sqcup y) \preceq z$. □

Im Licht des obigen Satzes können wir Verbände auf zwei äquivalente Weise betrachten: als eine geordnete Menge $(M, \leq)$ mit der Eigenschaft dass infima und suprema existieren, oder als eine Menge $(M, \vee, \wedge)$ mit zwei Operationen die kommutativ, assoziativ und absorptiv sind. Deswegen manchmal definiert man sogarder Begriff Verband als so eine Menge mit zwei Operationen.

8.3 Distributivität von Verbänden

Die Klasse der distributiven Verbände ist für die Anwendungen in der Informatik besonders interessant. Die Überprüfung eines Verbandes auf diese Eigenschaft durch Nachrechnen ist jedoch mühsam. Deshalb werden wir in diesem Abschnitt ein hilfreiches Distributivitätskriterium etablieren.

Sei $(V, \vee, \wedge)$ ein Verband. Ein Unterverband ist eine Menge $W \subset V$ mit der Eigenschaft

dass für alle $x, y \in W$ haben wir $x \vee y \in W$ und $x \wedge y \in W$.

Beispiel 8.3.1. *Die Menge* $\{\emptyset, \{1\}, \{1,2\}, \{1,2,3\}\}$ *ist ein Unterverband von* $\mathcal{P}(\{\infty, \in, \ni\})$, *und die Menge* $\mathcal{M} := \{\emptyset, \{\infty\}, \{\infty, \in\}, \{\ni\}, \{\infty, \in, \ni\}\}$ *ist kein Unterverband davon, da* $\{1\} \wedge \{3\} = \{1,3\} \notin \mathcal{M}$.

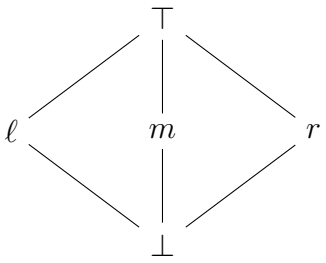
Es ist zu bemerken dass die Menge $\mathcal{M}$ *wird zu einem Verband, wenn wir sie zusammen mit der Teilmengerelation betrachten. Trotzdem, wie oben geschrieben, dieser Verband ist kein Unterverband von* $\mathcal{P}(\{\infty, \in, \ni\})$.

Wir sagen dass zwei Verbände $(V, \vee, \wedge)$ und $(V', \vee', \wedge')$ sind isomorph gdw. es eine bijektion $\phi\colon V \to V'$ gibt mit der Eigenschaft dass für all $x, y \in V$ haben wir $\phi(x \vee y) = \phi(x) \vee' \phi(y)$ und $\phi(x \wedge y) = \phi(x) \wedge' \phi(y)$.

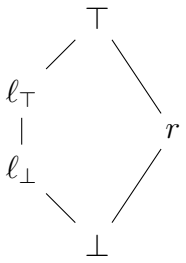
Bemerkung 8.3.2. (a) Äquivalent gesagt, zwei Verbände $(V, \leq)$ und $(V', \geq)$ sind isomporh gdw. es eine bijektion $\phi\colon V \to V'$ gibt mit der Eigenschaft dass für alle $x, y \in V$ haben wir $x \leq y \iff \phi(x) \leq' \phi(y)$.

(b) Noch anders, äquivalent, gesagt, zwei Verbände sind isomorph, wenn sie "gleiche" Hasse-diagramme haben, wobei "gleiche" bedeutet dass der einzig mögliche Unterschied sind die Namen von Knoten.

Hier sind zwei Beispiel von Verbände die nicht distributiv sind, gegeben durch seine Hasse-dagramme.



M_3



N_5

Dass diese Verbände nicht distributiv sind, sehen wir jeweils mit konkreten Beispielen. Im Fall von M_3 haben wir $\ell \vee (m \wedge r) = l$ und $(\ell \vee m) \wedge (\ell \vee r) = \top$. Im Fall von N_5 haben wir $\ell_\top \wedge (\ell_\bot \vee r) = \ell_\top$ und $(\ell_\top \wedge \ell_\bot) \vee (\ell_\top \wedge r) = \ell_\bot$.

Satz 8.3.3 (Charakterisierung Distributivität)**.** *Sei* $\mathcal{V} = (V, \vee, \wedge)$ *ein Verband. Dann ist* $\mathcal{V}$ *distributiv gdw. kein Unterverband von* $\mathcal{V}$ *isomorph zu den Verbänden* M_3 *oder* N_5 *ist.*

Beweisskizze. Nehmen wir erst an, dass es gibt ein Unterverband von $\mathcal{V}$, der entweder zu M_3 oder zu N_5 isomorph ist.

Sei $U \subseteq V$ eine Teilmenge, die ein Unterverband von V ist, und der isomorph zu M_3 ist. Sei $\phi\colon V \to M_3$ ein Isomorphismus. Seien $x := \phi^{-1}(\ell)$, $y := \phi^{-1}(m)$, $z := \phi^{-1}(r)$. Wir sehen jetzt dass

$$x \vee (y \wedge z) \neq (x \vee y) \wedge (x \vee z)$$

In der Tat,

$$\phi(x \vee (y \wedge z)) = \ell \vee (m \wedge r) = \ell$$

und

$$\phi((x \vee y) \wedge (x \vee z)) = (\ell \vee m) \wedge (\ell \vee r) = \top.$$

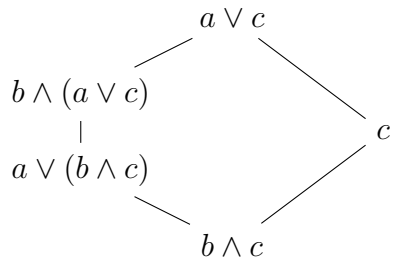
Also in diesem Fall sehen wir dass $\mathcal{V}$ nicht-distributiv ist. Analog beweisen wir dass wenn U isomorph zu N_5 ist dann auch $\mathcal{V}$ nicht isomorph ist.

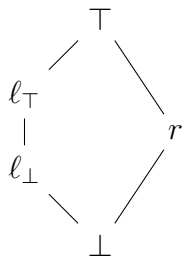
Umgekehrt sei $\mathcal{V}$ nicht distributiv. Wir zeigen, dass $\mathcal{V}$ dann eine zu M_3 oder N_5 isomorphe Unterverband hat.

Fall 1: Es existieren $a, b, c \in V$ mit $a \preceq b$ und

$$a \vee (b \wedge c) \neq (a \vee b) \wedge (a \vee c) = b \wedge (a \vee c) \ .$$

Es folgt, dass das linke Hasse-Diagramm eine Unterstruktur von $\mathcal{V}$ ist (viel Nachrechnen). Der Isomorphismus zu N_5 ist offensichtlich.





Beispiele vom Nachrechnen (nicht vollständig) - Details sind in [BS] zu finden:

- Partielle Ordnung: Wir zeigen $a \vee (b \wedge c) \preceq b \wedge (a \vee c)$. Da $a \preceq b$ und $b \wedge c \preceq b$ gilt auch $a \vee (b \wedge c) \preceq b$. Weiterhin gelten $a \preceq a \vee c$ und $b \wedge c \preceq c \preceq a \vee c$ und damit $a \vee (b \wedge c) \preceq a \vee c$. Aus den beiden Aussagen $a \vee (b \wedge c) \preceq b$ und $a \vee (b \wedge c) \preceq a \vee c$ folgt nun direkt $a \vee (b \wedge c) \preceq b \wedge (a \vee c)$.

- Suprema und Infima: Wir zeigen $\big(b \wedge (a \vee c)\big) \vee c = a \vee c$. Da $a \preceq b$ und $a \preceq a \vee c$ gelten auch $a \preceq b \wedge (a \vee c)$ und $a \vee c \preceq \big(b \wedge (a \vee c)\big) \vee c$. Für die umgekehrte Richtung gilt $(b \wedge (a \vee c)) \vee c \preceq a \vee c \vee c = a \vee c$.

- Ungleichheit: Wir zeigen $a \vee (b \wedge c) \neq b \wedge c$. Sei $a \vee (b \wedge c) = b \wedge c$. Also $a \preceq b \wedge c \preceq c$, womit $a \vee (b \wedge c) = b \wedge c = b \wedge (a \vee c)$ im Widerspruch zur Annahme gilt.

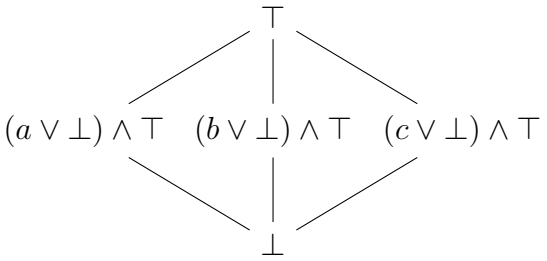
Fall 2: Für alle $x, y, z \in V$ mit $x \preceq y$ gilt $x \vee (y \wedge z) = y \wedge (x \vee z)$. Trotzdem existieren $a, b, c \in V$, so dass

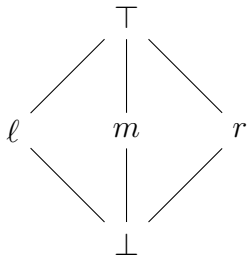
$$a \vee (b \wedge c) \neq (a \vee b) \wedge (a \vee c) \ .$$

Es folgt, dass das linke Hasse-Diagramm mit

$$\bot = (a \wedge b) \vee (a \wedge c) \vee (b \wedge c)$$
$$\top = (a \vee b) \wedge (a \vee c) \wedge (b \vee c)$$

eine Unterstruktur von $\mathcal{V}$ ist (noch mehr Nachrechnen). Der Isomorphismus zu M_3 ist offensichtlich.





□

Kapitel 9

Allgemeine algebraische Strukturen

9.1 Strukturbegriff

Zuletzt haben wir über teilweise geordnete Mengen und Verbände gesprochen. Dabei haben wir jeweils eine Menge und eine Relation zu einer Einheit zusammengefasst. Eine Einheit aus einer Menge U und Relationen, Funktionen, und Konstanten, die U gewissermaßen strukturell anreichern, nennen wir algebraische Struktur. Sei U eine Grundmenge und seien

- $R_1, \dots, R_k \subseteq U \times U$ Relationen auf U,
- $f_1, \dots, f_\ell \colon U \times U \to U$ binäre (zweistellige) Funktionen auf U,
- $g_1, \dots, g_m \colon U \to U$ unäre (einstellige) Funktionen auf U und
- $c_1, \dots, c_n \in U$ Elemente (auch: Konstanten) von U.

Dann ist $\big(U, \langle R_1, \dots, R_k\rangle, \langle f_1, \dots, f_\ell\rangle, \langle g_1, \dots, g_m\rangle, \langle c_1, \dots, c_n\rangle\big)$ eine algebraische Struktur des Typs (k, ℓ, m, n). Wir betrachten nur binäre und unäre Funktionen und Relationen. Dabei ist die Reihenfolge im Typ:

1. Anzahl Relationen
2. Anzahl binärer Funktionen
3. Anzahl unärer Funktionen
4. Anzahl Konstanten

In der Praxis entfällt oft die Gruppierung der Strukturkomponenten.

Beispiele 9.1.1.

- *Das „System“* $(\mathbb{N}, \mathit{nachfolger}, 0)$ *ist eine algebraische Struktur des Typs* $(0, 0, 1, 1)$ *mit*
  - *einer Funktion nachfolger*: $\mathbb{N} \to \mathbb{N}$ *und*

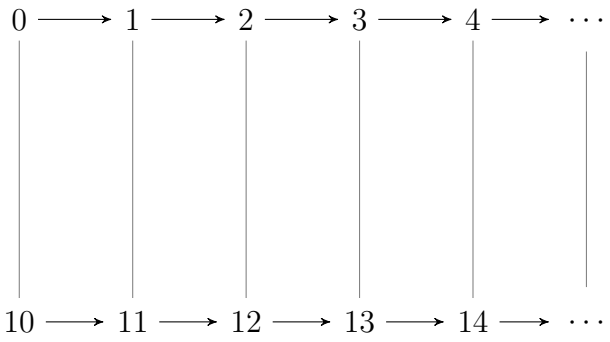
– *einer Konstante* $0 \in \mathbb{N}$.

- *Die Peano-Axiome spezifizieren algebraische Strukturen* (N, s, z) *des Typs* $(0, 0, 1, 1)$ *mit einer Funktion* $s\colon N \to N$ *und einer Konstante* $z \in N$.
- *Jede Äquivalenzrelation* $\equiv$ *auf* M *liefert eine algebraische Struktur* $\big(M, \langle\equiv\rangle, \langle\rangle, \langle\rangle, \langle\rangle\big)$ *des Typs* $(1,\ 0,\ 0,\ 0)$.
- *Jede teilweise geordnete Menge* $(M, \preceq)$ *mit einer Relation* $\preceq\ \subseteq M \times M$ *ist eine algebraische Struktur des Typs* $(1, 0, 0, 0)$.
- *Die Wahrheitswerte liefern eine algebraische Struktur* $\big(\{0,\ 1\}, \langle\rangle, \langle\vee,\ \wedge\rangle, \langle\neg\rangle, \langle 0,\ 1\rangle\big)$ *des Typs* $(0,\ 2,\ 1,\ 2)$.
- *Jede Potenzmenge* $\mathcal{P}(M)$ *liefert eine algebraische Struktur* $\big(\mathcal{P}(M), \subseteq, \cup, \cap, \cdot^c, \emptyset, M\big)$ *des Typs* $(1, 2, 1, 2)$.

9.2 Isomorphie

Wir haben bereits beobachtet, dass sich zwei Strukturen sehr ähnlich sein können. Beispielsweise haben wir festgestellt, dass zwischen den Äquivalenzrelationen auf einer Menge M und den Zerlegungen von M eine gewisse Korrespondenz besteht. Kennzeichnend für diese Korrespondenz ist die Tatsache, dass sich Äquivalenzrelationen und Zerlegungen bijektiv aufeinander abbilden lassen. Eine weitere Form der Ähnlichkeit ist die Isomorphie zweier algebraischer Strukturen gleichen Typs. Sie liegt vor, wenn beide Strukturen bis auf Umbenennung ihrer Elemente gleich sind. In isomorphen Strukturen funktioniert das Rechnen also auf dieselbe Weise und die Elemente stehen in den gleichen Relationen (z.B. sind auf die gleiche Weise angeordnet).

Beispiel 9.2.1. *Die Strukturen* $(\mathbb{N}, \leq)$ *und* $(\mathbb{N} \setminus \{0, \ldots, 9\}, \leq)$ *sind isomorph.*



Entsprechend dem Umbenennungsgedanken definieren wir die Isomorphie über die Existenz einer strukturerhaltenden Bijektion zwischen den algebraischen Strukturen. Seien

$$\mathcal{U} = \big(U, \langle R_1, \ldots, R_k\rangle, \langle f_1, \ldots, f_\ell\rangle, \langle g_1, \ldots, g_m\rangle, \langle c_1, \ldots, c_n\rangle\big)$$
$$\mathcal{U}' = \big(U', \langle R'_1, \ldots, R'_k\rangle, \langle f'_1, \ldots, f'_\ell\rangle, \langle g'_1, \ldots, g'_m\rangle, \langle c'_1, \ldots, c'_n\rangle\big)$$

zwei algebraische Strukturen gleichen Typs. Eine Funktion $\varphi\colon U \to U'$ heißt Isomorphismus von $\mathcal{U}$ nach $\mathcal{U}'$, falls

- φ bijektiv ist,
- für alle $1 \leq i \leq k$ und $u_1, u_2 \in U$ gilt

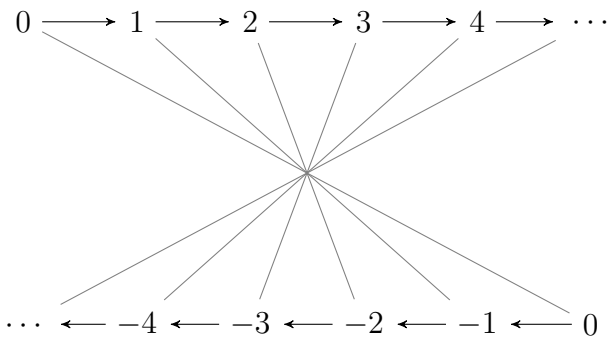
$$(u_1, u_2) \in R_i \text{ gdw. } \big(\varphi(u_1), \varphi(u_2)\big) \in R'_i$$

- für alle $1 \leq i \leq \ell$ und $u_1, u_2 \in U$ gilt

$$\varphi\big(f_i(u_1, u_2)\big) = f'_i\big(\varphi(u_1), \varphi(u_2)\big)$$

- $\varphi\big(g_i(u)\big) = g'_i\big(\varphi(u)\big)$ für alle $1 \leq i \leq m$ und $u \in U$,
- $\varphi(c_i) = c'_i$ für alle $1 \leq i \leq n$.

Die Strukturen $\mathcal{U}$ und $\mathcal{U}'$ heißen isomorph gdw. ein solcher Isomorphismus existiert. Es ist leicht nachzuweisen, dass die Isomorphie als eine Äquivalenzrelation auf den algebraischen Strukturen eines bestimmten Typs betrachtet werden kann.



Beispiele 9.2.2. *Die Strukturen* $\big(\mathbb{N}, \mathit{nachfolger}, 0\big)$ *und* $\big(\{z \in \mathbb{Z} \mid z \leq 0\}, g, 0\big)$ *mit*

$$g(z) = z - 1 \quad \textit{für alle } z \leq 0$$

sind isomorph vermittels

$$\varphi\colon \mathbb{N} \to \{z \in \mathbb{Z} \mid z \leq 0\} \qquad \varphi(n) = -n \quad \textit{für alle } n \in \mathbb{N}$$

denn φ ist bijektiv und es gelten sowohl $\varphi(0) = 0$ als auch

$$\varphi\big(\mathit{nachfolger}(n)\big) = \varphi(n+1) = -n - 1 = g(-n) = g\big(\varphi(n)\big) \ .$$

Nicht isomorph sind hingegen die Strukturen $(\mathbb{N}, \leq)$ und $\big(\{z \in \mathbb{Z} \mid z \leq 0\}, \leq\big)$. Sei φ Isomorphismus und $z = \varphi(0)$. Da $z - 1 \leq 0$ und φ bijektiv, existiert $n \in \mathbb{N} \setminus \{0\}$,

so dass $\varphi(n) = z - 1$. Es gilt $0 \leq n$, aber $\varphi(0) = z \not\leq z - 1 = \varphi(n)$ im Widerspruch zur Isomorphismus-Eigenschaft. Also existiert kein Isomorphismus zwischen $(\mathbb{N}, \leq)$ und $\big(\{z \in \mathbb{Z} \mid z \leq 0\}, \leq\big)$ und die Strukturen sind nicht isomorph.

Zur weiteren Illustration für die Beweisführung mit Isomorphmismen beweisen wir eine einfache Aussage über die rationalen Zahlen, die wir im Folgenden jedoch nicht benötigen werden. Der Beweis zeigt jedoch eine typische Herangehensweise zur Identifikation eines Isomorphismuses in isomorphen algebraischen Strukturen. Zunächst versucht man bzgl. der Operationen bzw. Relationen der algebraischen Strukturen ausgezeichnete Elemente zu finden (z.B. das kleinste Element einer Ordnungsrelation oder ein neutrales Element einer zweistelligen Operation wie im folgenden Beweis).

Satz 9.2.3. *Die Abbildung $\mathrm{id}_{\mathbb{Q}}$ ist der einzige Isomorphismus von und auf $(\mathbb{Q}, +, \cdot)$.*

Beweis. Trivialerweise ist $\mathrm{id}_{\mathbb{Q}}$ ein solcher Isomorphismus. Sei $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ ein Isomorphismus von und auf $(\mathbb{Q}, +, \cdot)$. Wir zeigen zunächst $\varphi(0) = 0$, $\varphi(1) = 1$ und $\varphi(-1) = -1$.

- Es gilt $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$. Es gibt nur eine Zahl $z \in \mathbb{Q}$, so dass $z = z + z$. Also $\varphi(0) = 0$. (neutrales Element der Addition)
- Es gilt $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$. Es gibt nur zwei Zahlen $z \in \mathbb{Q}$, so dass $z = z \cdot z$. Da $\varphi(0) = 0$ und φ injektiv ist, gilt also $\varphi(1) = 1$. (neutrales Element der Multiplikation)
- Es gilt $\varphi(1) = \varphi((-1) \cdot (-1)) = \varphi(-1) \cdot \varphi(-1)$. Es gibt nur zwei Zahlen $z \in \mathbb{Q}$, so dass $\varphi(1) = 1 = z \cdot z$. Da $\varphi(1) = 1$ und φ injektiv ist, gilt also $\varphi(-1) = -1$.

Für jedes $n \in \mathbb{N}$ gilt

$$\varphi(n) = \varphi(\underbrace{1 + \cdots + 1}_{n \text{ mal}}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{n \text{ mal}} = \underbrace{1 + \cdots + 1}_{n \text{ mal}} = n$$

Analoges gilt für alle $z \in \mathbb{Z}$ mit $z \leq 0$ unter Nutzung von -1.

Seien $m, n \in \mathbb{Z}$ mit $n > 0$. Zu zeigen: $\varphi(\frac{m}{n}) = \frac{m}{n}$. Es gilt

$$m = \varphi(m) = \varphi(\frac{m}{n} \cdot n) = \varphi(\frac{m}{n}) \cdot \varphi(n) = \varphi(\frac{m}{n}) \cdot n \ .$$

Diese Gleichung läßt sich eindeutig lösen und wir erhalten $\varphi(\frac{m}{n}) = \frac{m}{n}$. Also gilt $\varphi = \mathrm{id}_{\mathbb{Q}}$. □

9.3 Unterstrukturen

Kehren wir zum Strukturbegriff zurück. Seien

$$\mathcal{O} = \big(O, \langle R_1, \ldots, R_k\rangle, \langle f_1, \ldots, f_\ell\rangle, \langle g_1, \ldots, g_m\rangle, \langle c_1, \ldots, c_n\rangle\big)$$
$$\mathcal{U} = \big(U, \langle R'_1, \ldots, R'_k\rangle, \langle f'_1, \ldots, f'_\ell\rangle, \langle g'_1, \ldots, g'_m\rangle, \langle c'_1, \ldots, c'_n\rangle\big)$$

zwei algebraische Strukturen gleichen Typs. Dann ist $\mathcal{U}$ eine Unterstruktur von $\mathcal{O}$ gdw.

- $U \subseteq O$,
- für alle $1 \leq i \leq k$ und $u_1, u_2 \in U$ gilt

$$(u_1, u_2) \in R'_i \text{ gdw. } (u_1, u_2) \in R_i \ ,$$

- $f'_i(u_1, u_2) = f_i(u_1, u_2)$ für alle $1 \leq i \leq \ell$ und $u_1, u_2 \in U$,
- $g'_i(u) = g_i(u)$ für alle $1 \leq i \leq m$ und $u \in U$,
- $c'_i = c_i$ für alle $1 \leq i \leq n$.

Die Relationen, Funktionen und Konstanten der Oberstruktur $\mathcal{O}$ übertragen sich eingeschränkt auf U auf die Unterstruktur $\mathcal{U}$. Wir sagen daher $U \subseteq O$ bildet eine Unterstruktur, falls

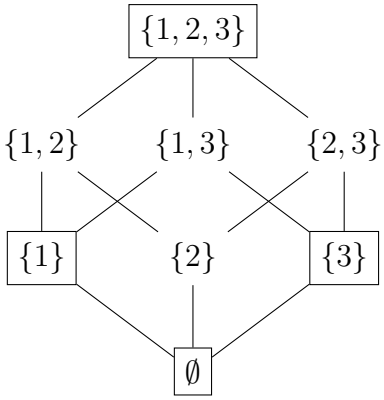
$$\big(U, \langle R'_1, \ldots, R'_k\rangle, \langle f'_1, \ldots, f'_\ell\rangle, \langle g'_1, \ldots, g'_m\rangle, \langle c_1, \ldots, c_n\rangle\big)$$

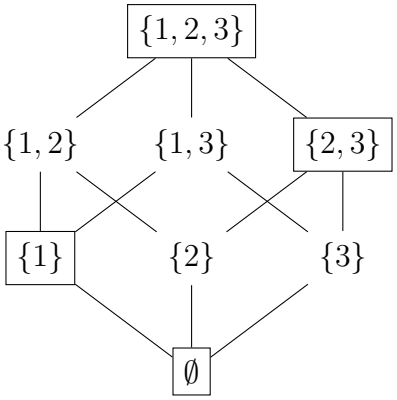
eine algebraische Struktur ist, wobei

- $R'_i = R_i \cap U^2$ für alle $1 \leq i \leq k$,
- $f'_i = f_i \cap U^3$ für alle $1 \leq i \leq \ell$,
- $g'_i = g_i \cap U^2$ für alle $1 \leq i \leq m$.

Beispiel 9.3.1. *Wir betrachten den Verband* $\mathcal{O} = \big(\mathcal{P}(\{1, 2, 3\}), \cup, \cap\big)$.

- *Die Teilmenge* $U = \big\{\emptyset, \{1\}, \{3\}, \{1, 2, 3\}\big\}$ *bildet keine Unterstruktur von* $\mathcal{O}$, *denn* $\{1\}, \{3\} \in U$, *aber* $\{1\} \cup \{3\} = \{1, 3\} \notin U$.
- *Die Teilmenge* $U' = \big\{\emptyset, \{1\}, \{2, 3\}, \{1, 2, 3\}\big\}$ *bildet eine Unterstruktur von* $\mathcal{O}$.


{1, 2, 3}
{1, 2}
{1, 3}
{2, 3}
{1}
{2}
{3}
∅


{1, 2, 3}
{1, 2}
{1, 3}
{2, 3}
{1}
{2}
{3}
∅

Kapitel 10

Boolesche Algebren

Wir werden die Klasse der distributiven Verbände noch weiter einschränken und so die für die Informatik extrem wichtige Strukturklasse der Booleschen Algebren[1] erhalten. Die Gemeinsamkeiten zwischen Mengen und Logik basieren wesentlich auf den Gesetzmäßigkeiten für Boolesche Algebren. In der Praxis sind Boolesche Algebren beispielsweise im Schaltungsentwurf und in der Wissensrepräsentation von Bedeutung.

Sei $(M, \preceq)$ ein Verband mit kleinstem Element $\bot$ und größtem Element $\top$ und sei $x \in M$. Ein Element $y \in M$ heißt Komplement von x gdw. $x \wedge y = \bot$ und $x \vee y = \top$. Der Verband $(M, \preceq)$ heißt komplementiert gdw. für jedes $x \in M$ ein Komplement $y \in M$ von x existiert. Die Komplemente sind im Allgemeinen in Verbänden nicht eindeutig. So hat das Element ℓ im Verband M_3 die Komplemente m und r (siehe Abbildung). Ein Verband $(M, \preceq)$ heißt Boolesche Algebra gdw. er sowohl komplementiert als auch distributiv ist und $\bot \neq \top$ gilt.

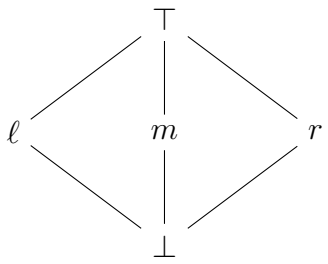


Abbildung 10.1: M_3

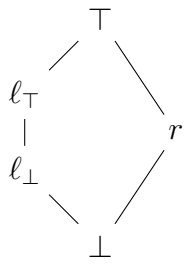


Abbildung 10.2: N_5

Satz 10.0.1. *Sei $(M, \preceq)$ ein distributiver Verband mit kleinstem Element $\bot$ und größtem Element $\top$. Für jedes $x \in M$ existiert höchstens ein Komplement von x.*

[1] George Boole (1815–1864)

Beweis. Sei $x \in M$ und seien $y, z \in M$ Komplemente von x.

- Wir zeigen $y = y \wedge z$

$$y = \top \wedge y = (x \vee z) \wedge y = (x \wedge y) \vee (z \wedge y) = \bot \vee (z \wedge y) = y \wedge z$$

- Ebenso $z = y \wedge z$

$$z = \top \wedge z = (x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z) = \bot \vee (y \wedge z) = y \wedge z$$

Also $y = y \wedge z = z$. □

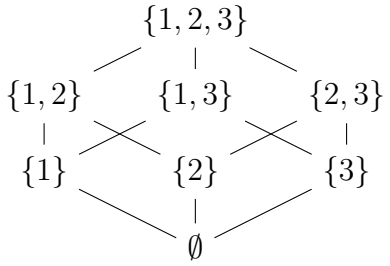
Beispiele 10.0.2.

- *Der Verband* $\big(\{0,\,1\}, \{(0,0),\,(0,1),\,(1,1)\}\big)$ *der Wahrheitswerte mit*
  - *kleinstem Element* 0*, größtem Element* 1*,*
  - *Supremum* $\vee$ *und Infimum* $\wedge$

  ist distributiv, da total geordnet. Für jedes $b \in \{0,\,1\}$ *gilt* $b \wedge \underbrace{(1-b)}_{\neg b} = 0$ *und* $b \vee \underbrace{(1-b)}_{\neg b} = 1$*. Also ist er auch komplementiert und damit Boolesche Algebra.*

- *Für jede Menge* M *ist* $\big(\mathcal{P}(M), \subseteq\big)$ *ein distributiver Verband mit*
  - *kleinstem Element* $\emptyset$*, größtem Element* M*,*
  - *Supremum* $\cup$ *und Infimum* $\cap$*.*

  Es gelten $M' \cap (M')^c = \emptyset$ *und* $M' \cup (M')^c = M$ *für jedes* $M' \in \mathcal{P}(M)$*. Also ist der Verband auch komplementiert und sogar eine Boolesche Algebra, falls* $M \neq \emptyset$*.*



- *Sei* $M \neq \emptyset$ *eine unendliche Menge und*

$$\mathcal{M} = \big\{X \in \mathcal{P}(M) \mid X \text{ endlich}\big\} \cup \big\{X \in \mathcal{P}(M) \mid M \setminus X \text{ endlich}\big\}$$

  Dann ist $\mathcal{M}$ *ein distributiver, unvollständiger Verband*
  - *mit kleinstem Element* $\emptyset$*, größtem Element* M*,*
  - *Supremum* $\cup$ *und Infimum* $\cap$*.*

Es gelten $M' \cap (M')^c = \emptyset$ und $M' \cup (M')^c = M$ für jedes $M' \in \mathcal{P}(M)$, also ist der Veband auch komplementiert und damit Boolesche Algebra.

Für eine Boolesche Algebra $\mathcal{M} = (M, \preceq)$ und $x \in M$ bezeichnen wir das Komplement von x häufig mit x^c. Die Boolesche Algebra $\mathcal{M}$ induziert also eine Abbildung $\cdot^c \colon M \to M$.

Satz 10.0.3. *Sei $(M, \preceq)$ eine Boolesche Algebra mit kleinstem Element $\bot$ und größtem Element $\top$. Dann gelten*

1. *$(x^c)^c = x$ für alle $x \in M$ und*
2. *$(x \wedge y)^c = x^c \vee y^c$ und $(x \vee y)^c = x^c \wedge y^c$ für alle $x, y \in M$.*

Beweis.

1. Per Definition ist $(x^c)^c$ das Komplement von x^c. Aufgrund der Kommutativität von $\wedge$ und $\vee$ ist x auch Komplement von x^c. Da das Komplement eindeutig ist gilt $x = (x^c)^c$.
2. Wir zeigen, dass $(x \vee y) \wedge (x^c \wedge y^c) = \bot$ und $(x \vee y) \vee (x^c \wedge y^c) = \top$. Aufgrund der Eindeutigkeit des Komplements ist dann $(x \vee y)^c = x^c \wedge y^c$. Es gilt

$$\begin{aligned}(x \vee y) \wedge (x^c \wedge y^c) &= (x \wedge x^c \wedge y^c) \vee (y \wedge x^c \wedge y^c) \\ &= (\bot \wedge y^c) \vee (\bot \wedge x^c) = \bot \vee \bot = \bot \ .\end{aligned}$$

   Analog rechnen wir die zweite Gleichheit

$$\begin{aligned}(x \vee y) \vee (x^c \wedge y^c) &= (x \vee y \vee x^c) \wedge (x \vee y \vee y^c) \\ &= (\top \vee y) \vee (\top \vee x) = \top \vee \top = \top \ .\end{aligned}$$

   Ebenso für das zweite De Morgansche Gesetz. □

Auch Boolesche Algebren lassen sich operational charakterisieren.

Satz 10.0.4. *Sei $(M, \sqcap, \sqcup, \cdot^*, \bot, \top)$ eine algebraische Struktur des Typs $(0, 2, 1, 2)$, so dass*

- *$\sqcap$ und $\sqcup$ assoziativ, kommutativ, distributiv und absorptiv sind und*
- *$\cdot^*$ jedes Element $x \in M$ auf sein Komplement abbildet:*

$$x \sqcap x^* = \bot \qquad \text{und} \qquad x \sqcup x^* = \top \ .$$

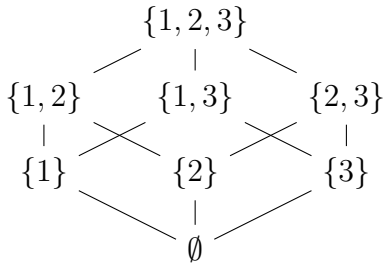
Dann ist $(M, \preceq)$ mit $x \preceq y$ gdw. $x = x \sqcap y$ eine Boolesche Algebra.

Wir wollen die Struktur von Booleschen Algebren genauer untersuchen. Zunächst adaptieren wir das Konzept der logischen Atome. Sei $(M, \preceq)$ eine Boolesche Algebra mit kleinstem Element $\bot$. Ein Element $x \in M \setminus \{\bot\}$ ist ein Atom gdw. $y \in \{\bot, x\}$ für alle $y \in M$ mit $y \preceq x$ gilt. Atome sind also die direkten Nachbarn des kleinsten Elements $\bot$ im Hasse-Diagramm und die minimalen Elemente in $M \setminus \{\bot\}$.

Beispiele 10.0.5.

- *Boolesche Algebra der Wahrheitswerte hat nur das Atom* 1.

- *Potenzmenge von* $M = \{1, 2, 3\}$ *hat die Atome* $\{1\}$, $\{2\}$ *und* $\{3\}$.



Wir fassen typische Eigenschaften von Atomen in dem folgenden Satz zusammen.

Satz 10.0.6. *Sei* $(M, \preceq)$ *eine Boolesche Algebra mit endlichem* M *und kleinstem Element* $\bot$. *Es gelten*

1. $a \wedge m \in \{\bot, a\}$ *für jedes* $m \in M$ *und jedes Atom* $a \in M$,
2. $a \wedge b = \bot$ *für alle Atome* $a, b \in M$ *mit* $a \neq b$,
3. *für jedes* $m \in M \setminus \{\bot\}$ *existiert ein Atom* $a \in M$ *mit* $a \preceq m$.

Das Infimum mit einem Atom a kann also nur das kleinste Element $\bot$ oder a liefern. Das Infimum mit zwei verschiedenen Atomen ist immer das kleinste Element $\bot$, denn Atome sind unvergleichbar. Außerdem liegt jedes Nicht-Atom außer $\bot$ „über“ einem Atom.

Beweis.

1. Offenkundig gilt $a \wedge m \preceq a$. Da a Atom ist, gilt $a \wedge m \in \{\bot, a\}$.
2. Wenn a und b Atome sind, dann folgen aus $a \wedge b \preceq a$ und $a \wedge b \preceq b$ sowohl $a \wedge b \in$

$\{\bot, a\}$ als auch $a \wedge b \in \{\bot, b\}$. Wegen $a \neq b$ muss $a \wedge b = \bot$ gelten.

3. Sei $m_0 \in M \setminus \{\bot\}$ beliebig. Falls m_0 ein Atom ist, dann gilt $m_0 \preceq m_0$. Andernfalls existiert $m_1 \in M$ mit $m_1 \preceq m_0$ und $m_1 \notin \{\bot, m_0\}$. Wir schreiben $x \succ y$ gdw. $y \preceq x$ und $x \neq y$. Also $m_0 \succ m_1$. Mit m_1 können wir das Argument wiederholen und damit eine Kette

$$m_0 \succ m_1 \succ m_2 \succ m_3 \succ \cdots$$

konstruieren. Dies Kette muss mit einem Atom m_i mit $m_i \preceq m_0$ terminieren, da M endlich ist. □

Im Folgenden interessieren wir uns vor allem für endliche Boolesche Algebren. Jedes Element einer solchen lässt sich als ein Supremum von Atomen darstellen. Ferner zeigen wir, dass diese Darstellung sogar eindeutig ist. Die Atome bestimmen also sehr stark die Struktur einer endlichen Booleschen Algebra.

Satz 10.0.7. *Sei $(M, \preceq)$ eine Boolesche Algebra mit endlichem M, kleinstem Element $\bot$ und größtem Element $\top$. Seien $m \in M$ und $A_m = \{a \in M \mid a \text{ Atom}, a \preceq m\}$ die Menge der kleineren Atome. Dann gilt $m = \sup A_m$.*

Beweis. Wir beweisen die Aussage zunächst für $m = \top$. Da $\top$ das größte Element ist, enthält $A_\top$ alle Atome $A_\top = \{a_1, \ldots, a_k\}$. Nehmen wir nun an, dass $\top \neq \sup A_\top$. Dann gilt auch $\top^c = \bot \neq (\sup A_\top)^c = a_1^c \wedge \cdots \wedge a_k^c$ aufgrund der Eindeutigkeit der Komplemente. Da $a_1^c \wedge \cdots \wedge a_k^c \neq \bot$ existiert ein Atom $a_i \in A_\top$, so dass $a_i \preceq a_1^c \wedge \cdots \wedge a_k^c$. Es gilt

$$a_i = a_i \wedge a_1^c \wedge \cdots \wedge a_k^c = a_i \wedge a_i^c \wedge \cdots = \bot \ ,$$

da $a_i \in A_\top$. Also ist $a_i = \bot$ kein Atom. Widerspruch.

Also gilt $\top = \sup A_\top$. Sei nun m beliebig. Es gilt

$$\begin{aligned} m = \top \wedge m = \Big(\sup A_\top\Big) \wedge m &= (a_1 \vee \cdots \vee a_k) \wedge m \\ &= (a_1 \wedge m) \vee \cdots \vee (a_k \wedge m) = \underbrace{(a_1 \wedge m)}_{\in\{a_1, \bot\}} \vee \cdots \vee \underbrace{(a_k \wedge m)}_{\in\{a_k, \bot\}}. \end{aligned}$$

Für jedes $1 \leq i \leq k$ gilt $a_i \wedge m = a_i$ gdw. $a_i \preceq m$. Sei $A_m = \{a_{j_1}, \ldots, a_{j_n}\}$. Also gilt

$$m = (a_{j_1} \wedge m) \vee \cdots \vee (a_{j_n} \wedge m) = a_{j_1} \vee \cdots \vee a_{j_n} = \sup A_m. \qquad \square$$

Satz 10.0.8. *Sei $(M, \preceq)$ eine Boolesche Algebra mit endlichem M und kleinstem*

Element $\bot$. Weiterhin sei A die Menge aller Atome von $(M, \preceq)$. Für alle $X \subseteq A$ und $Y \subseteq A$ mit $X \neq Y$ gilt $\sup X \neq \sup Y$.

Beweis. (indirekt) Seien $X \subseteq A$ und $Y \subseteq A$ Teilmengen der Atome, so dass $X \neq Y$ und $\sup X = \sup Y$. O. B. d. A.[a] existiert $a \in X$, so dass $a \notin Y$. Also gilt

$$\begin{aligned} a &= a \vee \bot = (a \wedge a) \vee \sup\{\bot\} = (a \wedge a) \vee \sup\{a \wedge x \mid x \in X \setminus \{a\}\} \\ &= a \wedge \sup X = a \wedge \sup Y = \sup\{a \wedge y \mid y \in Y\} = \sup\{\bot\} = \bot \ . \end{aligned}$$

Also gilt $a = \bot$, womit a kein Atom ist. Widerspruch. □

[a] Bedeutet „Ohne Beschränkung der Allgemeinheit“. Zeigt an, dass eine nebensächliche Annahme vorausgesetzt wird, die die Allgemeinheit des Beweises nicht einschränkt.

Mit den gewonnenen Erkenntnissen können wir Satz 3.0.4 über die Anzahl der Elemente einer Potenzmenge auf beliebige endliche Boolesche Algebren verallgemeinern.

Satz 10.0.9. *Eine endliche Boolesche Algebra $(M, \preceq)$ mit n Atomen hat genau 2^n Elemente.*

Beweis. Sei A die Menge der Atome. Dann ist $\sup\colon \mathcal{P}(A) \to M$ injektiv per Satz 10.0.8. Also

$$2^n = 2^{|A|} = |\mathcal{P}(A)| \leq |M| \ .$$

Sei $f\colon M \to \mathcal{P}(A)$, so dass $f(m) = A_m$. Diese Funktion ist auch injektiv per Satz 10.0.7 und damit

$$|M| \leq |\mathcal{P}(A)| = 2^n \ ,$$

womit $|M| = 2^n$ folgt. □

Die Struktur endlicher Boolescher Algebren ist so spezifisch, dass jede endliche Boolesche Algebra isomorph zu einer Potenzmengenalgebra ist. Das Rechnen in ihnen entspricht also dem Rechnen mit Teilmengen einer endlichen Menge. Alle Gesetze der endlichen Potenzmengenalgebra $\big(\mathcal{P}(M), \subseteq\big)$ gelten auch in allen Booleschen Algebren dieser Größe.

Satz 10.0.10 (Isomorphiesatz von Stone[2])**.** *Sei $\mathcal{M} = (M, \preceq)$ eine endliche Boolesche Algebra mit Atomen A. Dann sind $\mathcal{M}$ und $\big(\mathcal{P}(A), \subseteq\big)$ isomorph.*

Beweis. Für jedes Element $m \in M$ sei $A_m = \{a \in A \mid a \preceq m\}$ die Menge der Atome unterhalb von m. Wir definieren die Funktion $\varphi\colon M \to \mathcal{P}(A)$ durch $\varphi(m) = A_m$ für alle $m \in M$.

- Injektivität: Seien $x, y \in M$, so dass $A_x = \varphi(x) = \varphi(y) = A_y$. Gemäß Satz 10.0.7

[2] Marshall Harvey Stone (1903–1989)

gilt

$$x = \sup A_x = \sup A_y = y \ .$$

- Surjektivität: Sei $X \subseteq A$ eine Teilmenge der Atome. Da A endlich ist, existiert das Supremum $m = \sup X$ (siehe Beweis von Satz 8.1.6). Also gilt $\varphi(m) = X$ gemäß Satz 10.0.8.

Also ist φ bijektiv. Es bleibt zu zeigen, dass die Struktur erhalten wird. Seien $x, y \in M$ beliebig. Zu zeigen:

$$x \preceq y \ \text{ gdw. } \ \varphi(x) \subseteq \varphi(y) \ .$$

$(\rightarrow)$ Sei $x \preceq y$ und $a \in \varphi(x) = A_x$. Offensichtlich gilt $a \preceq x$ und damit auch $a \preceq y$. Also $a \in A_y = \varphi(y)$, womit $\varphi(x) \subseteq \varphi(y)$ gezeigt ist.

$(\leftarrow)$ Sei $\varphi(x) \subseteq \varphi(y)$. Dann gilt $A_x \subseteq A_y$ und damit

$$x = \sup A_x \preceq \sup A_x \vee \sup(A_y \setminus A_x) = \sup\big(A_x \cup (A_y \setminus A_x)\big) = \sup A_y = y \ .$$

Also sind $\mathcal{M}$ und $\big(\mathcal{P}(A), \subseteq\big)$ isomorph. □

Gilt diese Isomorphie auch für unendliche Boolesche Algebren? Ist die Menge M endlich, dann ist auch $\mathcal{P}(M)$ endlich. Ist die Menge M abzählbar unendlich, dann ist $|\mathcal{P}(M)| > |M|$. Also ist jede unendliche Potenzmengenalgebra überabzählbar. Es gibt aber abzählbar unendliche Boolesche Algebren, also ist nicht jede Boolesche Algebra isomorph zu einer Potenzmengenalgebra.

Kapitel 11

Kommutative Gruppen

Nachdem wir uns in den vorherigen Kapiteln vorrangig mit geordneten Strukturen und Mengen beschäftigt haben, widmen wir uns den Algebraische Strukturen die von von den Zahlen motiviert sind.

Wir wollen zunächst einige elementare Rechengesetze identifizieren. Betrachten wir zunächst die natürlichen Zahlen mit der Addition, also die Struktur $(\mathbb{N}, +)$. Bekanntlich gelten

- $x + (y + z) = (x + y) + z$ für alle $x, y, z \in \mathbb{N}$ und (Assoziativität)
- $x + y = y + x$ für alle $x, y \in \mathbb{N}$. (Kommutativität)

Des Weiteren beobachten wir, dass sich die Null bei der Addition neutral verhält, also dass

- $x + 0 = x$ für alle $x \in \mathbb{N}$

gilt. Da der Null eine gewisse Sonderstellung zukommt, wollen wir sie als besondere Konstante in unsere Struktur aufnehmen: $(\mathbb{N}, +, 0)$. Ganz analog könnten wir versuchen, die Subtraktion in unsere Struktur einzubeziehen. Immerhin kehrt sie die Addition gewissermaßen um und ermöglicht damit erst das Lösen einfacher Gleichungen der Form $x + 42 = 0$. Problematisch ist jedoch, dass die Subtraktion aus der Menge $\mathbb{N}$ herausführt.

Diese Problematik lässt sich auflösen, indem man einfach zu den ganzen Zahlen übergeht. Wir betrachten also die Struktur $(\mathbb{Z}, +, (-\cdot), 0)$ mit der einstelligen Funktion $-\cdot$, die jeder Zahl ihre entgegengesetzte Zahl zuordnet und stellen fest, dass sich nicht nur die drei obigen Eigenschaften auf $\mathbb{Z}$ übertragen, sondern zusätzlich die Eigenschaft

- $x + (-x) = 0$ für alle $x \in \mathbb{Z}$

erfüllt ist. Diese vier Eigenschaften sind prägend für das Rechnen mit Zahlen. Folglich interessieren wir uns für diejenigen Strukturen, die mindestens diese Eigenschaften erfüllen.

11.1 Definitionen und Grundeigenschaften

Eine algebraische Struktur $(M, \oplus, \cdot^*, e)$ des Typs $(0, 1, 1, 1)$ ist eine kommutative oder auch Abelsche Gruppe[1] gdw. für alle $x, y, z \in M$ gilt:

- $x \oplus (y \oplus z) = (x \oplus y) \oplus z$, (Assoziativität)
- $x \oplus y = y \oplus x$, (Kommutativität)
- $e \oplus x = x$, (neutrales Element)
- $x \oplus x^* = e$. (inverse Elemente)

Beispiele 11.1.1.

- *Die algebraischen Strukturen* $\big(\mathbb{Z}, +, (-\cdot), 0\big)$, $\big(\mathbb{Q}, +, (-\cdot), 0\big)$, $\big(\mathbb{R}, +, (-\cdot), 0\big)$, $\big(\mathbb{Q} \setminus \{0\}, \cdot, \cdot^{-1}, 1\big)$ *und* $\big(\mathbb{R} \setminus \{0\}, \cdot, \cdot^{-1}, 1\big)$ *sind kommutative Gruppen.*
- *Die algebraische Struktur* $\big(\mathbb{N}, +, (-\cdot), 0\big)$ *ist keine kommutative Gruppe, denn für* 1 *gibt es kein Inverses (es gibt kein* $n \in \mathbb{N}$*, so dass* $1 + n = 0$*).*
- *Die algebraische Struktur* $\big(\mathbb{Q}, \cdot, \cdot^{-1}, 1\big)$ *ist ebenfalls keine kommutative Gruppe, denn für* 0 *gibt es kein Inverses (es gibt kein* $q \in \mathbb{Q}$*, so dass* $0 \cdot q = 1$*).*

Bemerkung 11.1.2. Wir betrachten nur kommutative Gruppen. Es gibt allerdings auch nicht-kommutative Gruppen, für die im Wesentlichen die gleichen Bedingungen ohne die Kommutativität von $\oplus$ gelten.

Kommutative Gruppen werden manchmal auch multiplikativ geschrieben, also beispielsweise so: $(M, \odot, \cdot^{-1}, 1)$.

Die folgenden Sätze zeigen, dass die zweistellige Verknüpfung in Verbindung mit den Gruppeneigenschaften eine Gruppe bereits vollständig festlegt.

Satz 11.1.3. *Seien* $(M, \oplus, \cdot^*, e)$ *und* $(M, \oplus, \cdot^\dagger, u)$ *zwei kommutative Gruppen mit gleicher binärer Operation* $\oplus$*. Dann gilt* $e = u$*; d.h. das neutrale Element ist eindeutig bestimmt.*

Beweis. Unter Anwendung der Gesetze gilt

$$\underbrace{e = u \oplus e}_{\text{Neutralität } u} = \underbrace{e \oplus u = u}_{\text{Neutralität } e} .$$

□

[1] Niels Henrik Abel (1802–1829)

Satz 11.1.4. *Seien $(M, \oplus, \cdot^*, e)$ und $(M, \oplus, \cdot^\dagger, e)$ zwei kommutative Gruppen mit gleicher binärer Operation $\oplus$ und gleichem neutralen Element e. Dann gilt $x^* = x^\dagger$ für alle $x \in M$; d.h. die Inversen sind eindeutig bestimmt.*

Beweis. Unter Anwendung der Gesetze gilt für alle $x \in M$

$$x^* = e \oplus x^* = \underbrace{(x \oplus x^\dagger)}_{e} \oplus x^* = (x^\dagger \oplus x) \oplus x^* = x^\dagger \oplus \underbrace{(x \oplus x^*)}_{e} = x^\dagger \oplus e = x^\dagger \ . \qquad \square$$

Aufgrund der nachgewiesenen Eindeutigkeit wir könnten die Kommutative Gruppen auch so definieren: Eine algebraische Struktur $(M, \oplus)$ des Typs $(0, 1, 0, 0)$ ist eine kommutative Gruppe, gdw.

- $\oplus$ kommutativ und assoziativ ist,
- ein Element $e \in M$ existiert, so dass $e \oplus x = x$ für alle $x \in M$,
- für alle $x \in M$ ein $y \in M$ existiert, so dass $x \oplus y = e$.

Diese Art, über Gruppen zu schreiben, d.h. als eine Struktur $(M, +)$, ist häufiger, weil sie kürzer ist. Es ist jedoch wichtig, daran zu erinnern, dass die Axiome implizieren, dass die inverse Operation und das neutrale Element eindeutig bestimmt sind.

Wir werden häufig das folgende Lemma verwenden.

Lemma 11.1.5. *Sei $(M, +)$ eine kommutative Gruppe und $x, y \in M$. Dann existiert genau ein $z \in M$, so dass $x + z = y$.*

Beweis. Wir definieren $z := y + (-x)$. Dann $x + z = x + (y + (-x)) = x + ((-x) + y) = (x + (-x)) + y = 0 + y = y$.

Für eindeutigkeit, wenn $x + z = x + z'$ dann auch $(-x) + (x + z) = (-x) + (x + z')$,aber mit Assoziativität sehen wir dass das $z = z'$ bedeuted. $\square$

Im Beweiss haben wir auch die Eigenschaft gesehen dass in in jeder kommutativen Gruppe wenn wir Elemente $m, x, y \in M$ mit $m + x = m + y$ haben, dann gilt $x = y$.

In einer Gruppe kann man also gemeinsame Summanden aus Gleichungen streichen (formal: auf beiden Seiten subtrahieren).

11.2 Untergruppen und Quotienten

Bei einer kommutativen Gruppe $(M, +)$ sagt man, dass $N \subset M$ eine Untergruppe ist, wenn für $0 \in N$, für alle $x, y \in N$ $x + y, -x \in N$ gilt.

Beispiel 11.2.1. *(a) Gegeben eine Gruppe $(M,+)$, bezeichnen wir mit 0_M das neutrale Element von M. Dann ist die Menge $\{0_M\}$ die "triviale Untergruppe" von M.*

(b) $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe

(c) $\mathbb{N} \subset \mathbb{Q}$ ist keine Untergruppe

(d) $n\mathbb{Z} \subset \mathbb{Z}$ ist eine Untergruppe, wobei $n\mathbb{Z} := \{nx \colon x \in \mathbb{Z}\}$.

(e) $\mathbb{Z}$ ist isomorph zu vielen verschiedenen Untergruppen von $\mathbb{Z}^2$, zum Beispiel $\{(x,0) \colon x \in \mathbb{Z}\}$, $\{(x,x) \colon x \in \mathbb{Z}\}$, $\{(5x,7x) \colon x \in \mathbb{Z}\}$.

Bemerkung 11.2.2. Kurzum: Eine Menge U bildet eine Untergruppe gdw. man die Menge U nicht mit den Operationen verlassen kann. Aus diesen Eigenschaft folgt ebenfalls direkt, dass U eine Untergruppe bildet gdw. U eine Unterstruktur von $(M, \odot, \cdot^{-1}, i)$ ist. An dieser Stelle können wir den Unterschied zwischen einer Unterstruktur von $(M, \odot, \cdot^{-1}, i)$ und einer Unterstruktur von $(M, \odot)$ noch einmal verdeutlichen. Obwohl die Inversen $\cdot^*$ und das neutrale Element i eindeutig bestimmt sind, ergibt sich an dieser Stelle ein Unterschied. Dafür betrachten wir die Gruppe der ganzen Zahlen $\big(\mathbb{Z}, +, (-\cdot), 0\big)$ und die Menge der natürlichen Zahlen $\mathbb{N}$. Offensichtlich bildet $\mathbb{N}$ eine Unterstruktur von $(\mathbb{Z}, +)$, denn die Summe von zwei natürlichen Zahlen ist wieder eine natürliche Zahl. Allerdings bildet $\mathbb{N}$ keine Unterstruktur von $\big(\mathbb{Z}, +, (-\cdot), 0\big)$ und damit auch keine Untergruppe, denn $1 \in \mathbb{N}$, aber $-1 \notin \mathbb{N}$.

Bei einer abelschen Gruppe $(A,+)$ und einer Untergruppe $N \subset A$ betrachten wir die Äquivalenzrelation auf A, die gegeben ist durch $x \sim_N y$ iff $x - y \in N$. (Übung: Beweisen Sie, ob dies eine Äquivalenzrelation ist). Äquivalenzklassen dieser Relation werden Nebenklassen genannt. Die Menge aller Nebenklassen, d.h. $A/\sim_N$ wird mit A/N bezeichnet, und man nennt sie die Faktorgruppe von A durch N.

Lemma 11.2.3. *Jede Nebenklasse hat die Form $x + N := \{x + n \colon n \in N\}$ für irgendein $x \in A$. Umgekehrt ist jede Menge der Form $x + N$ eine Nebenklasse.*

Beweis. Zunächst sei $E \subset A$ eine Äquivalenzklasse, und $x \in E$. Wenn $y \in x + N$ ist, dann ist $y = x + n$ für irgendein $n \in N$ und somit $y - x = n \in N$. Dies zeigt, dass $x + N \subset E$. Und wenn $y \in E$, dann ist per Definition $x - y \in N$, also $x - y = n$ für irgendein $n \in N$, und somit $y = x - n = x + (-n)$, was zeigt, dass $y \in x + N$ ist. Dies zeigt, dass $E \subset x + N$, und so sehen wir $E = x + N$.

Umgekehrt wollen wir zeigen, dass $x + N$ eine Äquivalenzklasse ist. In der Tat sehen

wir leicht, dass die Klasse von x genau gleich $x + N$ ist, und zwar mit den gleichen Argumenten wie oben. □

Wenn E eine Nebenklasse ist und $x + N$, dann sagt man, dass x ein Nebenklassenrepräsentant ist. Man beachte, dass jedes $y \in x + N$ ein Repräsentant der Nebenklasse $x + N$ ist.

Der Grund, warum A/N Faktorgruppe genannt wird, ist natürlich, dass wir eine Gruppenstruktur auf A/N haben, die durch die folgende Operation definiert ist:

$$(x + N) \oplus (y + N) := (x + y) + N$$

Lemma 11.2.4. *Die Operation $\oplus$ ist wohldefiniert und darüber hinaus ist $(A/N, \oplus)$ eine Gruppe. Das neutrale Element ist die Teilmenge $N = 0 + N$. Die Inverse von $x + N$ ist $-x + N$.*

Beweis. Wohldefiniertheit: Angenommen $x + N = x' + N$ und $y + N = y' + N$. Wir müssen zeigen, dass $x + y + N = x' + y' + N$. Wir nehmen an, dass $x - x', y - y' \in N$, und somit ist $(x + y) - (x' + y') = x - x' + y - y'$ tatsächlich ein Element von N.

Wir müssen prüfen, ob $(A/N, \oplus)$ die Axiome der Gruppen erfüllt. Die Kommutativität folgt aus der Kommutativität von A: $x + N \oplus y + N = x + y + N$, und $y + N \oplus x + N = y + x + N$. Ähnlich verhält es sich mit der Assoziativität. Wir sehen, dass die Teilmenge N tatsächlich das neutrale Element ist: $0 + N \oplus x + N = 0 + x + N = x + N$. Schließlich sehen wir, dass es Inversen gibt: $x + N \oplus -x + N = x - x + N = 0 + N = N$. □

Üblicherweise wird die Kardinalität einer Gruppe als Ordnung der Gruppe bezeichnet. Die Ordnung von A/N heißt Index von N in A und wird mit $|A : N|$ oder $(A : N)$ bezeichnet.

11.3 Isomorphismen und Homomorphismen

Ein Isomorphismus von Gruppen $(M, +)$ und $(N, +)$ ist eine Bijektion $\phi\colon M \to N$, so dass $\phi(a + b) = \phi(a) + \phi(b)$ für alle $a, b \in M$. Daraus folgt, dass $\phi(0_M) = 0_N$, $\phi(-x) = -\phi(x)$ für alle $x \in M$.

Führen wir nun einen weiteren nützlichen Begriff ein, den des Gruppenhomomoprhismus: Ein Homomorphismus von $(M, +)$ zu $(N, +)$ ist eine Funktion $\phi\colon M \to N$, so dass für alle $a, b \in M$ gilt $\phi(a + b) = \phi(a) + \phi(b)$ und außerdem $\phi(0_M) = 0_N$ und $\phi(-x) = -\phi(x)$ für alle $x \in M$.

Man beachte, dass es reicht die Eigenschaft $\phi(a + b) = \phi(a) + \phi(b)$ checken. Die zwei weitere Eigenschaften folgen leicht mit der hilve von Lemma 11.1.5.

Beispiele 11.3.1. *(a) Gegeben zwei Gruppen A, B können wir $\phi(a) := 0_B$ für alle a definieren. Dies wird manchmal als "trivialer Homomoprhismus" bezeichnet.*

(b) Wenn $A \subset B$ eine Untergruppe ist, dann können wir den injektiven Homomorphismus $\phi\colon A \to B$ betrachten, der durch $\phi(x) := x$ gegeben ist.

(c) Bei zwei Gruppen A, B haben wir surjektive Homomorphismen $A \times B \to A$ und $A \times B \to B$, gegeben durch $\phi(a, b) := a$ bzw. $\phi(a, b) := b$.

(d) Gegeben zwei Homomoprhismen $\alpha\colon A \to B$ und $\beta\colon A \to C$ können wir einen Homomoprhismus $(\alpha, \beta)\colon A \to B \times C$ bilden, gegeben durch $(\alpha, \beta)(a) := (\alpha(a), \beta(a))$.

(e) Wir haben einen surjektiven Homomorphismus $\phi\colon A \to A/N$, gegeben durch $\phi(a) := a + N$. Diesen Homomorphismus nennen wir die Faktorkarte.

11.4 Die Gruppen der Residuen modulo n

Beispiel 11.4.1. *Die Gruppe der Residuen Modul n ist die Gruppe $\mathbb{Z}/n\mathbb{Z}$. Die Nebenklassenrepräsentanten sind zum Beispiel $0, 1, 2, 3, \ldots n-1$. Die Gruppenoperation auf diesen Repräsentanten ist die Standardaddition, aber wenn wir über $n-1$ hinausgehen, müssen wir eine Zahl kleiner als $n-1$ finden, die kongruent modulo n ist. Zum Beispiel haben wir in $\mathbb{Z}/5\mathbb{Z}$ $2 + 2 \equiv 4, 4 + 4 \equiv 8 \equiv 3$.*

Bemerkung 11.4.2. Jede endliche Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$. Dies ist eine sehr wichtige Tatsache, die normalerweise in einem Kurs über lineare Algebra bewiesen wird. Wir werden sie in diesem Kurs nicht beweisen.

Bemerkung 11.4.3. Wenn $n \mid m$, dann haben wir einen Surjektivhomomomorphismus $\phi\colon \mathbb{Z}/m\mathbb{Z}\ zu\mathbb{Z}/n\mathbb{Z}$, gegeben durch $\phi(a+m\mathbb{Z}) := a \mod n$. Dies ist ein Spezialfall der Faktorabbildung, da $\{nx + m\mathbb{Z}, x \in \mathbb{Z}\}$ eine Untergruppe von $\mathbb{Z}/m\mathbb{Z}$ ist.

Das folgende Theorem ist als "Chinesischer Restsatz" bekannt

Satz 11.4.4. *Seien a, b positive koprimale ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.*

Beweis. Wir betrachten den Homomoprhismus $\phi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\phi := (\alpha, \beta)$ definiert ist, wobei α, β die jeweiligen Faktorabbildungen sind. Explizit haben wir $\phi(k) = k \mod a, k, \mod b)$. Wir müssen prüfen, ob ϕ bijektiv ist.

Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben, genügt es

zu prüfen, dass ϕ injektiv ist. Dazu nehmen wir an, dass $x, y \in \{0, \ldots, n-1\}$ so sind, dass $\phi(x) = \phi(y)$ und nehmen wir widerspruchshalber $x < y$ an. Dann ist $\phi(y-x) = (y-x \mod a, y-x \mod b)$ und wir sehen, dass $y-x$ durch a und durch b teilbar ist. Da aber a und b koprim sind, bedeutet dies, dass $y-x$ durch $ab = n$ teilbar ist, was ein Widerspruch zu der Tatsache ist, dass $0 < y - x < n$. □

Kapitel 12

Ringe und Körper

Natürlich gibt es für Zahlenmengen wie $\mathbb{Z}$ oder $\mathbb{Q}$ zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des Rings (oder "kommutativen Rings mit Eins").

Ein Ring ist eine algebrische Struktur $(M, +, \cdot)$, so dass

(a) $(M, +)$ ist eine abelsche Gruppe (genannt additive Gruppe des Rings)

(b) $\cdot$ ist assoziativ und kommutativ

(c) es gibt $1_M \in M$ so dass für alle $m \in M$ gilt $1_M \cdot m = m$ (daraus folgt, dass 1_M eindeutig ist).

(d) für alle $a, b, c \in M$ wir haben $a \cdot (b + c) = a \cdot b + a \cdot c$.

Bemerkung 12.0.1. Wie bei Gruppen könnten wir Ringe als $(M, +, -\cdot, 0_M, \cdot, \cdot^{-1}, 1_M)$ mit geeigneten Axiomen definieren.

Beispiel 12.0.2. *(a)* $(\mathbb{Z}, +, \cdot)$ *ist ein Ring*

(b) $(\mathbb{Q}, +, \cdot)$ *is ein Ring*

Bemerkung 12.0.3. In einem Ring $(M, +, \cdot)$ haben wir $0 \cdot x = 0$ für alle x. Tatsächlich haben wir $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, und da $(M, +)$ ein Kommutativ ist, leiten wir $0 \cdot x = 0$ ab.

Eine besondere wichtige Klasse von Ringen sind Körper - ein Ring $(M, +, \cdot)$ ist ein Körper, wenn für jedes $x \in M$ mit $x \neq 0_M$ $y \in M$ so existiert, dass $xy = 1_M$. Äquivalent dazu ist ein Ring $(M, +, \cdot)$ ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist. Beispiele für Körper sind $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$.

Bemerkung 12.0.4. (a) In einem Körper $(M, +, \cdot)$ gilt, dass $xy = 0$ impliziert, dass entweder $x = 0$ oder $y = 0$. In der Tat, wenn $x \neq 0$ dann können wir schreiben $y = x^{-1}xy = x^{-1}0 = 0$. Wir beschreiben diese Eigenschaft, indem wir sagen, dass Felder "nur triviale Nullteiler haben".

(b) Wenn A und B Ringe sind, dann ist $A \times B$ ebenfalls ein Ring. Wenn A und B jedoch Ringe sind, die nicht Null sind, dann ist $A \times B$ kein Körper: wir haben $(1_A, 0_B) \cdot (0_A, 1_B) = (0_A, 0_B)$

12.1 Ideale und Faktorringe

Sei $(M, +, \cdot)$ ein Ring. Wir sagen, dass $I \subset M$ ein ideal ist, wenn I eine Untergruppe von $(M, +)$ ist und für alle $m \in M$ gilt $mI \subset I$.

Beispiele 12.1.1. *(a) M ist ein Ideal von M. Jedes andere Ideal heißt proper. Ein Ideal ist echt, wenn es 1_M nicht als Element enthält.*

(b) $\{0\} \subset M$ ist ein Ideal.

(c) $n\mathbb{Z} \subset \mathbb{Z}$ ist ein Ideal für jede natürliche Zahl n.

(d) Wenn $m \in M$ dann $mM := \{mx : x \in M\}$ ist das Hauptideal erzeugt durch m. Oft wird es durch (m) bezeichnet.

Ist $I \subset M$ ein Ideal, so ist sie insbesondere eine Untergruppe von $(M, +)$ und wir können damit die Quotientengruppe M/I bilden.

Lemma 12.1.2. *$(M/I, +, \cdot)$ wird zu einem Ring, wenn wir die Multiplikation mit $[m] \cdot [n] := [mn]$ definieren*

Beweis. Die Tatsache, dass alle Axiome erfüllt sind, folgt direkt aus der Tatsache, dass M ein Ring ist. Die einzige Eigenschaft, die wir überprüfen müssen, ist, dass die Multiplikation wohldefiniert ist. Nehmen wir also $[m] = [m']$ und $[n] = [n']$ an, so haben wir $m-m', n-n' \in I$. Da I ein Ideal ist, haben wir auch $n(m-m'), m(n-n') \in I$. Daraus folgt, dass $n'(m-m') + m(n-n') = mn - n'm' \in I$ und somit tatsächlich $[mn] = [m'n']$. □

Beispiel 12.1.3. *$\mathbb{Z}/m\mathbb{Z}$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b]$ in $\mathbb{Z}/m\mathbb{Z}$ mit $[a], [b] \neq [0]$ so finden, dass $[a][b] = 0$. Wenn also m nicht prim ist, dann ist $\mathbb{Z}/m\mathbb{Z}$ kein Feld.*

Lemma 12.1.4. *$\mathbb{Z}/p\mathbb{Z}$ ist ein Körper gdw. p eine Primzahl ist.*

Beweis. Wir haben im obigen Beispiel gesehen, dass, wenn p keine Primzahl ist, $\mathbb{Z}/p\mathbb{Z}$ kein Körper ist. Nehmen wir nun an, dass p eine Primzahl ist. Wir nehmen $[x]$ $in\mathbb{Z}/p\mathbb{Z}$ mit $x \not\equiv 0$. Wir müssen zeigen, dass für einige $[y] \in \mathbb{Z}/p\mathbb{Z}$ $xy \equiv 1$ haben. Betrachten wir die Abbildung $\mu\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, gegeben durch $\mu([a]) := [x][a] = [xa]$. Diese Abbildung ist injektiv: Wenn nämlich $\mu(a) \equiv \mu(b)$, dann $xa \equiv xb$, also $xa - xb \equiv 0$ und somit p teilt $x(a-b)$. Da $x \not\equiv 0$, folgern wir $p \mid a - b$, was $a \equiv b$ bedeutet.

Da aber $\mathbb{Z}/p\mathbb{Z}$ endlich ist, leiten wir ab, dass μ ebenfalls surjektiv ist, und es folgt, dass für irgendein a gilt $xa \equiv 1$. □

Bemerkung 12.1.5. Der Körper $\mathbb{Q}$ und die Körper $\mathbb{Z}/p\mathbb{Z}$ werden als Primkörper bezeichnet. Jeder Körper enthält ein Primkörper.

12.2 Polynome

Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \ldots, a_n \in M$ mit $a_n \neq 0$. Wir assoziieren mit dieser endlichen Folge ein Polynom, das man sich als folgende Formel vorstellen soll:

$$p = a_0 + a_1 X + \ldots a_n X^n.$$

Dieses Polynom p definiert eine Funktion $M \to M$ für alle $x \in M$ die am meinstens wieder mit dem Symbol p bezeichnet wird, durch

$$p(x) = a_0 + a_1 x + \ldots a_n x^n.$$

Wir schreiben auch $\text{grad}(p) = n$. Das Nullpolynom p mit $p = ()$ hat Grad $-\infty$. Ein Element $x \in M$ ist Nullstelle von p gdw. $p(x) = 0$. Die Menge von allen Polynomen mit Koeffizienten aus M wird mit $M[X]$ bezeichnet.

Beispiel 12.2.1. *Im Körper $\mathbb{Z}/5\mathbb{Z}$ betrachten wir das Polynom $[1]X^2 + [4]X + 2]$. Es gilt*

$$p([2]) = [2] + ([4] \cdot [2]) + ([2] \cdot [2]) = [2] + [3] + [4] = [4]$$

Für die Bestimmung der Nullstellen von p berechnen wir:

- $p([0]) = [2]$,
- $p([1]) = [2] + [4] + [1] = [2]$,
- $p([2]) = [4]$,
- $p([3]) = [2] + [2] + [4] = [3]$ *und*

- $p([4]) = [2] + [1] + [1] = [4]$.

Offenbar hat p keine Nullstellen.

Die folgenden Sätze sind für die Handhabung von Polynomen von großer Wichtigkeit. Obwohl die Beweise nicht schwer sind, geben wir sie hier nicht mit an.

Satz 12.2.2 (Horner-Schema)**.** *Sei $(M, +, \cdot)$ ein Ring und sei $p = a_0 + a_1X + \ldots + a_nX$ ein Polynom von einem Grad $n \geq 0$. Dann gilt für alle $x \in M$*

$$p(x) = a_0 + x \cdot (a_1 + x \cdot (a_2 + \ldots x a_n))$$

Satz 12.2.3. *(Polynomdivision) Sei $(M, +, \cdot)$ ein Körper. Weiterhin seien p und q Polynome mit* $\operatorname{grad}(q) \geq 0$*. Dann existieren Polynome t und r mit*

$$p(X) = t(X) \cdot q(X) + r(X)$$

und $\operatorname{grad}(r) < \operatorname{grad}(q)$.

Die Polynome t und r aus dem vorherigen Satz erhält man per Polynomdivision.

Beispiel 12.2.4.

$$\begin{array}{rl} & x^3 \quad - x - 2 \\ \hline x^2 + 1 \big) & x^5 \quad - 2x^2 + 4x + 7 \\ & \underline{- x^5 - x^3} \\ & \quad - x^3 - 2x^2 + 4x \\ & \quad \underline{x^3 \quad + x} \\ & \quad - 2x^2 + 5x + 7 \\ & \quad \underline{2x^2 \quad + 2} \\ & \quad 5x + 9 \end{array}$$

Wir wissen, dass es für jede Primzahl p einen Körper $\mathbb{Z}/p\mathbb{Z}$ mit genau p Elementen gibt.

Beispiel 12.2.5. *Der Ring $\mathbb{Z}/5\mathbb{Z}[X]/(X^2 + X + 2)$ ist ein Körper. In der Tat betrachten wir für $f \in \mathbb{Z}/5\mathbb{Z}[X]$ die Abbildung $M_f \colon \mathbb{Z}/5\mathbb{Z}[X]/(X^2 + X + 2) \to \mathbb{Z}/5\mathbb{Z}[X]/(X^2 + X + 2)$, gegeben durch $M_f(g) = fg$. Wir wollen zeigen, dass diese Abbildung surjektiv ist, und dass insbesondere für einige g gilt $fg = 1$. Wir stellen jedoch fest, dass $\mathbb{Z}/5\mathbb{Z}[X](X^2 + X + 2)$ endlich ist (jedes Element ist durch $aX + b$, $a, b \in \mathbb{Z}/5$ repräsentiert), so dass es genügt zu zeigen, dass M_f injektiv ist. Wenn $M_f(a) = M_f(b)$ dann $f(a - b) = 0$. Daraus folgt, dass $X^2 + X + 2$ teilt $f(a - b)$. Da wir annehmen können, dass* $\operatorname{grad}(f) = \operatorname{grad}(a - b) = 1$*, folgt, dass $f(a - b)$ eine Faktorisierung von $X^2 + X + 2$ in Polynome vom Grad 1 ist, so dass insbesondere*

> $X^2 + X + 2$ *Nullstellen hat, was, wie wir gesehen haben, nicht der Fall ist.*

Wir schließen dieses Kapitel mit der Charakterisierung der endlichen Körper ab. Ein Körper $\big(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i\big)$ ist endlich oder auch Galois-Körper[1], falls M endlich ist.

Satz 12.2.6 (Moore)**.**

- *Sei $(M, +, \cdot)$ ein Galois-Körper (endlicher Körper).*
  Dann existieren $n, p \in \mathbb{N}$ mit p prim, so dass $|M| = p^n$.
- *Seien $\mathcal{K}$ und $\mathcal{N}$ Galois-Körper mit gleich vielen Elementen.*
  Dann sind $\mathcal{K}$ und $\mathcal{N}$ isomorph.

Sei $\mathcal{M} = \big(M, \oplus, \odot, (-\cdot), \cdot^{-1}, e, i\big)$ ein Galois-Körper. Falls $p = |M|$ prim ist, dann ist $\mathcal{M}$ isomorph zu dem bereits bekannten Körper $\big(\mathbb{Z}_p, +_p, \cdot_p, (-\cdot), \cdot^{-1}, 0, 1\big)$. Die weiteren Galois-Körper ergeben sich mit Hilfe von Polynomen über einem solchen Basiskörper. Insbesondere kann man den Satz von Moore verwenden, um zu zeigen, dass kein Körper 6 Elemente hat. Die genaue Kenntnis der endlichen Körper ist in der Kodierungstheorie und Kryptographie entscheidend.

[1] Évariste Galois (1811–1832)

Kapitel 13

Graphen und Bäume

Gerichtete Graphen sind genau die algebraischen Strukturen des Typs $(1, 0, 0, 0)$. Jeder Graph ist also eine Struktur (E, K) mit einer Menge E, deren Elemente Ecken genannt werden, und einer Relation $K \subseteq E \times E$, deren Elemente Kanten genannt werden. Für eine Kante $(s, z) \in K$ heißt s Startecke und z Zielecke von (s, z). Intuitiv handelt es sich bei einem Graphen um eine Menge von benannten Punkten die beliebig miteinander verbunden sind. Wir werden nur endliche Graphen betrachten.

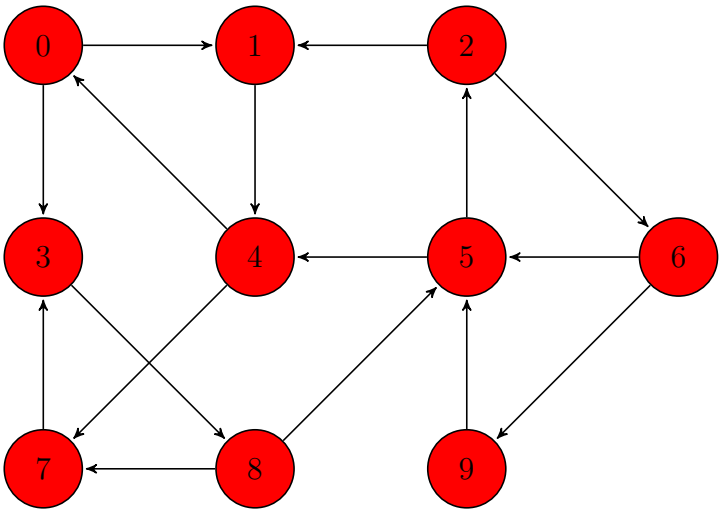


Abbildung 13.1: Beispielgraph

Ein Graph $\mathcal{G} = (E, K)$ ist ungerichtet gdw. K symmetrisch ist. Man beachte, dass ein ungerichteter Graph immer auch gerichtet ist, obwohl der Terminus das Gegenteil nahelegt. Des Weiteren heißt $\mathcal{G}$ schlingenfrei gdw. K irreflexiv ist. Jede Kante $(s, s) \in K$ heißt Schlinge von $\mathcal{G}$. Sei $e \in E$ eine Ecke. Die Vorgänger von e sind alle Ecken, die eine Kante zu e haben:

$$V_{\mathcal{G}}(e) = \{s \in E \mid (s, e) \in K\} \ .$$

Die Nachfolger von e sind entsprechend alle Ecken, zu denen eine Kante von e aus existiert:

$$N_{\mathcal{G}}(e) = \{z \in E \mid (e, z) \in K\} \ .$$

Der Eingangsgrad von e ist Anzahl der Vorgänger und der Ausgangsgrad von e die Anzahl

der Nachfolger:

$$\text{in-grad}_{\mathcal{G}}(e) = |V_{\mathcal{G}}(e)| \qquad \text{und} \qquad \text{aus-grad}_{\mathcal{G}}(e) = |N_{\mathcal{G}}(e)| \ .$$

Beispiel 13.0.1. *Der abgebildete Beispielgraph ist nicht ungerichtet, aber endlich und schlingenfrei. Ferner gilt*

$$\begin{array}{llll} V_{\mathcal{G}}(0) = \{4\} \ , & N_{\mathcal{G}}(0) = \{1,\,3\} \ , & \text{in-grad}_{\mathcal{G}}(0) = 1 \ , & \text{aus-grad}_{\mathcal{G}}(0) = 2 \ , \\ V_{\mathcal{G}}(4) = \{1,\,5\} \ , & N_{\mathcal{G}}(4) = \{0,\,7\} \ , & \text{in-grad}_{\mathcal{G}}(4) = 2 \ , & \text{aus-grad}_{\mathcal{G}}(4) = 2 \ . \end{array}$$

Natürlich besteht ein enger Zusammenhang zwischen der Anzahl der Kanten und der Summe der Kantengrade.

Satz 13.0.2. *Für jeden Graphen $\mathcal{G} = (E, K)$ gilt $|K| = \sum_{s\in E} \text{aus-grad}_{\mathcal{G}}(s)$.*

Beweis.

$$\begin{aligned} |K| &= |\{(s,z) \mid (s,z) \in K\}| = \sum_{s\in E} |\{(s,z) \mid (s,z) \in K\}| \\ &= \sum_{s\in E} |\{z \mid (s,z) \in K\}| = \sum_{s\in E} |N_{\mathcal{G}}(s)| = \sum_{s\in E} \text{aus-grad}_{\mathcal{G}}(s) \end{aligned}$$

□

Analog gilt $|K| = \sum_{z\in E} \text{in-grad}_{\mathcal{G}}(z)$.

13.1 Wege, Pfade, Kreise

Sei (E, K) ein Graph und $n \in \mathbb{N}$. Eine Folge

$$(e_0 \to \cdots \to e_n)$$

mit $e_0, \ldots, e_n \in E$ heißt Weg von e_0 nach e_n gdw. $(e_i, e_{i+1}) \in K$ für alle $0 \leq i < n$. Ein solcher Weg hat die Länge n. Gelten zusätzlich $e_i \neq e_j$ für alle $0 \leq i < j < n$ und ebenso $e_n \notin \{e_1, \ldots, e_{n-1}\}$, dann ist $(e_0 \to \cdots \to e_n)$ sogar ein Pfad von e_0 nach e_n. Ein Weg ist also eine Sequenz von Ecken, so dass jede Ecke Nachfolger der vorherigen Ecke ist. In einem Pfad sind zusätzlich alle Ecken voneinander verschieden, nur die letzte Ecke darf mit der ersten Ecke übereinstimmen. Kreise sind genau die Pfade $(e_0 \to \cdots \to e_n)$ mit $e_0 = e_n$ und $n \geq 3$. Der Graph (E, K) ist kreisfrei gdw. er keinen Kreis enthält. Man beachte: Schlingen und Pfade der Form $(s \to z \to s)$ sind keine Kreise.

Beispiele 13.1.1. *Wir betrachten wieder den Beispielgraph.*

- *Die Folge*

  $$(6 \to 5 \to 4 \to 7 \to 3 \to 8 \to 5 \to 2)$$

  ist ein Weg von 6 *nach* 2 *mit Länge* 7*, aber kein Pfad.*

- *Die Folge*

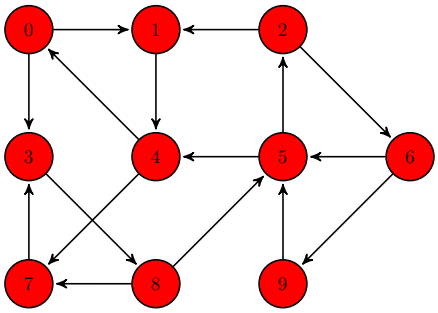
  $$(3 \to 8 \to 9 \to 5 \to 2 \to 1 \to 0)$$

  ist kein Weg von 3 *nach* 0*.*

- *Die Folge*

  $$(3 \to 8 \to 7 \to 3)$$

  ist ein Pfad von 3 *nach* 3 *und ein Kreis. Der Beispielgraph ist also nicht kreisfrei.*



13.2 Erreichbarkeit und Zusammenhang

Sei $\mathcal{G} = (E, K)$ ein Graph. Für alle $s, z \in E$ gelte $s \sim_{\mathcal{G}} z$ gdw. ein Weg von s nach z existiert und ein Weg von z nach s existiert. Man beachte: Die Folge (e) ist ein Weg der Länge 0 von e nach e für alle $e \in E$. Wir nennen diese Äquivalenzrelation beidseitig starke Erreichbarkeit.

Beweis (Nachweis der Äquivalenzeigenschaften).

- Reflexivität: Sei $e \in E$. Dann ist (e) ein Weg von e nach e und damit $e \sim_{\mathcal{G}} e$.
- Symmetrie: Sei $s \sim_{\mathcal{G}} z$. Dann existiert ein Weg von s nach z und ein Weg von z nach s. Also auch $z \sim_{\mathcal{G}} s$.
- Transitivität: Seien $s \sim_{\mathcal{G}} y$ und $y \sim_{\mathcal{G}} z$. Dann existieren Wege
  - $(s \to \cdots \to y)$ und $(y \to \cdots \to z)$ und
  - $(z \to \cdots \to y)$ und $(y \to \cdots \to s)$.

  Folglich existieren auch Wege $(s \to \cdots \to y \to \cdots \to z)$ und $(z \to \cdots \to y \to \cdots \to s)$ und damit $s \sim_{\mathcal{G}} z$. □

Die Äquivalenzklassen von $\sim_{\mathcal{G}}$ heißen starke Zusammenhangskomponenten von $\mathcal{G}$.

Beispiele 13.2.1.

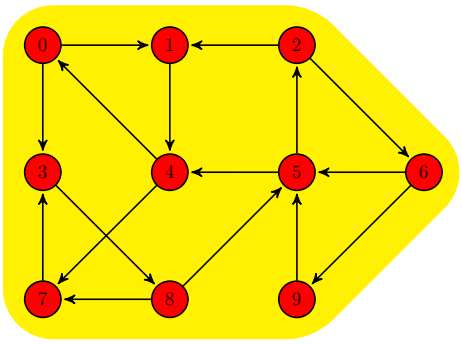


Abbildung 13.2: Graph 1

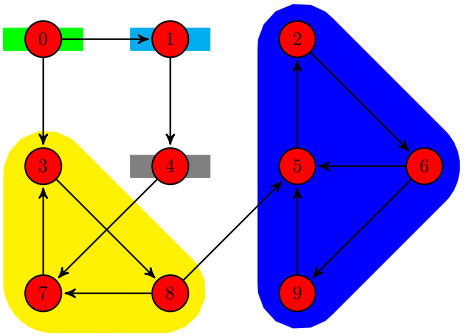


Abbildung 13.3: Graph 2

Graph 1 hat genau eine starke Zusammenhangskomponente $\{0, \ldots, 9\}$. *Graph 2 hat genau fünf starke Zusammenhangskomponenten*

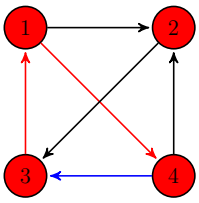
$$\big\{\{0\}, \{1\}, \{2, 5, 6, 9\}, \{3, 7, 8\}, \{4\}\big\} \ .$$

Seien $\mathcal{G} = (E, K)$ und $\mathcal{G}' = (E', K')$ zwei Graphen. Dann ist $\mathcal{G}'$ ein Teilgraph von $\mathcal{G}$ gdw.

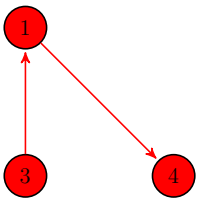
$$E' \subseteq E \qquad \text{und} \qquad K' \subseteq K \ .$$

Gelten $E' \subseteq E$ und $K' = K \cap (E' \times E')$, dann heißt $\mathcal{G}'$ auch Untergraph von $\mathcal{G}$.

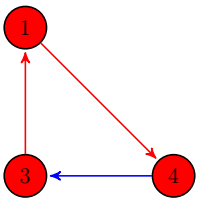
Beispiel 13.2.2.



Graph



Teilgraph



Untergraph

Der zweite Graph ist Teilgraph des ersten Graphen und der dritte Graph ist Untergraph des ersten Graphen.

13.3 Ungerichtete Graphen

Für jeden ungerichteten Graphen $\mathcal{G} = (E, K)$ und $e \in E$ gilt $V_{\mathcal{G}}(e) = N_{\mathcal{G}}(e)$. Dies legt eine Anpassung der Terminologie nahe. Die Menge $N_{\mathcal{G}}(e)$ heißt dann auch Nachbarschaft von e. Wir schreiben auch $\text{grad}_{\mathcal{G}}(e)$ statt $\text{aus-grad}_{\mathcal{G}}(e)$ und nennen es Grad von e. Die Einschränkung auf ungerichtete Graphen erlaubt die folgende hilfreiche Aussage.

Satz 13.3.1. *In jedem endlichen, schlingenfreien und ungerichteten Graphen $\mathcal{G} = (E, K)$ ist die Anzahl der Ecken mit ungeradem Grad gerade.*

Beweis. Ein endlicher, schlingenfreier und ungerichteter Graph hat eine gerade Zahl $|K|$ an Kanten. Also ist nach Satz 13.0.2 auch $|K| = \sum_{e \in E} \text{grad}_{\mathcal{G}}(e)$ gerade. Seien

$$E_g = \{e \in E \mid \text{grad}_{\mathcal{G}}(e) \text{ gerade}\} \qquad \text{und} \qquad E_u = E \setminus E_g \ .$$

Dann gilt

$$\sum_{e \in E} \text{grad}_{\mathcal{G}}(e) = \sum_{e \in E_g} \text{grad}_{\mathcal{G}}(e) + \sum_{e \in E_u} \text{grad}_{\mathcal{G}}(e) \ ,$$

womit $\sum_{e \in E_u} \text{grad}_{\mathcal{G}}(e)$ gerade ist. Da $\text{grad}_{\mathcal{G}}(e)$ für jedes $e \in E_u$ ungerade ist, muss $|E_u|$ gerade sein. □

Auf jedem Empfang schütteln also gerade viele Gäste ungerade vielen Gästen die Hand. Wir schließen eine weitere kombinatorische[1] Aussage an.

Satz 13.3.2. *Jeder endliche ungerichtete Graph $\mathcal{G} = (E, K)$ hat mindestens $|E| - \lfloor \frac{|K|}{2} \rfloor$ starke Zusammenhangskomponenten.*

Beweis. Der Beweis erfolgt durch vollständige Induktion über $|K|$.

- IA: Sei $|K| = 0$. Dann gibt es keine Kanten und nur Wege der Länge 0. Damit bildet jede Ecke ihre eigene starke Zusammenhangskomponente, wovon es $|E| = |E| - \lfloor \frac{|K|}{2} \rfloor$ gibt.
- IH: Gelte die Aussage für Graphen mit höchstens k Kanten.
- IS: Sei $|K| = k + 1$ und wähle $(s, z) \in K$ beliebig. Für $s = z$ hat $\mathcal{G}$ die gleiche Anzahl an Komponenten wie der Graph $\big(E, K \setminus \{(s, z)\}\big)$, der gemäß IH mindestens $|E| - \lfloor \frac{k}{2} \rfloor$ starke Zusammenhangskomponenten hat. Da $|E| - \lfloor \frac{k}{2} \rfloor \geq |E| - \lfloor \frac{k+1}{2} \rfloor$, gilt damit die Aussage.

  Andernfalls hat $\mathcal{G}' = \big(E, K \setminus \{(s, z), (z, s)\}\big)$ mindestens $|E| - \lfloor \frac{k-1}{2} \rfloor$ starke Zusammenhangskomponenten gemäß IH. Aufgrund von (s, z) hat $\mathcal{G}$ höchstens eine Komponente weniger als $\mathcal{G}'$ (denn evtl. verbindet (s, z) zwei Komponenten), also hat (E, K) mindestens $|E| - \lfloor \frac{k-1}{2} \rfloor - 1 = |E| - \lfloor \frac{k+1}{2} \rfloor$ starke Zusammenhangskomponenten. □

Graphen mit genau 1 starken Zusammenhangskomponente heißen auch stark zusammenhängend.

[1] Die Kombinatorik ist die Mathematik des Zählens.

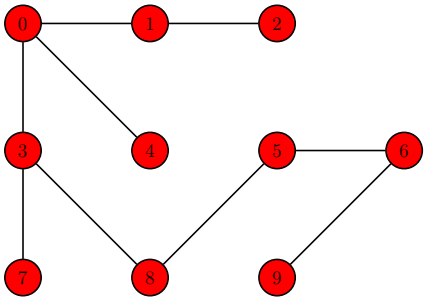
Folgerung 13.3.3. *Jeder stark zusammenhängende endliche ungerichtete Graph (E, K) hat also mindestens $2 \cdot (|E| - 1)$ Kanten.*

Beweis. Gemäß 13.3.2 gilt $|E| - \lfloor \frac{|K|}{2} \rfloor \leq 1$. Umformen liefert $|E| \leq \lfloor \frac{|K|}{2} \rfloor + 1 \leq \frac{|K|}{2} + 1$ und weiter $|K| \geq 2 \cdot (|E| - 1)$. □

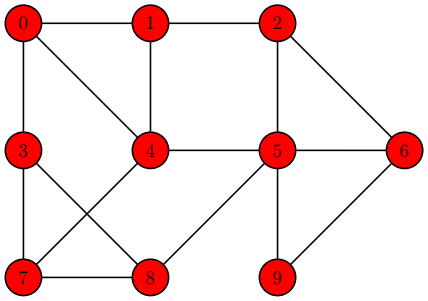
Es gibt jedoch Graphen mit mindestens $2 \cdot (|E| - 1)$ Kanten, die nicht stark zusammenhängend sind.

13.4 Bäume

Ein ungerichteter Graph $\mathcal{G} = (E, K)$ heißt auch Baum gdw. $\mathcal{G}$ stark zusammenhängend und schlingen- als auch kreisfrei ist.



Baum



kein Baum

Der folgende Satz sagt dass im jeden starkzusammenhängenden endlichen ungerichteten Graph, existiert ein Spannbaum, das heisst ein Baum der ein Teilgraph ist.

Satz 13.4.1. *Sei $\mathcal{G} = (E, K)$ ein stark zusammenhängender endlicher ungerichteter Graph. Dann existiert ein Baum $\mathcal{T} = (E, B)$, der ein Teilgraph von $\mathcal{G}$ ist.*

Beweis. Wir betrachten die Menge

$$\mathcal{M} = \{(E', K') \in \mathcal{P}(E) \times \mathcal{P}(K) \mid (E', K') \text{ ist ein Baum}\}$$

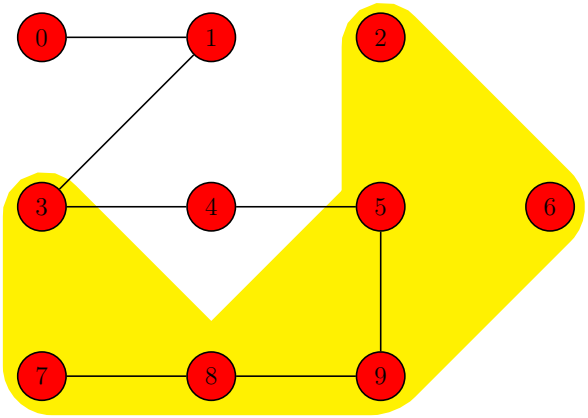
die endlich und nichtleer ist, denn für jedes $e \in E$ ist $(\{e\}, \emptyset) \in \mathcal{M}$. Wir wählen $(E', K') \in \mathcal{M}$ mit maximaler Anzahl von Ecken; d. h. $|E'| \geq |E''|$ für alle $(E'', K'') \in \mathcal{M}$. Wir zeigen $E' = E$ indirekt.

Sei also $E' \subsetneq E$. Per Definition gilt $\emptyset \neq E' \subseteq E$ und sei $s \in E'$ und $z \in E \setminus E'$. Da $\mathcal{G}$ nur eine starke Zusammenhangskomponente hat, gilt $s \sim_{\mathcal{G}} z$ und damit existiert ein Weg $(e_0 \to e_1 \to \cdots \to e_n)$ mit $e_0 = s$ und $e_n = z$.

Da $s \in E'$ und $z \notin E'$ existiert $i \leq n$, so dass $e_{i-1} \in E'$ und $e_i \notin E'$. Wir konstruieren

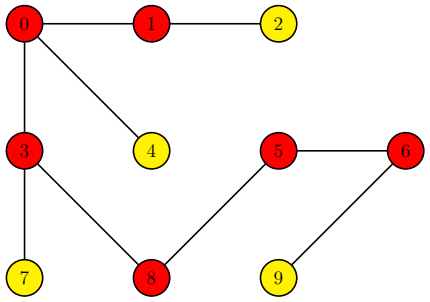
$$\mathcal{T}' = \Big(E' \cup \{e_i\},\, K' \cup \big\{(e_{i-1}, e_i),\, (e_i, e_{i-1})\big\}\Big) \ .$$

Dies ist offensichtlich ein Baum, denn wir haben nur eine neue Ecke e_i und die beiden Kanten, die diese Ecke mit e_{i-1} verbinden, hinzugefügt. Offenbar ist $\mathcal{T}' \in \mathcal{M}$. Es gilt allerdings $|E' \cup \{e_i\}| > |E'|$, womit der Widerspruch gezeigt ist. Also gilt $E' = E$ und damit die Behauptung. □



Sei $\mathcal{T} = (E, K)$ ein Baum. Eine Ecke $e \in E$ mit $\text{grad}_{\mathcal{T}}(e) = 1$ heißt auch Blatt.

Beispiel 13.4.2. *Wir markieren die Blätter.*



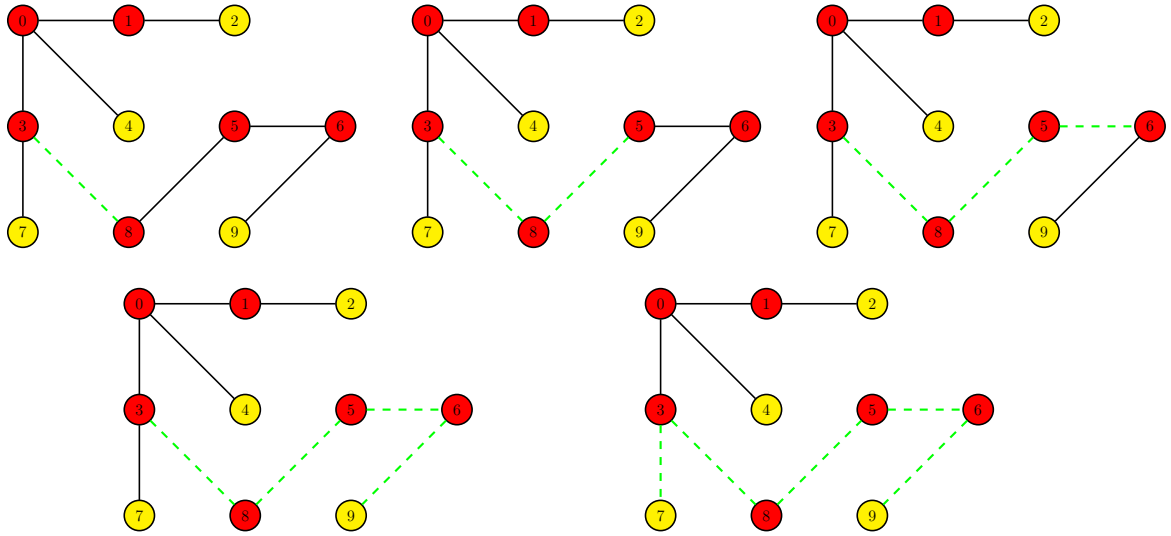
Satz 13.4.3. *Ein endlicher Baum $\mathcal{T} = (E, K)$ mit $|E| \geq 2$ hat mindestens zwei Blätter.*

Beweis. Da $\mathcal{T}$ stark zusammenhängend ist, muss es eine Kante geben. Sei $(s, z) \in K$. Da $\mathcal{T}$ schlingenfrei ist, gilt $s \neq z$. Da es nur endlich viele Pfade gibt (da sich die Ecken auf dem Pfad nicht wiederholen können), existiert ein Pfad $(e_0 \to \cdots \to e_n)$ maximaler Länge, so dass $e_i \neq e_n$ für alle $0 \leq i < n$. Alle Ecken des Pfads sind also verschieden. Wir zeigen indirekt, dass e_0 und e_n Blätter sind.

Sei e_0 kein Blatt; d. h. es existiert $e \in E$, so dass $(e, e_0) \in K$ und $e \neq e_1$. Dann folgt auch $e \neq e_i$ für alle $i \leq n$, denn sonst gäbe es einen Kreis $e \to e_0 \to \cdots \to e_i = e$. Dann ist jedoch $(e \to e_0 \to \cdots \to e_n)$ ein längerer Pfad mit paarweise verschiedenen

Ecken. Widerspruch! Analog für e_n. □

Wir visualisieren die Konstruktion eines maximalen Pfads:



Für Bäume besteht erfreulicherweise eine starke Korrespondenz zwischen der Anzahl der Ecken und der Anzahl der Kanten.

Satz 13.4.4. *Sei $\mathcal{T} = (E, K)$ ein endlicher Baum. Dann gilt $|E| = \frac{|K|}{2} + 1$.*

Beweis. (indirekt) Sei (E, K) ein Baum mit der geringsten Anzahl an Ecken, so dass

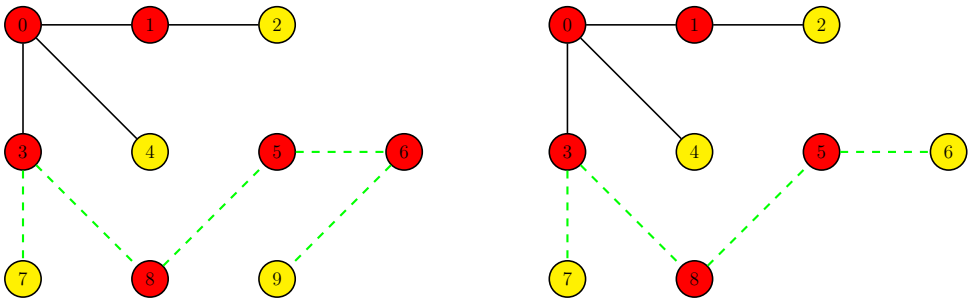
$$|E| \neq \tfrac{|K|}{2} + 1 \ .$$

Das heißt: Für alle Bäume (E', K') mit $|E'| < |E|$ gilt $|E'| = \frac{|K'|}{2} + 1$. Offensichtlich gilt $|E| \geq 2$, denn alle Bäume (E', K') mit einer Ecke haben keine Kanten und damit gilt $1 = |E'| = \frac{|K'|}{2} + 1 = 1$. Folglich hat (E, K) zwei Blätter a, b nach Satz 13.4.3. Wir betrachten den Graph

$$\mathcal{G} = \Big(E \setminus \{b\},\ K \setminus \big\{(b, e),\ (e, b)\big\}\Big) \ ,$$

wobei $N_{\mathcal{G}}(b) = \{e\}$. Dies ist wieder ein Baum und da er kleiner ist, gilt die Behauptung für ihn. Also $|E| - 1 = \frac{|K|-2}{2} + 1$. Daraus folgt jedoch $|E| = \frac{|K|}{2} + 1$. Widerspruch. □

Entfernen eines Blattes in einem Baum:



13.5 Planarität

Ein ungerichteter Graph (E, K) ist planar gdw. er in der $(\mathbb{R}\times\mathbb{R})$-Ebene so darstellbar ist, dass die Kantenbögen, also die Strecken zwischen den Ecken, sich nicht überschneiden. Ein und derselbe Graph kann natürlich völlig verschiedenen dargestellt werden. Im Sinne der Definition genügt jedoch bereits eine überschneidungsfreie Darstellung für den Planaritätsnachweis.

Beispiel 13.5.1. *Der ungerichtete Graph* $(\{1, 2, 3, 4, 5\}, K)$ *mit*

$$K = \big\{(1,2),\,(2,3),\,(3,4),\,(4,5),\,(5,1),\\ (2,1),\,(3,2),\,(4,3),\,(5,4),\,(1,5)\big\}$$

ist planar.

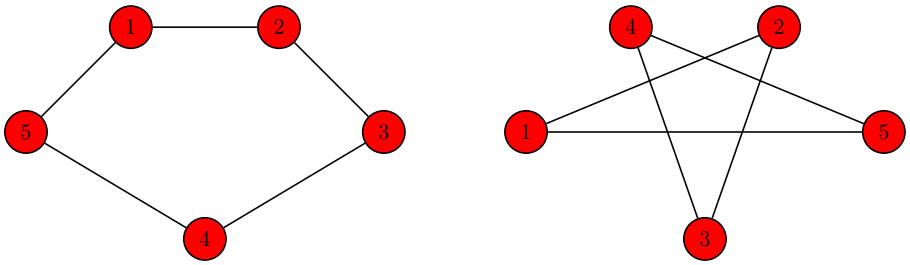


Abbildung 13.4: Planare vs. nicht-planare Darstellung

Zum einen werden Planaritätsbetrachtungen mit wachsender Komplexität der Graphen immer komplizierter, zum anderen ist der Planaritätsbegriff bei näherer Betrachtung unscharf. Wir sind dementsprechend an klaren Planaritätskriterien interessiert. Die folgenden Sätze sind uns bei Suche behilflich.

Satz 13.5.2 (Eulersche Polyederformel[2])**.** *Sei* $\mathcal{G} = (E, K)$ *ein endlicher, schlingenfreier, stark zusammenhängender, planarer und ungerichteter Graph. Dann gilt*

$$\textit{Anzahl der Flächen} = \tfrac{|K|}{2} - |E| + 2$$

Beweis. Wir führen eine vollständige Induktion über $n = \frac{|K|}{2} - |E| + 1$. Da $\mathcal{G}$ stark zusammenhängend ist, muss $|E| \leq \frac{|K|}{2} + 1$ und damit $n \geq 0$ gelten. Im IA sei daher $n = 0$ und damit $\frac{|K|}{2} = |E| - 1$. Gemäß Satz 13.4.1 hat $\mathcal{G}$ einen Baum (E, K') als Teilgraph. Gemäß Satz 13.4.4 gilt jedoch $|E| = \frac{|K'|}{2} + 1$ und damit $|K'| = |K|$. Also ist $\mathcal{G}$ selbst ein Baum und hat damit weder Kreise noch Schlingen. Also hat $\mathcal{G}$ keine innere Fläche und die Anzahl seiner Flächen ist 1.

$$\tfrac{|K|}{2} - |E| + 2 = \tfrac{|K|}{2} - \big(\tfrac{|K|}{2} + 1\big) + 2 = 1 \ .$$

[2]Leonhard Euler (1707–1783)

IH: Gelte die Aussage für n.

IS: Wir betrachten $n+1 > 0$. Dann ist $|E| < \frac{|K|}{2} + 1$ und $\mathcal{G}$ offenbar kein Baum (Satz 13.4.4). Also existiert ein Kreis $(e_0 \to e_1 \to \cdots \to e_n)$. Wir entfernen die Kanten $K'' = \{(e_0, e_1), (e_1, e_0)\}$, wodurch zwei vorher getrennte Flächen (links und rechts der Kante) zu einer Fläche verschmelzen. Für den Graphen $\mathcal{G}' = (E, K')$ mit $K' = K \setminus K''$ gilt die Eulersche Polyederformel gemäß IH, da

$$\frac{|K'|}{2} - |E| + 1 = \frac{|K| - 2}{2} - |E| + 1 = \frac{|K|}{2} - |E| + 1 - \frac{2}{2} = n + 1 - 1 = n$$

Also gilt

$$\begin{aligned} &\text{Anzahl der Flächen von } \mathcal{G} = \text{Anzahl der Flächen von } \mathcal{G}' + 1 \\ &= \frac{|K'|}{2} - |E| + 2 + 1 \qquad = \frac{|K| - 2}{2} - |E| + 3 \qquad = \frac{|K|}{2} - |E| + 2 \ . \end{aligned}$$

□

Satz 13.5.3. *Sei $\mathcal{G} = (E, K)$ ein endlicher, schlingenfreier, stark zusammenhängender, planarer und ungerichteter Graph mit $|K| \geq 6$. Dann gilt*

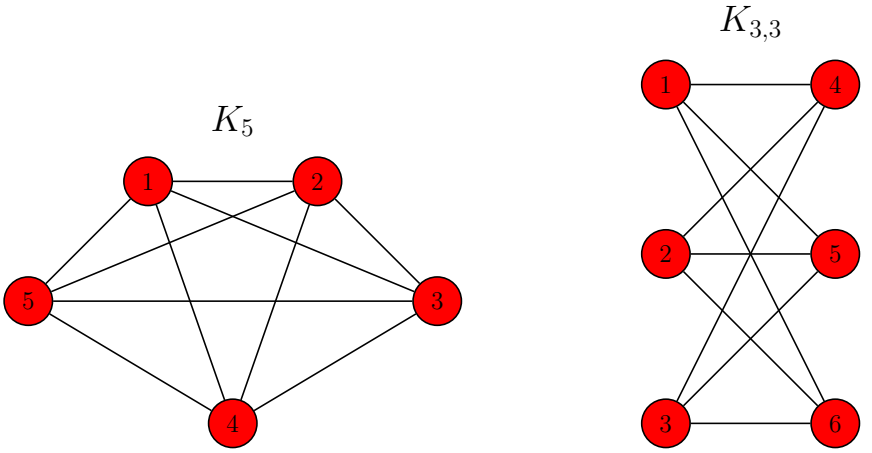
$$|K| \leq 6 \cdot |E| - 12 \ .$$

Beweis. Sei a die Anzahl der Flächen. Jede Fläche wird von mindestens 3 Kantenpaaren begrenzt und jedes Kantenpaar $\{(s,z),(z,s)\}$ kann nur 2 Flächen begrenzen. Ein Auflistung (nicht die Menge) der begrenzenden Kantenpaare für a Flächen hat demzufolge mindestens $3 \cdot a$ Einträge, wobei jedes Kantenpaar höchstens doppelt vorkommen kann. Daher benötigen wir mind. $\frac{3 \cdot a}{2}$ Kantenpaare, also $\frac{3 \cdot a}{2} \leq \frac{|K|}{2}$. Unter Nutzung der Eulerschen Polyederformel erhalten wir

$$3 \cdot \left(\frac{|K|}{2} - |E| + 2 \right) = \frac{3}{2}|K| - 3|E| + 6 \leq |K| \ .$$

Durch Umstellen erhalten wir die Behauptung. □

Wir können die vorhergehenden Sätze nun als Argument für die Nicht-Planarität des Graphen K_5 aus der folgenden Abbildung ins Feld führen. Der Graph ist endlich, schlingenfrei, stark zusammenhängend und ungerichtet und es sind $|K| = 20$ sowie $|E| = 5$. Damit kann er gemäß Satz 13.5.3 nicht planar sein, denn $20 > 6 \cdot 5 - 12 = 18$.



Dieses Beispiel zeigt, dass wir ein notwendiges Kriterium für die Planarität gefunden haben. Das Kriterium ist allerdings nicht hinreichend, denn Satz 13.5.3 steht im Einklang mit dem Graphen $K_{3,3}$:

$$18 = |K| \leq 6 \cdot |E| - 12 = 6 \cdot 6 - 12 = 24 \ .$$

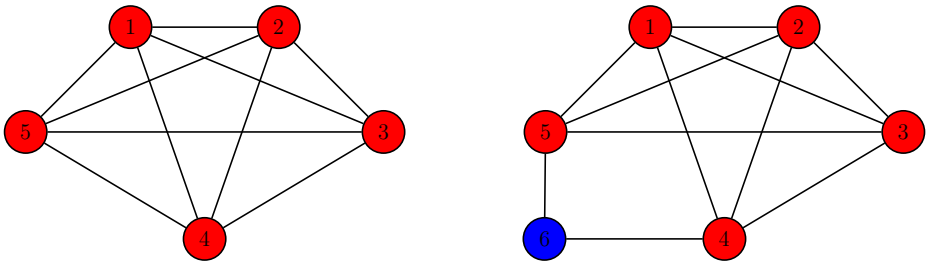
Jedoch ist dieser Graph ebenfalls nicht planar. Zur Etablierung eines notwendigen und hinreichendes Planaritätskriteriums benötigen wir einen neuen Begriff. Sei $\mathcal{G} = (E, K)$ ein ungerichteter, schlingenfreier Graph. Ein Graph $\left(E \cup \{e\}, K'\right)$ mit $e \notin E$ ist eine primitive Unterteilung von $\mathcal{G}$ gdw. eine Kante $(s,z) \in K$ existiert, so dass

$$K' = \Big(K \setminus \{(s,z),\ (z,s)\} \Big) \cup \{(s,e),\ (e,s),\ (z,e),\ (e,z)\} \ .$$

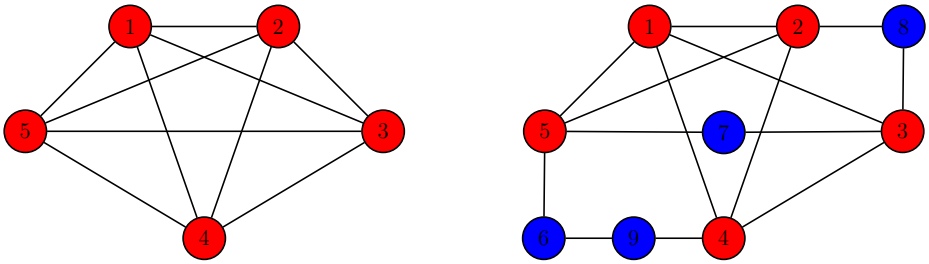
Ein Graph $\mathcal{G}' = (E', K')$ ist eine Unterteilung von $\mathcal{G}$ gdw. Graphen $\mathcal{G}_1, \ldots, \mathcal{G}_n$ existieren, so dass

- $\mathcal{G}_1 = \mathcal{G}$ und $\mathcal{G}_n = \mathcal{G}'$ und
- $\mathcal{G}_{i+1}$ eine primitive Unterteilung von $\mathcal{G}_i$ für alle $i < n$ ist.

Beispiel 13.5.4. *Wir sehen rechts eine primitive Unterteilung vom Graphen links.*

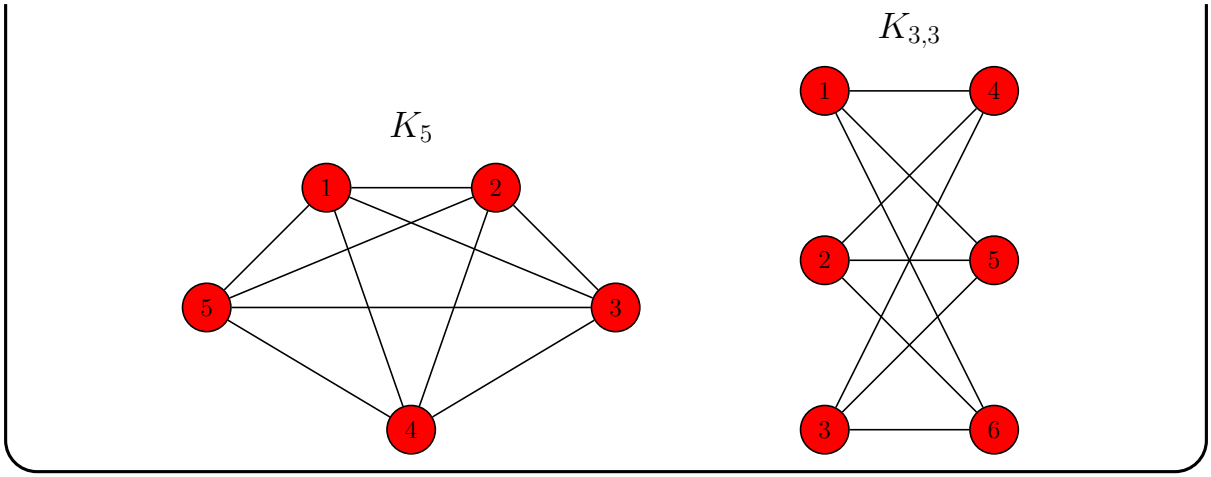


Wir sehen rechts eine Unterteilung vom Graphen links.



Satz 13.5.5 (Kuratowski[3])**.** *Ein ungerichteter Graph $\mathcal{G}$ ist genau dann planar, wenn er keinen Teilgraphen hat, der isomorph zu*

- *einer Unterteilung von K_5 oder*
- *einer Unterteilung von $K_{3,3}$ ist.*



Der Beweis ist zu komplex, um ihn hier anzugeben. Wir zeigen zumindest die Nicht-Planarität des Graphen $K_{3,3}$.

Beweis. (indirekt) Angenommen $K_{3,3} = (E, V)$ wäre planar. Dann liefert die Eulersche Polyederformel

$$\text{Anzahl } F \text{ der Flächen} = \frac{|K|}{2} - |E| + 2 = \frac{18}{2} - 6 + 2 = 5 \ .$$

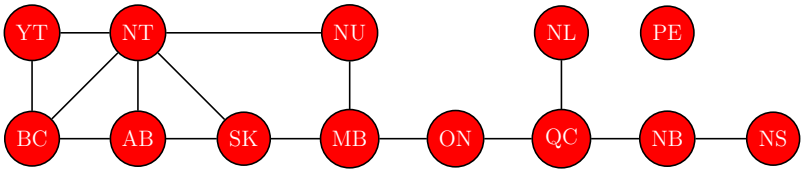
Für jede Fläche existiert ein begrenzender Kreis. Ein Kreis hat mindestens die Länge 3, aber $K_{3,3}$ hat keine Kreise der Länge 3. Daher ist jede Fläche von einem Kreis der Länge mindestens 4 begrenzt und wir benötigen mindestens $4F$ solche Flächenbegrenzer. Wie bereits eher (Satz 13.5.3) beobachtet, kann jedes Kantenpaar $\{(s, z), (z, s)\}$ nur 2 Flächen begrenzen. Es folgt, dass mindestens $\frac{4F}{2} = 2F = 10$ Kantenpaare oder $4F = 20$ Kanten benötigt werden. Der Graph $K_{3,3}$ hat jedoch nur 18 Kanten. Widerspruch. □

13.6 Färbbarkeit

Eine historische Anwendung der Graphplanarität besteht in der Färbung von Landkarten, wobei benachbarte Länder üblicherweise verschiedene Farben erhalten sollen. Modernere Anwendungen bestehen zum Beispiel in der Frequenzwahl von Mobilfunktürmen, wobei verschiedene Frequenzen bei Türmen mit überlappender Abdeckung verwendet werden sollen oder auch bei der Registerbelegung von Variablen in Maschinencode bezüglich gleichzeitig verwendeter Variablen in verschiedenen Registern. Wir konzentrieren uns nun auf die Landkartenanwendung.

Zunächst ignorieren wir alle Probleme, die sich in der Praxis ergeben: nichttriviale Landgrenzen, Wassergrenzen und Trivialgrenzen, die nur in einem Berührungspunkt bestehen (z.B. Saskatchewan und Nunavut). Wir fassen nun die Länder als Ecken auf und verbinden die Nachbarn durch Kanten.

[3] Kazimierz Kuratowski (1896–1980)



Sei $n \in \mathbb{N}$. Ein ungerichteter Graph (E, K) ist n-färbbar, falls eine Funktion

$$c\colon E \to \{i \in \mathbb{N} \mid 1 \leq i \leq n\}$$

existiert, so dass $c(s) \neq c(z)$ für alle $(s, z) \in K$. Man beachte: Für $n \geq 1$ ergibt sich

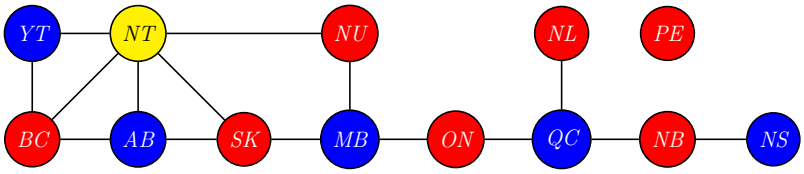
$$\{i \in \mathbb{N} \mid 1 \leq i \leq n\} = \{1, \ldots, n\}$$

und für $n = 0$

$$\{i \in \mathbb{N} \mid 1 \leq i \leq n\} = \{i \in \mathbb{N} \mid 1 \leq i \leq 0\} = \emptyset \ .$$

Ein Graph heißt also n-färbbar, falls alle Ecken mit n Farben $\{1, \ldots, n\}$ so belegt werden können, dass Nachbarn verschiedene Farben tragen.

Beispiel 13.6.1 (Fortsetzung)**.** *Der Kanada-Graph ist weder 0-, 1- noch 2-färbbar. (Ausprobieren!)*



Er ist jedoch 3-färbbar mit

$$1 = c(BC) = c(SK) = c(NU) = c(ON) = c(NL) = c(PE) = c(NB)$$
$$2 = c(YT) = c(AB) = c(MB) = c(QC) = c(NS)$$
$$3 = c(NT)$$

Wir wollen nun, ganz analog zu unserem Vorgehen bezüglich der Planarität, Färbbarkeitskriterien finden. Wir beginnen mit einigen einfachen Beobachtungen.

Lemma 13.6.2. *Sei $n \in \mathbb{N}$. Jeder n-färbbare Graph (E, K) ist schlingenfrei.*

Beweis. (Kontraposition) Sei (E, K) nicht schlingenfrei; d. h. K ist nicht irreflexiv. Also existiert $(e, e) \in K$ für $e \in E$. Für jede Funktion $c\colon E \to \{i \in \mathbb{N} \mid 1 \leq i \leq n\}$ gilt jedoch $c(e) = c(e)$ und damit kann die Färbbarkeit nicht erfüllt werden. □

Satz 13.6.3. *Ein ungerichteter Graph (E, K)*

1. *ist* 0*-färbbar genau dann, wenn* $E = \emptyset$.
2. *ist* 1*-färbbar genau dann, wenn* $K = \emptyset$.

Beweis.

1. ($\leftarrow$) Sei $E = \emptyset$ und damit auch $K = \emptyset$, da $K \subseteq E \times E$. Dann ist $c = \emptyset$ eine Funktion $c\colon \emptyset \to \emptyset$ und offenbar gilt $c(s) \neq c(z)$ für alle $(s, z) \in K$.

   ($\rightarrow$) Sei (E, K) 0-färbbar. Dann existiert eine Funktion $c\colon E \to \emptyset$. Allerdings existiert eine derartige Funktion nur falls $E = \emptyset$, da $c(e) \in \emptyset$ für alle $e \in E$ gelten muss.

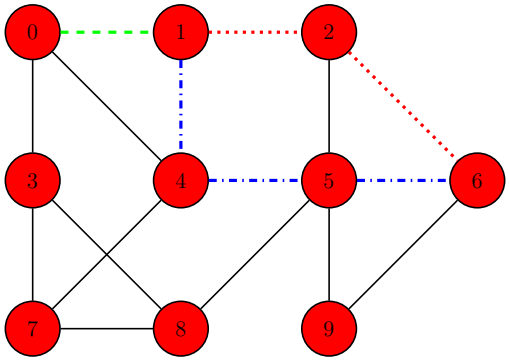
2. ($\leftarrow$) Sei $K = \emptyset$. Die Funktion $c\colon E \to \{1\}$ sei durch $c(e) = 1$ für alle $e \in E$ gegeben. Es gilt offenbar $c(s) \neq c(z)$ für alle $(s, z) \in K$.

   ($\rightarrow$) (Kontraposition) Sei $K \neq \emptyset$ und damit existiert $(s, z) \in K$ mit $s, z \in E$. Falls $s = z$, dann ist (E, K) nicht schlingenfrei und damit nicht 1-färbbar nach Lemma 13.6.2. Andernfalls, $s \neq z$ und es gilt $c(s) = c(z) = 1$ für jede Funktion $c\colon E \to \{1\}$. Damit ist (E, K) nicht 1-färbbar. □

Lemma 13.6.4. *Sei (E, K) ein Baum und $s, z \in E$ mit $s \neq z$. Dann existiert genau ein Pfad von s nach z.*

Beweis. Da (E, K) stark zusammenhängend ist, gibt es offenbar einen Weg von s nach z und damit einen Pfad von s nach z. Seien nun $(e_0 \to \cdots \to e_\ell)$ und $(e'_0 \to \cdots \to e'_k)$ verschiende Pfade von $e_0 = s = e'_0$ nach $e_\ell = z = e'_k$. O. B. d. A. sei $\ell \leq k$. Nun zeigen wir, dass die Verschiedenheit der Pfade widersprüchlich ist. Seien die Pfade also verschieden. Dann existiert der kleinste Index $1 \leq i \leq \ell$, so dass $e_i \neq e'_i$ (erste Ecke an der sich die beiden Pfade unterscheiden) und der kleinste Index $i \leq j \leq \ell$, so dass $e_j = e'_{j'}$ für ein $j' \leq k$ (erste Ecke ab erstem Unterschied, die wieder zum zweiten Pfad gehört). Offenbar ist dann $j' \geq i$ und $(e_{i-1} \to \cdots \to e_j)$, gefolgt von $(e'_{j'} \to \cdots \to e'_{i-1})$ ein Kreis, da entweder $j > i$ oder $j' > i$. Dies steht im Widerspruch zur Kreisfreiheit. □

Visualisierung zum Beweis:



Aus den Pfaden $(0 \to 1 \to 2 \to 6)$ und $(0 \to 1 \to 4 \to 5 \to 6)$ konstruieren wir die Pfade $(1 \to 2 \to 6)$ und $(6 \to 5 \to 4 \to 1)$, die zusammen den Kreis $(1 \to 2 \to 6 \to 5 \to 4 \to 1)$ bilden.

Wir haben also gute Kriterien für 0- und 1-Färbbarkeit gewonnen, müssen aber auch einsehen, dass es sich um sehr einfache Spezialfälle handelt. Die 2-färbbaren Graphen sind für uns schon interessanter, vor allem falls sie zusätzlich nicht 1-färbbar sind. Solche Graphen nennen wir bipartit.

Lemma 13.6.5. *Sei $n \in \mathbb{N}$. Ein ungerichteter Graph $\mathcal{G} = (E, K)$ ist n-färbbar gdw. der von Z gebildete Untergraph n-färbbar ist für jedes $Z \in (E/\sim_{\mathcal{G}})$.*

Satz 13.6.6. *Jeder Baum (E, K) ist 2-färbbar. Gilt weiterhin $|E| \geq 2$, so ist (E, K) bipartit.*

Beweis. Da (E, K) stark zusammenhängend ist, gilt offenbar $E \neq \emptyset$. Sei $r \in E$ also eine beliebige Ecke. Sei $d(r) = 0$ und für jede Ecke $e \in E \setminus \{r\}$ sei $d(e)$ die Länge des eindeutigen Pfades von r nach e (vgl. Lemma 13.6.4). Wir definieren die Funktion $c\colon E \to \{1, 2\}$, so dass

$$c(e) = \begin{cases} 1 & \text{falls } d(e) \text{ gerade ist} \\ 2 & \text{sonst.} \end{cases}$$

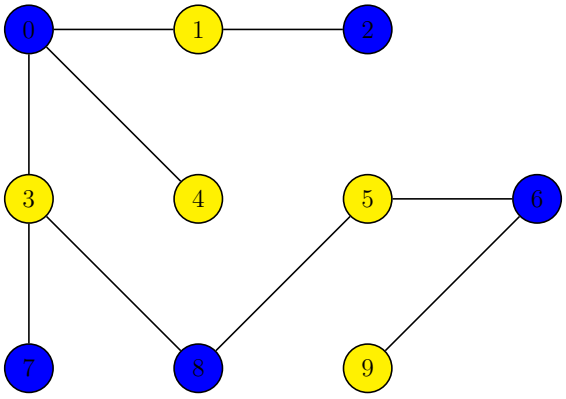
Sei nun $(s, z) \in K$ eine Kante. Da (E, K) schlingenfrei ist, gilt offenbar $s \neq z$. Wir müssen zeigen, dass $c(s) \neq c(z)$.

Falls $s = r$, dann gilt $d(s) = 0$ und damit $c(s) = 1$. In diesem Fall ist $(s \to z)$ der einzige Pfad von r nach z (vgl. Lemma 13.6.4), womit $d(z) = 1$ und damit $c(z) = 2$. Entsprechend für $z = r$. Sei also nun $r \notin \{s, z\}$ und $(e_0 \to \cdots \to e_k)$ der Pfad von r nach s (vgl. Lemma 13.6.4). Wir unterscheiden zwei weitere Fälle:

- Sei $z \in \{e_0, \ldots, e_k\}$ und damit existiert $j \leq k$ mit $e_j = z$. Dann muss $j = k - 1$ gelten, denn sonst gäbe es einen weiteren Pfad $(e_0 \to \cdots \to e_j \to s)$ von r nach s. Somit gelten $d(s) = k$ und $d(z) = k - 1$, womit $c(s) \neq c(z)$.

- Sei $z \notin \{e_0, \ldots, e_k\}$. Dann ist $(e_0 \to \cdots \to e_k \to z)$ der Pfad von r nach z, womit $d(s) = k$ und $d(z) = k + 1$ und damit wiederum $c(s) \neq c(z)$.

Die zweite Aussage folgt direkt aus Satz 13.6.3. □



Satz 13.6.7. *Ein schlingenfreier ungerichteter Graph (E, K) ohne Kreise ungerader Länge ist 2-färbbar.*

Beweis. Der Beweis erfolgt durch vollständige Induktion über $|K|$.

- Induktionsanfang: Sei $|K| = 0$. Dann ist (E, K) 1-färbbar und damit 2-färbbar nach Satz 13.6.3.
- Induktionshypothese: Gelte die Aussage für $|K| = n$.
- Induktionsschritt: Sei $|K| = n+2$. O. B. d. A. sei (E, K) stark zusammenhängend (vgl. Lemma 13.6.5) und $(s, z) \in K$ eine beliebige Kante. Da (E, K) schlingenfrei ist, gilt $s \neq z$. Gemäß der Induktionshypothese gilt die Aussage für

$$\mathcal{G}' = \Big(E,\ K \setminus \big\{(s, z), (z, s)\big\}\Big) \ .$$

  Sei $c\colon E \to \{1, 2\}$ die notwendige Färbung für $\mathcal{G}'$. Wir unterscheiden drei Fälle.

  - Sei $c(s) \neq c(z)$. Dann ist c offenbar auch eine Färbung für (E, K).
  - Sei $c(s) = c(z)$ und seien die Ecken s und z in der selben starken Zusammenhangskomponente von $\mathcal{G}'$. Dann existiert ein Weg und damit auch ein Pfad

$$(e_0 \to \cdots \to e_\ell)$$

    minimaler Länge ℓ von s nach z in $\mathcal{G}'$. Da $c(s) = c(z)$ muss ℓ gerade sein. Dann ist jedoch $(\underbrace{e_0}_{s} \to \cdots \to \underbrace{e_\ell}_{z} \to s)$ ein Kreis in (E, K) ungerader Länge im Widerspruch zur Annahme.

– Sei $c(s) = c(z)$ und seien die Ecken s und z in verschiedenen starken Zusammenhangskomponenten S und Z. Dann ist $c' \colon E \to \{1, 2\}$, so dass für alle $e \in E$

$$c'(e) = \begin{cases} c(e) & \text{falls } e \in E \setminus [s]_{\sim_{G'}} \\ 3 - c(e) & \text{sonst} \end{cases}$$

eine Färbung für $\mathcal{G}'$ und (E, K), da $c'(s) \neq c'(z)$. □

Im interessanten Fall liegen s und z in verschiedenen starken Zusammenhangskomponenten und haben die gleiche Färbung gemäß der Induktionshypothese. Gemäß Lemma 13.6.5 ist die Färbung von verschiedenen starken Zusammenhangskomponenten unabhängig. Wir invertieren die Färbung einer Komponente und erhalten dann eine gültige Färbung.

Satz 13.6.8. *Ein ungerichteter Graph (E, K) mit einem Kreis ungerader Länge ist nicht 2-färbbar.*

Beweis. (indirekt) Sei $(e_0 \to \cdots \to e_\ell)$ ein Kreis ungerader Länge und $c \colon E \to \{1, 2\}$ eine Färbung. O. B. d. A. sei $c(e_0) = 1$ und damit

$$c(e_i) = \begin{cases} 1 & \text{falls } i \text{ gerade ist} \\ 2 & \text{sonst.} \end{cases}$$

Dann gilt $c(e_0) \neq c(e_\ell)$, obwohl $e_0 = e_\ell$. Widerspruch. □

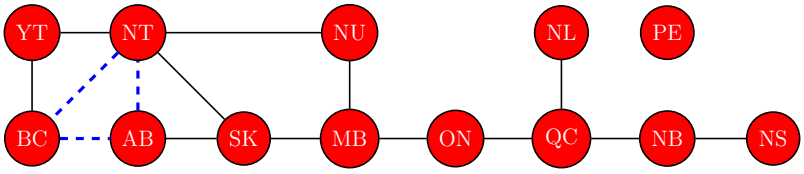
Wir erhalten ein notwendiges und hinreichendes Kriterium für die 2-Färbbarkeit.

Folgerung 13.6.9. *Ein schlingenfreier ungerichteter Graph (E, K) ist 2-färbbar genau dann, wenn er keinen Kreis ungerader Länge enthält.*

Der Kanada-Graph ist also nicht 2-färbbar, da der Kreis

$$(\text{BC} \to \text{AB} \to \text{NT} \to \text{BC})$$

der Länge 3 vorhanden ist.



Wie viele Farben braucht man nun aber, um beliebige Landkarten einfärben zu können?

Satz 13.6.10 (Vierfarbensatz, Appel & Haken[4] 1976–1989)**.** *Jeder schlingenfreie planare Graph ist* 4*-färbbar.*

Dieses Problem ist seit 1840 bekannt und es gab mehrere ungenügende Beweisversuche, zum Beispiel von Kempe (1879) und Tait (1880). Bei dem tatsächlichen Beweis handelt es sich um den ersten ernsten computergestützten Beweis. Es mussten viele Konfigurationen in über 1.000 Stunden per Computer verifiziert werden. Die Debatte über den Status von computergestützten Beweisen dauert bis heute an.

[4]Kenneth Ira Appel (1932–2013) und Wolfgang Haken (geb. 1928)

Literaturverzeichnis

[BS] S. Burris and H.P. Sankappanavar, *A Course in Universal Algebra*, The Millennium Edition, available at `https://www.math.uwaterloo.ca/~snburris/`