Sebastian Thomas

RWTH Aachen, WS 2016/17
17.10.2016–27.10.2016

Diskrete Strukturen

Vorlesungen 1 bis 3

1 Mathematische Logik

Zu Beginn geben wir einen Einblick in die mathematische Logik. Hierbei beschränken wir uns auf einige wenige Grundbegriffe, welche uns helfen sollen, ein Gefühl für die Struktur mathematischer Argumentführung zu entwickeln.
Die durch Anführungsstriche markierten Wörter in diesem Abschnitt werden nicht genauer präzisiert.

Aussagen

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

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

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

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

denn beim ersten Ausdruck scheitert die Zuordnung eines eindeutigen Wahrheitswertes an der mangelnden Objektivität, während dies beim zweiten Ausdruck nicht (ohne Weiteres) gelingt, da a, b und c nicht spezifiziert ([2]) sind.
Neben solchen einfachen Aussagen gibt es auch zusammengesetzte Aussagen wie etwa

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

Um diese Aussage zu analysieren, betrachten wir die Aussagen

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

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

Unsere ursprüngliche Aussage lässt sich dann umformulieren zu

„Wenn ‚es regnet' oder ‚es schneit', dann ‚die Straße ist nass'."

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

„Wenn (A oder B), dann C."

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

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

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

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

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

Syntax der Aussagenlogik

Nach unserem einführenden Beispiel werden wir nun die Logik beim Zusammensetzen von Aussagen systematisch studieren. Bevor wir die Wahrheitswerte zusammengesetzter Aussagen betrachten, führen wir zunächst eine formale Sprache ein. Die Wörter dieser Sprache werden uns als Ersatz für unsere konkreten Aussagen dienen.
Da wir noch nicht die Begriffe der Mengenlehre beherrschen, führen wir diese Sprache der Aussagenlogik etwas informell ein. Eine weitergehende Präzisierung wird erst in weiterführenden Veranstaltungen vorgenommen. Vgl. auch Anwendungsbeispiel (6.26).
Unter einem *Alphabet* verstehen wir eine vorgegebene Menge an „Symbolen", welche wir auch *Buchstaben* oder *Zeichen* des Alphabets nennen. Die *Wörter* einer *Sprache* entstehen dann einfach durch *Aneinanderreihung* dieser Buchstaben. Vgl. Definition (6.23) und Definition (6.25).

(1.1) Definition (aussagenlogische Formeln)**.**

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

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

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

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

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

- Die Aussagenvariablen sind Wörter in der Sprache der Aussagenlogik.

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

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

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

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

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

(1.2) Beispiel.

(a) Es ist A eine aussagenlogische Formel.

(b) Es ist 1 eine aussagenlogische Formel.

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

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

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

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

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

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

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

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

- Es binde $\neg$ stärker als alle anderen Junktoren.
- Es binde $\wedge$ stärker als $\vee$, $\Rightarrow$ und $\Leftrightarrow$.
- Es binde $\vee$ stärker als $\Rightarrow$ und $\Leftrightarrow$.

Nach Konvention (1.3) schreiben wir etwa $A \vee B \wedge \neg C$ statt $A \vee (B \wedge (\neg C))$, und wir schreiben $A \Rightarrow \neg B$ statt $A \Rightarrow (\neg B)$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1.6) Beispiel (aussagenlogische Formel)**.**

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

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

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

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

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

Beweis.

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

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

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

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

Semantik der Aussagenlogik

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

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

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

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

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

0-*stellige Junktoren.*

0	1

1-*stellige Junktoren.*

F	$\neg F$
1	0
0	1

2-*stellige Junktoren.*

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

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

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

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

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

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

(1.8) Beispiel.

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

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

Beweis.

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

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

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

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

(1.10) Beispiel.

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

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

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

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

Beweis.

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

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

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

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

□

Tautologien und Kontradiktionen

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

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

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

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

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

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

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

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

Beweis.

(a) Wir erstellen eine Wahrheitstafel:

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

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

(b) Wir erstellen eine Wahrheitstafel:

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

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

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

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

Logische Äquivalenz

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

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

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

Beweis. Wir erstellen eine Wahrheitstafel:

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

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

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

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

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

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

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

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

Beweis.

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

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

Wir halten einige oft benutzte logische Äquivalenzen fest:

(1.18) Beispiel.

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

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

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

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

(ii) *Idempotenz der Disjunktion.* Es gilt $A \vee A \equiv A$.

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

(ii) *Komplemente der Disjunktion.* Es gilt $A \vee \neg A \equiv 1$.

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

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

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

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

Beweis. Dies sei dem Leser zur Übung überlassen. □

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

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

Beweis. Dies sei dem Leser zur Übung überlassen. □

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

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

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

Beweis. Dies sei dem Leser zur Übung überlassen. □

Semantische Implikation

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

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

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

Beweis. Wir erstellen eine Wahrheitstafel:

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

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

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

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

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

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

Direkter Beweis

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

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

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

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

Beweis. Dies sei dem Leser zur Übung überlassen. □

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

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

Beweis. Dies sei dem Leser zur Übung überlassen. □

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

(1.28) Beispiel.

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

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

Beweis. Dies sei dem Leser zur Übung überlassen. □

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

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

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

Beweis. Dies sei dem Leser zur Übung überlassen. □

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

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

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

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

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

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

Somit ist auch n^2 gerade. □

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

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

Kontraposition

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

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

Beweis. Dies sei dem Leser zur Übung überlassen. □

Wir verdeutlichen die Strategie der Kontraposition wieder an einem Beispiel.

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

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

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

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

Indirekter Beweis

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Beweis einer Äquivalenz

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

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

Beweis. Dies sei dem Leser zur Übung überlassen. □

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

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

Disjunktive und konjunktive Normalform

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

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

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

(1.39) Beispiel. Es ist

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1.41) Beispiel.

(a) Die aussagenlogische Formel

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

ist in disjunktiver Normalform.

(b) Die aussagenlogische Formel

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

ist in konjunktiver Normalform.

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

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

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

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

Die aussagenlogische Formel

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

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

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

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

Die aussagenlogische Formel

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

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

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

(1.43) Beispiel.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Beweis.

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

jedem Fall der Wahrheitswert von F unter der Interpretation $v_1 \dots v_n$ gleich dem $v_1 \dots v_n$ zugewiesenen Wahrheitswert in der potentiellen Wahrheitstafel.

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

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

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

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

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

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

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

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

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

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

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

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

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

Beweis.

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

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

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

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

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

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

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

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

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

Beweis.

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

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

(1.48) Beispiel.

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

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

gegeben.

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

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

gegeben.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

□

Prädikate

Zum Abschluss dieses Abschnitts skizzieren wir noch einige Aspekte der Prädikatenlogik. Dabei werden wir diesen Kalkül noch knapper und informeller als den der Aussagenlogik behandeln, da eine weiterführende Formalisierung ohne Kenntnis einiger mathematischer Strukturen sehr abstrakt und nur schwer verständlich ist. Weitergehende Präzisierungen überlassen wir daher weiterführenden Vorlesungen. Der Zweck dieser kurzen Abhandlung ist es, eine intuitive Idee von Ausdrücken der Form $\exists x : P(x)$ zu bekommen.
Während die Aussagenlogik Modelle für Aussagen und deren logische Zusammensetzungen studiert, wird in der Prädikatenlogik auf die innere Struktur von Aussagen eingegangen. Anstelle von Aussagen betrachtet man nun Prädikate über einem zuvor festgelegten *Individuenbereich* (auch *Diskursuniversum* genannt). Ein *Prädikat* (manchmal etwas irreführend auch *Aussageform* genannt, vgl. Definition (1.1)(b)) ist hierbei eine „Eigenschaft“ oder eine „Beziehung“, welche für die Individuen aus dem zuvor festgelegten Bereich entweder gilt oder nicht. Betrachtet man ein Prädikat von konkreten Individuen, so erhält man eine Aussage.
Beispielsweise ist „Anne speist mit Christian.“ eine Aussage. Betrachten wir nun den Individuenbereich „Freundeskreis (des Dozenten)“, so sind „Anne“ und „Christian“ Individuen und es ist „… speist mit …“ ein zweistelliges Prädikat über diesem Bereich (zweistellig, da das Prädikat zwei Individuen in Verbindung setzt).

Syntax der Prädikatenlogik

So wie in der Aussagenlogik die Aussagen durch Aussagenvariablen abstrahiert werden, treten bei der Formalisierung der Prädikatenlogik nun *Individuenvariablen* an die Stelle von Individuen und *Prädikatvariablen* an die Stelle der Prädikate. So lässt sich oben genanntes Beispiel etwa durch $P(x, y)$ formalisieren, wobei „Anne“ durch x bzw. „Christian“ durch y sowie „... speist mit ...“ durch P ersetzt wird.
Desweiteren können in einer *prädikatenlogischen Formel* noch die aus der Aussagenlogik bekannten *Junktoren*, Hilfsklammern und die sogenannten *Quantoren* auftreten. Der *Existenzquantor* (Symbol $\exists$) formalisiert hierbei die Existenz eines Individuums, für welches ein gewisses Prädikat gilt, während der *Allquantor* (Symbol $\forall$) für die Allgemeingültigkeit des Prädikats für alle Individuen steht. Dabei wird $(\exists x)(P(x))$ als *es gibt ein x mit $P(x)$* und $(\forall x)(P(x))$ als *für alle x gilt $P(x)$* gelesen. Um die Bildung von Klammern zu reduzieren, schreiben wir meist $\exists x : P(x)$ statt $(\exists x)(P(x))$ sowie $\forall x : P(x)$ statt $(\forall x)(P(x))$.
Bei mehreren Individuenvariablen kommt es auf die Art und die Reihenfolge der Quantoren an. Wollen wir etwa die beiden in $P(x, y)$ vorkommenden *freien* Individuenvariablen x und y durch Quantoren *binden*, so haben wir die vier Möglichkeiten $\exists x : \exists y : P(x, y)$, $\exists x : \forall y : P(x, y)$, $\forall x : \exists y : P(x, y)$ und $\forall x : \forall y : P(x, y)$. Steht $P(x, y)$ wie oben für das Prädikat „... speist mit ...“, so steht $\exists x : \exists y : P(x, y)$ für die Aussage, dass es zwei nicht notwendigerweise verschiedene Individuen gibt ([14]), welche miteinander speisen („es gibt ein Paar von Individuen, welches miteinander speist“), während $\forall x : \forall y : P(x, y)$ der Aussage entspricht, dass jeder mit jedem speist. Die prädikatenlogische Formel $\exists x : \forall y : P(x, y)$ repräsentiert die Aussage, dass es ein Individuum gibt, welches mit allen (anderen und sich selbst) speist, während $\forall x : \exists y : P(x, y)$ die Existenz eines Tischpartners für jedes Individuum formalisiert.

Semantik der Prädikatenlogik

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

Logische Äquivalenz von prädikatenlogischen Formeln

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

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

und $\exists x : \neg P(x)$ sowie $\neg(\exists x : P(x))$ und $\forall x : \neg P(x)$ jeweils logisch äquivalente prädikatenlogische Formeln.

Zur Verwendung von logischen Symbolen

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

Sprachliche Konventionen

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

Sebastian Thomas

RWTH Aachen, WS 2016/17
26.10.2016–07.11.2016

Diskrete Strukturen

Vorlesungen 3 bis 5

2 Mengen

Unser nächstes Ziel ist die Einführung von Mengen und einiger damit verbundener Konzepte wie Mengenoperationen. Hierbei wollen wir nicht genau sagen, was eine Menge ist, sondern lediglich, was wir uns hierunter vorstellen und wie wir mit Mengen umgehen. Um Mengen auf einer soliden mathematischen Basis einführen zu können, bedarf es weiterer Formalismen innerhalb der *mathematischen Logik*, welcher den Rahmen unserer einführenden Veranstaltung sprengen würde. Für das erfolgreiche Studium der meisten Gebiete der Informatik (und auch der Mathematik) genügt jedoch eine Kenntnis über Mengen im Umfang dieser Anfängervorlesung. Dafür ist es nicht wichtig, zu wissen, was eine Menge ist, sondern eine gewisse Vorstellung von Mengen zu entwickeln und den Umgang mit Mengen zu verinnerlichen.
Die durch Anführungsstriche markierten Wörter in diesem Abschnitt werden nicht genauer präzisiert.

Begriffsbildung

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

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

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

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

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

Nach (2.1)(a) ist eine Menge X allein durch ihren „Umfang“ bestimmt, d.h. durch ihre Elemente festgelegt (*Extensionalitätsprinzip*): Für ein gegebenes Objekt x gilt entweder $x \in X$ oder $x \notin X$. Demnach kann ein Objekt auch nicht „mehrfach“ als Element vorkommen und es gibt auch keine „Ordnung“ der Elemente.
Im Folgenden werden wir einige Notationen zur Beschreibung von Mengen angeben. In aller Regel erfolgt eine solche Beschreibung durch die Angabe einer „Eigenschaft“ ([1]), welche die Elemente einer Menge erfüllen, oder durch eine einfache „Aufzählung“ ihrer Elemente. Letzteres wird vor allem bei einer Menge mit „endlich“ vielen Elementen gemacht – etwas unpräzise aber auch bei „unendlich“ vielen Elementen, sofern aus dem Kontext klar ist (bzw. klar sein sollte), welche Objekte aufgezählt werden.

(2.2) Notation.

(a) Es seien eine Menge X und eine Eigenschaft φ gegeben. Besteht X aus genau denjenigen Objekten, welche φ erfüllen, so schreiben wir

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

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

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

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

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

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

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

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

Wir erinnern daran, dass das „oder“ in der Mathematik, siehe Notation (2.2)(c), gemäß der semantischen Interpretation des Junktors $\vee$ in Definition (1.7)(b) für ein *einschließendes oder* steht: Für Objekte x, a und b gilt also genau dann $x = a$ oder $x = b$, wenn $x = a$ und $x \neq b$, oder wenn $x \neq a$ und $x = b$, oder wenn $x = a$ und $x = b$ gilt, d.h. wenn das Objekt x gleich einem oder beiden der beiden Objekte a und b ist. ([2]) Wenn wir sagen möchten, dass das Objekt x identisch zu genau einem der beiden Objekte a und b ist, so betonen wir dies und sagen „entweder $x = a$ oder $x = b$“. Ähnlich für beliebig viele Objekte.
Entsprechend bedeutet die Existenz eines Objektes mit einer vorgegebenen Eigenschaft, vgl. Notation (2.2)(d), dass es *mindestens* ein Objekt mit dieser Eigenschaft gibt.
Obwohl es sehr natürlich scheint, Mengen durch Eigenschaften zu beschreiben, möchten wir betonen, dass *nicht* jede Eigenschaft eine Menge beschreibt. Beispielsweise ist es nicht möglich, $\{x \mid x \text{ ist eine Menge}\}$ zu bilden. Es ist jedoch stets möglich, Mengen wie in (2.2)(b) zu bilden, d.h. Mengen, deren Elemente alle in einer bereits gegebenen Menge X liegen und zusätzlich eine gegebene Eigenschaft φ erfüllen. (*Aussonderung*)

(2.3) Beispiel. Wir wollen davon ausgehen, dass wir wissen, was die folgenden Mengen sind. ([3])

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

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

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

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

gegeben.

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

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

gegeben.

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

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

gegeben.

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

(2.4) Beispiel.

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

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

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

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

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

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

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

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

(2.6) Beispiel.

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

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

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

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

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

Wir können Mengen auch benutzen, um Zusammenfassungen des täglichen Lebens zu modellieren ([4]):

(2.7) Anwendungsbeispiel.

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

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

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

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

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

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

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

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

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

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

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

(2.10) Beispiel.

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

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

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

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

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

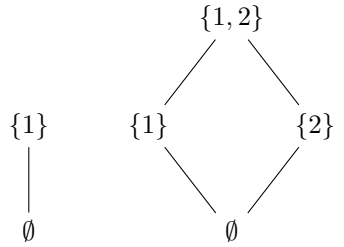


Abbildung 1: Teilmengen von $\{1\}$ und $\{1, 2\}$

Teilmengen

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

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

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

(2.12) Beispiel.

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

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

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

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

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

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

$$\mathrm{Pot}(X) := \{U \mid U \subseteq X\}.$$

(2.15) Beispiel.

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

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

Familien

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

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

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

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

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

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

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

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

(a) Es seien eine Menge I und für jedes $i \in I$ ein Objekt x_i gegeben. Wir nennen $x = (x_i)_{i \in I}$ eine *Familie* über I. Die Menge I wird *Indexmenge* von x genannt, ihre Elemente heißen *Indizes* (oder *Stellen*) von x. Für $i \in I$ heißt x_i die *Komponente* (oder der *Eintrag*) von x an der Stelle i.

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

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

(2.17) Beispiel.

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

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

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

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

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

(2.18) Beispiel.

(a) Es sei eine Familie x über $\{-1, 1\}$ gegeben durch $x = (i^2)_{i \in \{-1,1\}}$. Ferner sei eine Familie y über $\{-1, 1\}$ gegeben durch $y_{-1} = 1$, $y_1 = 1$. Dann ist $x = y$.

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

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

Beweis.

(a) Wegen

$$x_{-1} = (-1)^2 = 1 = y_{-1},$$
$$x_1 = 1^2 = 1 = y_1$$

gilt $x = y$.

(b) Wegen

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

gilt $x \neq y$.

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

(2.19) Anwendungsbeispiel.

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

$$K = \{\text{Hängeschrank}, \text{Bodenschrank}, \text{Schublade}, \text{Backofen}, \text{Kühlschrank}, \text{Kühltruhe}, \text{Waschmaschine}\},$$

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

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

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

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

auffassen.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Beweis.

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

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

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

(2.22) Beispiel. Es seien Familien a, b, c, d, e, f, g, h in $\{-1, 1\}$ über $\{0, 1, 2\}$ gegeben durch

$$\begin{array}{lll} a_0 = -1, & a_1 = -1, & a_2 = -1, \\ b_0 = 1, & b_1 = -1, & b_2 = -1, \\ c_0 = -1, & c_1 = 1, & c_2 = -1, \\ d_0 = 1, & d_1 = 1, & d_2 = -1, \\ e_0 = -1, & e_1 = -1, & e_2 = 1, \\ f_0 = 1, & f_1 = -1, & f_2 = 1, \\ g_0 = -1, & g_1 = 1, & g_2 = 1, \\ h_0 = 1, & h_1 = 1, & h_2 = 1. \end{array}$$

Dann ist

$$\{-1, 1\}^{\{0,1,2\}} = \{a, b, c, d, e, f, g, h\}.$$

(2.23) fehlt

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

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

Da für jede Menge I insbesondere $I = \{i \mid i \in I\}$ gilt, haben wir nach Notation (2.24) für jede Familie x über I stets

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

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

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

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

Tupel

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

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

(a) Ein *n-Tupel* ist eine Familie über $[1, n]$. ([5])
Für ein n-Tupel x schreiben wir auch

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

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

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

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

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

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

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

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

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

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

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

(2.29) Beispiel.

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

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

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

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

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

(2.30) Beispiel.

(a) Es sei ein Quadrupel x gegeben durch

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

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

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

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

Beweis.

(a) Es ist

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

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

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

gilt $x \neq y$.

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

(2.31) Beispiel. Es ist

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

(2.32) Anwendungsbeispiel.

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

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

modelliert.

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

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

(d) Ein Speicher mit 256 Speicherplätzen lässt sich als 256-Tupel auffassen. ([6])

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

Anwendungsbeispiel. Es sei $n \in \mathbb{N}_0$ gegeben. Eine Interpretation der Aussagenvariablen $A_1, \ldots, A_n$ lässt sich als n-Tupel in $\{0, 1\}$ modellieren. ([7])

Folgen

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

(2.33) Definition (Folge)**.** Eine *Folge* ist eine Familie über $\mathbb{N}$. ([8])
Für eine Folge x schreiben wir auch

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

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

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

[7] Die vereinbarte Notation aus Definition (1.7)(a) entspricht dann der Notation für Strings aus Definition (6.23).

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

Innere Mengenoperationen

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

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

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

heißt *Differenz* von X und Y.

(2.36) Beispiel. Es ist

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

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

(a) (i) Es seien eine nicht-leere Menge I und eine Familie von Mengen $X = (X_i)_{i \in I}$ über I ([9]) gegeben. Die Menge

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

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

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

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

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

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

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

heißt *Vereinigung* von X.

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

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

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

(2.38) Beispiel.

(a) (i) Es ist

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

(ii) Es ist

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

(b) (i) Es ist

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

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

(ii) Es ist

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

Beweis. Dies sei dem Leser zur Übung überlassen. □

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

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

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

(b) Es ist

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

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

(2.40) Bemerkung.

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

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

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

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

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

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

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

(e) (i) Für alle Mengen X, Y, Z ist

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

□

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

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

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

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

(a) Die Menge X und Y sind disjunkt.

(b) Die Menge X und Z sind disjunkt.

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

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

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

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

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

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

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

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

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

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

(2.44) Beispiel. Es ist

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

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

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

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

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

heißt *symmetrische Differenz* von X und Y.

(2.47) Beispiel. Es ist

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

Beweis. Es ist

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

Äußere Mengenoperationen

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(2.49) Beispiel.

(a) Es ist

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

(b) Es ist

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

Beweis.

(a) Es ist

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

(b) Es ist

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

□

Anwendung: Datenbanken

Als Anwendung der Konzepte einer Familie und eines kartesischen Produkts präsentieren wir ein mathematisches Modell für Datenbanken.

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

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

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

und den Domänen

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

auffassen, wobei Strings ein Modell für die „Menge der Strings“ darstelle ([10]). Ein typischer Datensatz ist dann etwa gegeben durch

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

Matrizen

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

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

(a) Eine $(m \times n)$-*Matrix* ist eine Familie über $[1, m] \times [1, n]$.
Für eine $(m \times n)$-Matrix x schreiben wir auch

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

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

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

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

(2.51) Beispiel.

(a) Es ist

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

eine (3×4)-Matrix.

[10] Für eine mögliche Formalisierung siehe Definition (6.23).

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

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

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

(c) Es ist

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

eine (2×2)-Matrix.

(2.52) Beispiel.

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

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

Dann ist

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

(b) Es ist

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

(c) Es ist

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

Beweis.

(a) Es ist

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

(b) Es seien

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

Wegen

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

gilt $x \neq y$.

(c) Es seien

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

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

(2.53) Beispiel. Es ist

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

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

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

modelliert.

Matrizen werden unter anderem zur knappen Beschreibung linearer Gleichungssysteme genutzt, siehe Abschnitt 14.
Bei Matrizen, welche nur aus genau einer Zeile oder genau einer Spalte bestehen lassen wir unter Missbrauch von Notationen den jeweils zweiten Index für die Einträge weg:

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

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

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

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

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

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

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

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

die *i-te Zeile* von x.

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

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

die *j-te Spalte* von x.

(2.57) Beispiel. Es sei

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

(a) Es ist

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

(b) Es ist

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

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

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

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

notieren wir als

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

Ähnlich für andere Zusammensetzungen.

Sebastian Thomas

RWTH Aachen, WS 2016/17
07.11.2016–09.11.2016

Diskrete Strukturen

Vorlesungen 5 und 6

3 Abbildungen

In diesem Abschnitt führen wir Abbildungen zwischen Mengen ein. Während Mengen von der Vorstellung her starre Gebilde sind, stellen wir uns unter einer Abbildung eine „Vorschrift“ vor, welche die Elemente einer Menge eindeutig auf gewisse Elemente einer anderen Menge „abbildet“.

Begriffsbildung

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

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

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

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

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

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

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

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

(3.2) Beispiel.

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

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

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

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

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

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

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

eine Abbildung.

Beweis.

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

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

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

(3.3) Beispiel. Es ist

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

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

Wir betrachten noch einige Modellierungen von alltäglichen Zuordnungen:

(3.4) Anwendungsbeispiel.

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

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

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

(3.5) Anwendungsbeispiel. Es sei $n \in \mathbb{N}_0$ gegeben. Eine potentielle Wahrheitstafel für die Aussagenvariablen $A_1, \ldots, A_n$ lässt sich als Abbildung von $\{0,1\}^n$ nach $\{0,1\}$ ([2]) modellieren.

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

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

(3.7) Beispiel.

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

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

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

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

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

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

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

Dann ist $f \neq f'$.

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

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

Beweis.

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

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

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

(b) Wegen

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

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

(c) Wegen

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

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

(d) Wegen

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

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

Zusammenhang zu Familien

Zwischen Abbildungen und Familien besteht ein enger Zusammenhang:

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

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

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

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

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

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

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

Komposition von Abbildungen

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

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

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

heißt *Kompositum* von f und g.

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

Beweis. Für $x \in \mathbb{N}$ ist

$$g(f(x)) = g(x+1) = 2(x+1)^2.$$ □

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Beweis.

(a) Für $x \in \mathbb{Q}_{>0}$ ist

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

und für $y \in \mathbb{Q}_{<0}$ ist

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

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

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

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

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

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

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

(3.21) Proposition.

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

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

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

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

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

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

Beweis.

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

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

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

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

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

Für iterierte Komposita verwenden wir folgende vereinfachte Schreibweise. ([3])

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

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

Wenn f invertierbar ist, so setzen wir

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

für $k \in \mathbb{N}$.

Injektivität und Surjektivität

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

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

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

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

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

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

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

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

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

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

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

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

(3.24) Beispiel.

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

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

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

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

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

[3] Bzgl. Komposition wird für jede Menge X die Menge der Abbildungen $\mathrm{Map}(X,X)$ ein Monoid, siehe Bemerkung (10.1) und Definition (6.12). Die Potenznotation in (3.22) entspricht dann gerade der Potenznotation in abstrakten (multiplikativ geschriebenen) Monoiden, siehe Notation (6.40)(a).

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

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

Somit ist f surjektiv.
Insgesamt ist f bijektiv. □

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

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

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

(3.26) Beispiel.

(a) Es ist

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

(b) Es ist

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

(c) Es ist

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

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

(a) Für eine Teilmenge U von X heißt

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

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

(b) Für eine Teilmenge V von Y heißt

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

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

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

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

Beweis. Es gilt

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

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

(a) Die folgenden Aussagen sind äquivalent.

(i) Die Abbildung f ist injektiv.

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

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

(b) Die folgenden Aussagen sind äquivalent.

(i) Die Abbildung f ist surjektiv.

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

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

(c) Die folgenden Aussagen sind äquivalent.

(i) Die Abbildung f ist bijektiv.

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

(iii) Die Abbildung f ist invertierbar.

Beweis.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Restriktion von Abbildungen

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

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

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

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

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

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

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

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

(a) Es ist

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

(b) Es ist

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

(c) Es ist

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

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

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

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

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

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

Indikatorfunktion

Ein Zusammenhang zwischen Teilmengen und Abbildungen ist durch die Indikatorfunktion gegeben, welche eine Bijektion zwischen der Potenzmenge einer gegebenen Menge und den Abbildungen von dieser Menge in eine zweielementige Menge liefert, siehe Satz (3.36).

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

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

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

Gemäß Konvention (3.9) fassen wir eine Indikatorfunktion ggf. auch als Familie auf und sprechen dann von einer *Indikatorfamilie* bzw. in den Spezialfällen von einem *Indikatortupel* bzw. einer *Indikatorfolge* bzw. einer *Indikatormatrix*.

(3.35) Beispiel.

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

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

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

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

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

$$\begin{aligned} &\mathrm{Pot}(X) \to \mathrm{Map}(X,\{0,1\}),\ U \mapsto \chi_U, \\ &\mathrm{Map}(X,\{0,1\}) \to \mathrm{Pot}(X),\ f \mapsto \{x \in X \mid f(x) = 1\} \end{aligned}$$

sind zueinander invers.

Beweis. Für den Zweck dieses Beweises sei

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

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

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

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

$$(\mathrm{U}_- \circ \chi_-)(U) = \mathrm{U}_{\chi_U} = \{x \in X \mid \chi_U(x) = 1\} = \{x \in X \mid x \in U\} = U = \mathrm{id}_{\mathrm{Pot}(U)}(U).$$

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

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

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

Endlichkeit und Kardinalität

Zum Schluss dieses Abschnitts betrachten wir noch das Konzept der Kardinalität einer endlichen Menge.

(3.37) Definition (Gleichmächtigkeit)**.** Es seien Mengen X und Y gegeben. Wir sagen, dass X *gleichmächtig* zu Y ist, falls es eine Bijektion von X nach Y gibt.

(3.38) Beispiel.

(a) Die Menge $\{1, 2, 3\}$ ist gleichmächtig zur Menge $\{4, 5, 6\}$.

(b) Die Menge $\mathbb{N}$ ist gleichmächtig zu $\mathbb{Z}$.

Beweisskizze.

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

(b) Die Abbildung $f\colon \mathbb{N} \to \mathbb{Z}$ gegeben für $x \in \mathbb{N}$ durch

$$f(x) = \begin{cases} \frac{x}{2}, & \text{falls } x \text{ gerade,} \\ \frac{1-x}{2}, & \text{falls } x \text{ ungerade,} \end{cases}$$

ist eine Bijektion. □

(3.39) Definition ((un)endliche Menge)**.** Es sei eine Menge X gegeben.

(a) Wir sagen, dass X *endlich* ist, falls es ein $n \in \mathbb{N}_0$ derart gibt, dass X gleichmächtig zu $[1, n]$ ist, und ansonsten, dass X *unendlich* ist.

(b) Es seien ein $n \in \mathbb{N}_0$ und eine Menge X gegeben. Eine Bijektion von $[1, n]$ nach X wird *Abzählung* von X genannt.

(3.40) Beispiel.

(a) Die Menge $\{1, 3, 17\}$ ist endlich.

(b) Die Mengen $\mathbb{N}$ und $\{x \in \mathbb{N} \mid x \text{ gerade}\}$ sind unendlich.

(c) Die leere Menge ist endlich.

(d) Die Menge $\{x \in \mathbb{R} \mid x^3 + 2x = 3x^2\}$ ist endlich.

Es lässt sich zeigen, dass es für jede endliche Menge X genau ein $n \in \mathbb{N}_0$ derart gibt, dass X gleichmächtig zu $[1, n]$ ist.

(3.41) Definition (Kardinalität)**.** Es seien eine endliche Menge X und ein $n \in \mathbb{N}_0$ derart gegeben, dass X gleichmächtig zu $[1, n]$ ist. Wir nennen

$$|X| := n$$

die *Kardinalität* (oder *Mächtigkeit*) von X.

(3.42) Beispiel.

(a) Es ist $|\{1, 3, 17\}| = 3$.

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

(c) Es ist $|\{\{1\}\}| = 1$.

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

Sebastian Thomas

RWTH Aachen, WS 2016/17
09.11.2016–10.11.2016

Diskrete Strukturen

Vorlesungen 6 und 7

4 Relationen

Durch Relationen werden Beziehungen zwischen den Elementen einer Menge formalisiert. In diesem Abschnitt studieren wir Eigenschaften von allgemeinen (binären) Relationen.

Begriffsbildung

Wir beginnen mit der Definition einer Relation.

(4.1) Definition (Relation)**.** Es sei eine Menge X gegeben. Eine *Relation* (genauer *binäre Relation*) auf X ist eine Teilmenge von $X \times X$.
Es seien eine Relation r auf X und $x, y \in X$ gegeben. Falls $(x, y) \in r$ ist, so sagen wir, dass x bzgl. r in *Relation* zu y *steht* und schreiben $x\ r\ y$.

Etwas allgemeiner lässt sich für Mengen X und Y eine *Relation* zwischen X und Y als Teilmenge von $X \times Y$ definieren. Wir werden dieses Konzept in dieser Veranstaltung nicht weiter verfolgen.

(4.2) Beispiel.

(a) Für $m, n \in \mathbb{N}$ gelte $m < n$, falls es ein $p \in \mathbb{N}$ mit $n = p + m$ gibt. Dann ist $<$ eine Relation auf $\mathbb{N}$. Als Teilmenge von $\mathbb{N} \times \mathbb{N}$ ist $<$ gegeben durch

$$< = \{(m, n) \in \mathbb{N} \times \mathbb{N} \mid \text{es gibt ein } p \in \mathbb{N} \text{ mit } n = p + m\}.$$

(b) Es sei eine Menge X gegeben. Dann ist $\subseteq$ eine Relation auf $\mathrm{Pot}(X)$. Wir nennen $\subseteq$ die *Teilmengenrelation* (oder *Inklusionsrelation* oder *Inklusion*) auf $\mathrm{Pot}(X)$. Als Teilmenge von $\mathrm{Pot}(X) \times \mathrm{Pot}(X)$ ist $\subseteq$ gegeben durch

$$\subseteq = \{(U, V) \in \mathrm{Pot}(X) \times \mathrm{Pot}(X) \mid \text{für } x \in U \text{ gilt } x \in V\}.$$

(c) Es sei eine Menge X gegeben. Dann ist $=$ eine Relation auf X. Wir nennen $=$ die *Gleichheitsrelation* (oder *Gleichheit*) auf X. Als Teilmenge von $X \times X$ ist $=$ gegeben durch

$$= = \{(x, x) \mid x \in X\}.$$

(d) Es sei eine Menge X gegeben. Dann ist $X \times X = \{(x, y) \mid x, y \in X\}$ eine Relation auf X, die *Allrelation* auf $X \times X$.

(e) Es ist $\{(1,1), (2,2), (3,3), (2,1), (3,1), (3,2)\}$ eine Relation auf $\{1, 2, 3\}$.

Wie in Beispiel (4.2)(a), (b), (c) schon angedeutet, ist es üblich, Relationen durch Angabe der Eigenschaft, welche für die in Relation stehenden Elemente erfüllt ist, zu definieren. Dies ist äquivalent zur Angabe der Teilmenge des kartesischen Produkts und meistens etwas leserlicher.
Wir geben noch einige Modellierungen von Beziehungen aus dem täglichen Leben durch Relationen an:

(4.3) Anwendungsbeispiel.

(a) Die Einwohner von Aachen seien als Elemente einer Menge A modelliert. Für $a, b \in A$ gelte genau dann $a\ n\ b$, wenn der durch a modellierte Einwohner ein Nachkomme des durch b modellierten Einwohners ist. Dann ist n eine Relation auf A.

(b) Die Studierenden des Moduls *Diskrete Strukturen* seien als Elemente einer Menge D modelliert. Für $s, t \in D$ gelte genau dann $s\ e\ t$, wenn der oder die durch s modellierte Studierende die gleichen Eltern wie der oder die durch t modellierte Studierende hat. Für $s, t \in D$ gelte genau dann $s\ g\ t$, wenn der oder die durch s modellierte Studierende den gleichen Geburtstag wie der oder die durch t modellierte Studierende hat. Dann sind e und g Relationen auf D.

(c) Die Stichwörter in einem Lexikon seien als Elemente einer Menge L modelliert. Für $v, w \in L$ gelte genau dann $v\ a\ w$, wenn das durch v modellierte Stichwort den gleichen Anfangsbuchstaben wie das durch w modellierte Stichwort hat. Für $v, w \in L$ gelte genau dann $v\ o\ w$, wenn das durch v modellierte Stichwort einen Anfangsbuchstaben hat, welcher im Alphabet vorm Anfangsbuchstaben des durch w modellierten Stichwort vorkommt. Dann sind a und o Relationen auf L.

(d) Farbige Glasperlen in einer Dose seien als Elemente einer Menge P modelliert. Für $p, q \in P$ gelte genau dann $p\ f\ q$, wenn die durch p modellierte Glasperle die gleiche Farbe wie die durch q modellierte Glasperle hat. Dann ist f eine Relation auf P.

Eigenschaften

Wir betrachten einige potentielle Eigenschaften von Relationen.

(4.4) Definition (Transitivität, Reflexivität, Symmetrie, Antisymmetrie, Vollständigkeit)**.** Es seien eine Menge X und eine Relation r auf X gegeben.

(a) Wir sagen, dass r *transitiv* ist, falls für $x, y, z \in X$ aus $x\ r\ y$ und $y\ r\ z$ stets $x\ r\ z$ folgt.

(b) Wir sagen, dass r *reflexiv* (auf X) ist, falls für $x \in X$ stets $x\ r\ x$ gilt.

(c) Wir sagen, dass r *symmetrisch* ist, falls für $x, y \in X$ aus $x\ r\ y$ stets $y\ r\ x$ folgt.

(d) Wir sagen, dass r *antisymmetrisch* ist, falls für $x, y \in X$ aus $x\ r\ y$ und $y\ r\ x$ stets $x = y$ folgt.

(e) Wir sagen, dass r *vollständig* (auf X) ist, falls für $x, y \in X$ stets $x\ r\ y$ oder $y\ r\ x$ gilt.

(4.5) Beispiel. Die Relation $<$ auf $\mathbb{N}$ ist transitiv und antisymmetrisch, aber nicht reflexiv, nicht symmetrisch und nicht vollständig.

Beweis. Es seien $m, n, p \in \mathbb{N}$ mit $m < n$ und $n < p$ gegeben. Dann gibt es $q, r \in \mathbb{N}$ mit $n = q + m$ und $p = r + n$. Es folgt $p = r + n = r + q + m$, also $m < p$. Folglich ist $<$ transitiv.
Für keine $m, n \in \mathbb{N}$ gilt $m < n$ und $n < m$. Folglich ist $<$ antisymmetrisch.
Für kein $m \in \mathbb{N}$ gibt es ein $p \in \mathbb{N}$ mit $m = p + m$, d.h. es gilt $m < m$ für kein $m \in \mathbb{N}$. Insbesondere ist $<$ nicht reflexiv und nicht vollständig.
Es seien $m, n \in \mathbb{N}$ mit $m < n$ gegeben. Dann gibt es ein $p \in \mathbb{N}$ mit $n = p + m$. Gäbe es ein $q \in \mathbb{N}$ mit $m = q + n$, so wäre $m = q + n = q + p + m$ und damit $q + p = 0$. Da mit $p, q \in \mathbb{N}$ dann aber auch $0 = q + p \in \mathbb{N}$ sein müsste, ist dies ein Widerspruch. Folglich gilt $n < m$ nicht. Insbesondere ist $<$ nicht symmetrisch. □

Vorsicht sind bei den Begriffen der Reflexivität und der Vollständigkeit geboten, da diese von der unterliegende Menge abhängig sind.

Beispiel.

(a) Die Relation $\{(1, 1)\}$ auf $\{1\}$ ist reflexiv.

(b) Die Relation $\{(1, 1)\}$ auf $\{1, 2\}$ ist nicht reflexiv.

Beweis. Es sei $r := \{(1, 1)\}$.

(a) Wegen $1\ r\ 1$ gilt $x\ r\ x$ für alle $x \in \{1\}$. Folglich ist r reflexiv.

(b) Da $2\ r\ 2$ nicht gilt, gibt es ein $x \in \{1, 2\}$ so, dass $x\ r\ x$ nicht gilt. Folglich ist r nicht reflexiv. □

Indikatormatrix

Es sei $n \in \mathbb{N}_0$ gegeben. Eine Relation r auf $[1,n]$ ist eine Teilmenge von $[1,n] \times [1,n]$. Die Indikatormatrix, vgl. Definition (3.34), liefert eine Verbildlichung einer solchen Relation.
Durch Wahl einer Abzählung, vgl. Definition (3.39)(b), lässt sich das Konzept auf Relationen auf beliebigen endlichen Mengen verallgemeinern:

(4.6) Definition (Indikatormatrix)**.** Es seien $n \in \mathbb{N}_0$, eine Menge X, eine Abzählung $e\colon [1,n] \to X$ und eine Relation r auf X gegeben. Die $(n \times n)$-Matrix $\chi_{r,e}$ in $\{0,1\}$ gegeben durch

$$\chi_{r,e} = ((\chi_r)_{e(i),e(j)})_{i,j\in[1,n]}$$

wird *Indikatormatrix* von r bzgl. e genannt.

(4.7) Beispiel.

(a) Es sei eine Relation r auf $\{1,2,3\}$ gegeben durch

$$r = \{(1,1),(2,2),(3,3),(2,1),(3,1),(3,2)\}.$$

Die Indikatormatrix von r ist gegeben durch

$$\chi_r = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

(b) Es sei eine Relation r auf $\{-1,0,1\}$ gegeben durch

$$r = \{(-1,-1),(1,1),(-1,1),(1,-1)\}.$$

Die Indikatormatrix von r bzgl. der Abzählung $e\colon [1,3] \to \{-1,0,1\}$, $1 \mapsto -1$, $2 \mapsto 0$, $3 \mapsto 1$ ist gegeben durch

$$\chi_{r,e} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Etwas informeller lässt sich die Indikatormatrix in Beispiel (4.7)(b) durch Beschriftung mit den abgezählten Elementen in einer *Indikatortafel* darstellen:

r	-1	0	1
-1	1	0	1
0	0	0	0
1	1	0	1

Sebastian Thomas

RWTH Aachen, WS 2016/17
10.11.2016

Diskrete Strukturen
Vorlesung 7

5 Äquivalenzrelationen und Quotientenmengen

Ziel dieses Abschnitts ist es, den Begriff der (absoluten) Gleichheit von Objekten abzuschwächen und zu formalisieren, was wir unter einer „Gleichheit unter einem gewissen Gesichtspunkt“ verstehen. Hierzu dient der Begriff der Äquivalenzrelation. Fassen wir die bzgl. einer Äquivalenzrelation in Relation stehende Objekte auf geeignete Art und Weise zusammen, so erhalten wir eine neue Menge, die sogenannte Quotientenmenge, wo dann tatsächliche Gleichheit herrscht.

Äquivalenzrelationen

Eine Äquivalenzrelation ist eine Relation, siehe Definition (4.1), welche drei der in Definition (4.4) eingeführten Eigenschaften erfüllt:

(5.1) Definition (Äquivalenzrelation)**.** Es sei eine Menge X gegeben. Eine *Äquivalenzrelation* auf X ist eine Relation auf X, welche transitiv, reflexiv und symmetrisch ist.

(5.2) Beispiel.

(a) Für $x, y \in \mathbb{R}$ gelte genau dann $x \; c \; y$, wenn $x = y$ oder $x = -y$ ist. Dann ist c eine Äquivalenzrelation auf $\mathbb{R}$.

(b) Für $x, y \in \mathbb{Z}$ gelte genau dann $x \equiv_2 y$, wenn x und y entweder beide gerade oder beide ungerade sind. Dann ist $\equiv_2$ eine Äquivalenzrelation auf $\mathbb{Z}$.

(c) Die Relation $\{(1,1),(2,2),(3,3),(4,4),(1,2),(2,1),(1,4),(4,1),(2,4),(4,2)\}$ auf $\{1,2,3,4\}$ ist eine Äquivalenzrelation.

(d) Für jede Menge X ist die Gleichheitsrelation $=$ auf X eine Äquivalenzrelation auf X.

Beweis.

(a) Es seien $x, y, z \in \mathbb{R}$ mit $x \; c \; y$ und $y \; c \; z$ gegeben. Dann gilt $x = y$ oder $x = -y$, sowie $y = z$ oder $y = -z$. Wir erhalten

$$x = \begin{cases} y, & \text{falls } x = y, \\ -y, & \text{falls } x = -y \end{cases} \Bigg\} = \begin{cases} z, & \text{falls } x = y,\ y = z, \\ -z, & \text{falls } x = y,\ y = -z, \\ -z, & \text{falls } x = -y,\ y = z, \\ -(-z), & \text{falls } x = -y,\ y = -z \end{cases} \Bigg\}$$

$$= \begin{cases} z, & \text{falls } x = y,\ y = z \text{ oder } x = -y,\ y = -z, \\ -z, & \text{falls } x = y,\ y = -z \text{ oder } x = -y,\ y = z. \end{cases}$$

Also ist $x = z$ oder $x = -z$, und damit $x \; c \; z$. Folglich ist c transitiv.

Da für alle $x \in \mathbb{R}$ wegen $x = x$ auch $x \; c \; x$ gilt, ist c reflexiv.

Es seien $x, y \in \mathbb{R}$ mit $x \; c \; y$ gegeben. Dann gilt $x = y$ oder $x = -y$, also auch $y = x$ oder $y = -x$ und damit $y \; c \; x$. Folglich ist c symmetrisch.

Insgesamt ist c eine Äquivalenzrelation auf $\mathbb{R}$.

(b) Es seien $x, y, z \in \mathbb{Z}$ mit $x \equiv_2 y$ und $y \equiv_2 z$ gegeben. Wenn x gerade ist, dann ist wegen $x \equiv_2 y$ auch y gerade und wegen $y \equiv_2 z$ dann auch z gerade. Wenn x ungerade ist, dann ist wegen $x \equiv_2 y$ auch y ungerade und wegen $y \equiv_2 z$ dann auch z ungerade. Also sind x und z entweder beide gerade oder beide ungerade, d.h. es gilt $x \equiv_2 z$. Folglich ist $\equiv_2$ transitiv.

Da x entweder gerade oder ungerade ist, ist $\equiv_2$ reflexiv.

Die Symmetrie von $\equiv_2$ folgt aus der symmetrischen Definition von $\equiv_2$.

Insgesamt ist $\equiv_2$ eine Äquivalenzrelation auf $\mathbb{Z}$. □

(5.3) Anwendungsbeispiel.

(a) Die Studierenden des Moduls *Diskrete Strukturen* seien als Elemente einer Menge D modelliert. Für $s, t \in D$ gelte genau dann $s\ e\ t$, wenn der oder die durch s modellierte Studierende die gleichen Eltern wie der oder die durch t modellierte Studierende hat. Für $s, t \in D$ gelte genau dann $s\ g\ t$, wenn der oder die durch s modellierte Studierende den gleichen Geburtstag wie der oder die durch t modellierte Studierende hat. Dann sind e und g Äquivalenzrelationen auf D.

(b) Die Stichwörter in einem Lexikon seien als Elemente einer Menge L modelliert. Für $v, w \in L$ gelte genau dann $v\ a\ w$, wenn das durch v modellierte Stichwort den gleichen Anfangsbuchstaben wie das durch w modellierte Stichwort hat. Dann ist a eine Äquivalenzrelation auf L.

(c) Farbige Glasperlen in einer Dose seien als Elemente einer Menge P modelliert. Für $p, q \in P$ gelte genau dann $p\ f\ q$, wenn die durch p modellierte Glasperle die gleiche Farbe wie die durch q modellierte Glasperle hat. Dann ist f eine Äquivalenzrelation auf P.

Die bzgl. einer Äquivalenzrelation in Relation stehenden Elemente wollen wir nun zu Teilmengen zusammenfassen:

(5.4) Definition (Äquivalenzklasse)**.** Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Für $x \in X$ heißt $[x] = [x]_c := \{\tilde{x} \in X \mid \tilde{x}\ c\ x\}$ die *Äquivalenzklasse* von x in X bzgl. c, und es heißt x ein *Repräsentant* von $[x]_c$.

Wir greifen die Beispiele aus (5.2) noch einmal auf:

(5.5) Beispiel.

(a) Für $x, y \in \mathbb{R}$ gelte genau dann $x\ c\ y$, wenn $x = y$ oder $x = -y$ ist. Dann ist $[x]_c = \{x, -x\}$ für $x \in \mathbb{R}$.

(b) Für $x, y \in \mathbb{Z}$ gelte genau dann $x \equiv_2 y$, wenn x und y entweder beide gerade oder beide ungerade sind. Dann ist $[0]_{\equiv_2} = 2\mathbb{Z} = \{2q \mid q \in \mathbb{Z}\}$ und $[1]_{\equiv_2} = 2\mathbb{Z} + 1 = \{2q + 1 \mid q \in \mathbb{Z}\}$.

(c) Es sei $c := \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,1), (1,4), (4,1), (2,4), (4,2)\}$. Dann ist $[1]_c = [2]_c = [4]_c = \{1, 2, 4\}$ und $[3]_c = \{3\}$.

(d) Es sei eine Menge X gegeben. Dann ist $[x]_= = \{x\}$ für alle $x \in X$.

(5.6) Proposition. Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben.

(a) Für $x \in X$ ist $x \in [x]_c$.

(b) Für $x, y \in X$ sind die folgenden Bedingungen äquivalent:

(i) Es ist $[x]_c = [y]_c$.

(ii) Es ist $[x]_c \subseteq [y]_c$.

(iii) Es gilt $x\ c\ y$.

Beweis.

(a) Da c reflexiv ist, haben wir $x\ c\ x$ und damit $x \in [x]$ für alle $x \in X$.

(b) Es seien $x, y \in X$ gegeben.

Wenn $[x] \subseteq [y]$ gilt, dann haben wir $x \in [x] \subseteq [y]$ nach (a) und somit $x \; c \; y$. Es sei also umgekehrt angenommen, dass $x \; c \; y$ gilt. Für alle $\tilde{x} \in [x]$ haben wir $\tilde{x} \; c \; x$, die Transitivität von c liefert also $\tilde{x} \; c \; y$, d.h. $\tilde{x} \in [y]$. Folglich ist $[x] \subseteq [y]$.

Somit gilt genau dann $[x] \subseteq [y]$, wenn $x \; c \; y$ ist; wir haben also die Äquivalenz von Bedingung (ii) und Bedingung (iii) gezeigt. Nun ist aber c symmetrisch, d.h. aus $x \; c \; y$ folgt $y \; c \; x$. Folglich impliziert $[x] \subseteq [y]$ bereits $[y] \subseteq [x]$ und damit $[x] = [y]$. Da $[x] = [y]$ aber stets $[x] \subseteq [y]$ impliziert, sind auch Bedingung (i) und Bedingung (ii) äquivalent.

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

Quotientenmengen

Als nächstes wollen wir die Äquivalenzklassen bzgl. einer Äquivalenzrelation wieder zu einer Menge zusammenfassen:

(5.7) Definition (Quotientenmenge)**.** Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Die Menge

$$X/c := \{[x]_c \mid x \in X\}$$

heißt *Quotientenmenge* (oder *Quotient*) von X modulo c. Die Abbildung

$$\mathrm{quo} = \mathrm{quo}^{X/c} \colon X \to X/c,\ x \mapsto [x]_c$$

wird *Quotientenabbildung* von X/c genannt.

Wir bestimmen die Quotientenmenge im Fall von Beispiel (5.2)(c):

(5.8) Beispiel. Es sei $c := \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,1), (1,4), (4,1), (2,4), (4,2)\}$. Dann ist

$$\{1,2,3,4\}/c = \{[1]_c, [3]_c\}.$$

Beweis. Nach Beispiel (5.5)(c) ist $[1] = [2] = [4]$ und damit

$$\{1,2,3,4\}/c = \{[1], [2], [3], [4]\} = \{[1], [3]\}.$$ □

Unter der Quotientenmenge einer Menge X bzgl. einer Äquivalenzrelation c auf X stellen wir uns eine „Vergröberung“ der Menge X vor. Diejenigen Elemente in X, welche in X nur äquivalent bzgl. c sind, werden über die Quotientenabbildung zu gleichen Elementen in der Quotientenmenge.

(5.9) Definition (Transversale)**.** Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Eine *Transversale* (oder ein *Repräsentantensystem*) von X bzgl. c ist eine Teilmenge T von X so, dass es für jedes $K \in X/c$ genau ein $t \in T$ mit $K = [t]_c$ gibt.

Wir bestimmen einige Transversalen für die Äquivalenzrelationen aus Beispiel (5.2):

(5.10) Beispiel.

(a) Für $x, y \in \mathbb{R}$ gelte genau dann $x \; c \; y$, wenn $x = y$ oder $x = -y$ ist. Dann sind $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} \mid x \geq 0\}$, $\mathbb{R}_{\leq 0} = \{x \in \mathbb{R} \mid x \leq 0\}$ und $\{x \in \mathbb{R} \mid x < -2 \text{ oder } 0 \leq x \leq 2\}$ Transversalen von $\mathbb{R}$ bzgl. c.

(b) Für $x, y \in \mathbb{Z}$ gelte genau dann $x \equiv_2 y$, wenn x und y entweder beide gerade oder beide ungerade sind. Dann sind $\{0,1\}$, $\{1,2\}$, $\{-3, 88\}$ Transversalen von $\mathbb{Z}$ bzgl. $\equiv_2$.

(c) Es sei $c := \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,1), (1,4), (4,1), (2,4), (4,2)\}$. Dann sind $\{1,3\}$, $\{2,3\}$, $\{3,4\}$ Transversalen von $\{1,2,3,4\}$ bzgl. c.

(d) Es sei eine Menge X gegeben. Dann ist X die einzige Transversale von X bzgl. $=$.

Der Homomorphiesatz für Mengen

Wir werden nun sehen, dass jede Abbildung Anlass zu einer Äquivalenzrelation gibt, welche schließlich zu einer Bijektion führt.

(5.11) Definition (Bildgleichheit)**.** Es sei eine Abbildung $f\colon X \to Y$ gegeben. Für $x, \tilde{x} \in X$ gelte genau dann $x =_f \tilde{x}$, wenn $f(x) = f(\tilde{x})$ ist. Die Relation $=_f$ auf X heißt *Bildgleichheit* bzgl. f.

(5.12) Beispiel. Es sei $f\colon \{1,2,3,4\} \to \mathbb{Z}$, $1 \mapsto 1$, $2 \mapsto 1$, $3 \mapsto 3$, $4 \mapsto 1$. Dann ist

$$=_f = \{(1,1),(2,2),(3,3),(4,4),(1,2),(2,1),(1,4),(4,1),(2,4),(4,2)\}$$

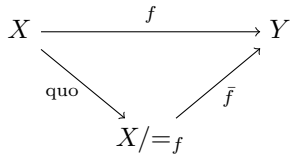
(5.13) Bemerkung. Für jede Abbildung $f\colon X \to Y$ ist $=_f$ eine Äquivalenzrelation auf X.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(5.14) Satz (Homomorphiesatz für Mengen)**.** Es sei eine Abbildung $f\colon X \to Y$ gegeben. Dann haben wir eine induzierte Abbildung $\bar{f}\colon X/{=_f} \to Y$, $[x] \mapsto f(x)$, welche $f = \bar{f} \circ \mathrm{quo}$ erfüllt. Es ist $\bar{f}$ injektiv und $\operatorname{Im} \bar{f} = \operatorname{Im} f$. Insbesondere ist

$$\bar{f}|^{\operatorname{Im} f}\colon X/{=_f} \to \operatorname{Im} f$$

eine Bijektion.



Beweis. Für $x, x' \in X$ ist nach Proposition (5.6)(b) genau dann $[x] = [x']$ in $X/{=_f}$, wenn $x =_f x'$ in X gilt, und dies ist nach Definition von $=_f$ äquivalent zu $f(x) = f(x')$ in Y. Folglich ist $\bar{f}\colon X/{=_f} \to Y$, $[x] \mapsto f(x)$ eine wohldefinierte Abbildung. Da für $x \in X$ stets

$$\bar{f}(\mathrm{quo}(x)) = \bar{f}([x]) = f(x)$$

ist, gilt $f = \bar{f} \circ \mathrm{quo}$. Ferner ist

$$\operatorname{Im} \bar{f} = \{\bar{f}(K) \mid K \in X/c\} = \{\bar{f}([x]) \mid x \in X\} = \{f(x) \mid x \in X\} = \operatorname{Im} f.$$

Für $x, x' \in X$ mit $\bar{f}([x]) = \bar{f}([x'])$ in Y gilt schließlich

$$f(x) = \bar{f}([x]) = \bar{f}([x']) = f(x')$$

in Y, also $x =_f x'$ in X und damit $[x] = [x']$ in $X/{=_f}$ nach Proposition (5.6)(b). Also ist $\bar{f}$ in der Tat injektiv. □

(5.15) Beispiel. Es sei $f\colon \{1,2,3,4\} \to \mathbb{Z}$, $1 \mapsto 1$, $2 \mapsto 1$, $3 \mapsto 3$, $4 \mapsto 1$. Dann ist $\{1,2,3,4\}/{=_f} = \{[1],[3]\}$ und es gilt $f = \bar{f} \circ \mathrm{quo}$ mit $\bar{f}\colon \{1,2,3,4\}/{=_f} \to \mathbb{Z}$, $[1] \mapsto 1$, $[3] \mapsto 3$.

Wir erläutern den Homomorphiesatz für Mengen (5.14) auch noch an einem Beispiel aus dem täglichen Leben:

(5.16) Anwendungsbeispiel. Farbige Glasperlen in einer Dose seien als Elemente einer Menge P modelliert. Farben seien als Elemente einer Menge F modelliert. Die Zuordnung der zugehörigen Farbe zu jeder Glasperle sei als Abbildung $a\colon P \to F$ modelliert. Für $p, q \in P$ gilt genau dann $p =_a q$, wenn die durch p modellierte Glasperle die gleiche Farbe wie die durch q modellierte Glasperle hat. Eine Äquivalenzklasse bzgl. $=_a$ entspricht der Gesamtheit aller Glasperlen einer Farbe. Die Quotientenmenge $P/{=_a}$ entspricht einer „Sortierung“ aller Glasperlen nach Farben; die Quotientenabbildung $\mathrm{quo}\colon P \to P/{=_a}$ entspricht der Zuordnung jeder Perle zu ihrem „Farbhäufchen“; und die induzierte Abbildung $\bar{a}\colon P/{=_a} \to F$ entspricht der Zuordnung jedes Häufchens zu „seiner“ Farbe.

Partitionen

Zum Abschluss wollen wir den mengentheoretischen Aspekt von Quotientenmengen noch etwas genauer beleuchten: Jede Äquivalenzrelation c auf einer Menge X partitioniert (also unterteilt) via X/c die Menge X in Teilmengen, nämlich in die Elemente von X/c. Gehen wir umgekehrt von einer Unterteilung von X in Teilmengen aus, so liefert uns dies wiederum eine Äquivalenzrelation, indem wir zwei Elemente als äquivalent betrachten, wenn sie im gleichen Teil der Unterteilung liegen. Es lässt sich zeigen, dass sich diese Konstruktionen gegenseitig umkehren, siehe den Hauptsatz über Äquivalenzrelationen (5.19).
Zunächst präzisieren wir, was wir unter einer Unterteilung einer Menge verstehen wollen:

(5.17) Definition (Partition)**.** Es sei eine Menge X gegeben. Eine *Partition* (genauer *Mengenpartition*) von X ist eine Teilmenge $\mathcal{P}$ von $\mathrm{Pot}(X)$ so, dass $\emptyset \notin \mathcal{P}$ und

$$X = \dot{\bigcup_{P \in \mathcal{P}}} P.$$

Für $x \in X$ heißt das eindeutige $P \in \mathcal{P}$ mit $x \in P$ der *Teil* von x in $\mathcal{P}$.

(5.18) Beispiel. Es ist $\{\{1,2,4\},\{3\}\}$ eine Partition von $\{1,2,3,4\}$.

(5.19) Satz (Hauptsatz über Äquivalenzrelationen)**.** Es sei eine Menge X gegeben. Wir haben eine wohldefinierte Bijektion

$$X/{-}\colon \{c \mid c \text{ ist Äquivalenzrelation auf } X\} \to \{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } X\},\ c \mapsto X/c.$$

Für jede Partition $\mathcal{P}$ von X ist die eindeutige Äquivalenzrelation c auf X mit $\mathcal{P} = X/c$ wie folgt gegeben: Für $x, y \in X$ gilt genau dann $x\ c\ y$, wenn es ein $P \in \mathcal{P}$ mit $x \in P$ und $y \in P$ gibt.

Beweis. Zunächst sei eine Äquivalenzrelation c gegeben. Dann ist $X/c = \{[x]_c \mid x \in X\}$. Für alle $K \in X/c$ gibt es also ein $x \in X$ mit $K = [x]_c$, und mit Proposition (5.6)(a) folgt $x \in [x]_c = K$. Insbesondere ist $K \neq \emptyset$ für alle $K \in X/c$ und damit $\emptyset \notin X/c$. Für $x \in X$ gilt ferner

$$x \in [x]_c \subseteq \bigcup_{y \in X} [y]_c = \bigcup_{K \in X/c} K,$$

es ist also $X = \bigcup_{K \in X/c} K$. Um die Disjunktheit von $(K)_{K \in X/c}$ zu zeigen, seien $K, L \in X/c$ mit $K \cap L \neq \emptyset$ gegeben. Ferner seien $x, y, z \in X$ mit $K = [x]_c$, $L = [y]_c$ und $z \in K \cap L$ gegeben. Wegen $z \in K = [x]_c$ gilt $z\ c\ x$ und wegen $z \in L = [y]_c$ gilt $z\ c\ y$. Wir erhalten also $x\ c\ y$ und somit $K = [x]_c = [y]_c = L$ nach Proposition (5.6)(b). Insgesamt ist X/c eine Partition von X.
Somit haben wir eine wohldefinierte Abbildung

$$X/{-}\colon \{c \mid c \text{ ist Äquivalenzrelation auf } X\} \to \{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } X\},\ c \mapsto X/c.$$

Umgekehrt sei eine Partition $\mathcal{P}$ von X gegeben. Da $(P)_{P \in \mathcal{P}}$ disjunkt ist, gibt es für jedes $x \in X$ genau ein $P \in \mathcal{P}$ mit $x \in P$. Somit haben wir eine Abbildung $q_{\mathcal{P}}\colon X \to \mathcal{P}$ mit $x \in q_{\mathcal{P}}(x)$. Die Bildgleichheit $=_{q_{\mathcal{P}}}$ ist nach Bemerkung (5.13) eine Äquivalenzrelation auf X.
Folglich haben wir auch eine wohldefinierte Abbildung

$$=_{q_-}\colon \{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } X\} \to \{c \mid c \text{ ist Äquivalenzrelation auf } X\},\ \mathcal{P} \mapsto =_{q_{\mathcal{P}}}.$$

Wir wollen zeigen, dass sich die Abbildungen $X/{-}$ und $=_{q_-}$ gegenseitig invertieren. Für jede Äquivalenzrelation c auf X gilt

$$\begin{aligned} =_{q_{X/c}} &= \{(x,y) \in X \times X \mid q_{X/c}(x) = q_{X/c}(y)\} = \{(x,y) \in X \times X \mid [x]_c = [y]_c\} \\ &= \{(x,y) \in X \times X \mid x\ c\ y\} = c \end{aligned}$$

nach Proposition (5.6)(b). Folglich ist $=_{q_-} \circ X/{-} = \mathrm{id}_{\{c \mid c \text{ ist Äquivalenzrelation auf } X\}}$ nach dem Gleichheitskriterium für Abbildungen (3.6). Umgekehrt sei eine Partition $\mathcal{P}$ von X gegeben. Für $x, y \in X$ gilt genau dann $y =_{q_{\mathcal{P}}} x$, wenn $q_{\mathcal{P}}(y) = q_{\mathcal{P}}(x)$ ist, und da $(P)_{P \in \mathcal{P}}$ disjunkt ist, ist dies äquivalent zu $y \in q_{\mathcal{P}}(x)$. Folglich ist

$$[x]_{=_{q_{\mathcal{P}}}} = \{y \in X \mid y =_{q_{\mathcal{P}}} x\} = q_{\mathcal{P}}(x)$$

für $x \in X$, also

$$X/{=_{q_\mathcal{P}}} = \{[x]_{=_{q_\mathcal{P}}} \mid x \in X\} = \{q_\mathcal{P}(x) \mid x \in X\} = \mathcal{P}.$$

Nach dem Gleichheitskriterium für Abbildungen (3.6) ist somit auch $X/- \circ =_{q_-} = \mathrm{id}_{\{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } X\}}$. Insgesamt sind $X/-$ und $=_{q_-}$ zueinander inverse Abbildungen. □

Sebastian Thomas

RWTH Aachen, WS 2016/17
16.11.2016

Diskrete Strukturen
Vorlesung 8

6 Algebraische Strukturen

Bisher haben wir Mengen und Abbildungen zwischen Mengen betrachtet. Die aus der Schule bekannten Mengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ haben jedoch neben der Zusammenfassung ihrer Elemente noch mehr Struktur – wir können etwa Elemente addieren und multiplizieren. Dieser Aspekt soll in diesem Abschnitt formalisiert werden. Wir beleuchten die algebraische Struktur dieser Zahlbereiche und gelangen dadurch zu Begriffen wie Gruppe und Ring, von denen wir im weiteren Verlauf auch neue Beispiele kennenlernen werden.

Verknüpfungen

Unser intuitives Verständnis der Zahlbereiche lässt an der Gültigkeit des folgenden Satzes keinen Zweifel:

(6.1) Satz.

(a) (i) Für $m, n, p \in \mathbb{N}$ gilt $m + (n + p) = (m + n) + p$.
(ii) Für $m, n \in \mathbb{N}$ gilt $m + n = n + m$.
(iii) Für $m, n, p \in \mathbb{N}$ gilt $m(np) = (mn)p$.
(iv) Für $m \in \mathbb{N}$ gilt $1m = m1 = m$.
(v) Für $m, n \in \mathbb{N}$ gilt $mn = nm$.

(b) (i) Für $m, n, p \in \mathbb{N}_0$ gilt $m + (n + p) = (m + n) + p$.
(ii) Für $m \in \mathbb{N}_0$ gilt $0 + m = m + 0 = m$.
(iii) Für $m, n \in \mathbb{N}_0$ gilt $m + n = n + m$.
(iv) Für $m, n, p \in \mathbb{N}_0$ gilt $m(np) = (mn)p$.
(v) Für $m \in \mathbb{N}_0$ gilt $1m = m1 = m$.
(vi) Für $m, n \in \mathbb{N}_0$ gilt $mn = nm$.

(c) (i) Für $x, y, z \in \mathbb{Z}$ gilt $x + (y + z) = (x + y) + z$.
(ii) Für $x \in \mathbb{Z}$ gilt $0 + x = x + 0 = x$.
(iii) Für $x \in \mathbb{Z}$ gilt $(-x) + x = x + (-x) = 0$.
(iv) Für $x, y \in \mathbb{Z}$ gilt $x + y = y + x$.
(v) Für $x, y, z \in \mathbb{Z}$ gilt $x(yz) = (xy)z$.
(vi) Für $x \in \mathbb{Z}$ gilt $1x = x1 = x$.
(vii) Für $x, y \in \mathbb{Z}$ gilt $xy = yx$.
(viii) Für $x, y, z \in \mathbb{Z}$ gilt $x(y + z) = xy + xz$ und $(x + y)z = xz + yz$.

(d) (i) Für $x, y, z \in \mathbb{Q}$ gilt $x + (y + z) = (x + y) + z$.
(ii) Für $x \in \mathbb{Q}$ gilt $0 + x = x + 0 = x$.
(iii) Für $x \in \mathbb{Q}$ gilt $(-x) + x = x + (-x) = 0$.
(iv) Für $x, y \in \mathbb{Q}$ gilt $x + y = y + x$.
(v) Für $x, y, z \in \mathbb{Q}$ gilt $x(yz) = (xy)z$.
(vi) Für $x \in \mathbb{Q}$ gilt $1x = x1 = x$.

(vii) Für $x \in \mathbb{Q} \setminus \{0\}$ gilt $x^{-1}x = xx^{-1} = 1$.

(viii) Für $x, y \in \mathbb{Q}$ gilt $xy = yx$.

(ix) Für $x, y, z \in \mathbb{Q}$ gilt $x(y + z) = xy + xz$ und $(x + y)z = xz + yz$.

Die Rechenregeln aus Satz (6.1) geben die grundsätzlichen Eigenschaften der Addition und der Multiplikation von rationalen Zahlen und gewissen Teilmengen wieder. Im Folgenden wollen wir diese Eigenschaften genauer analysieren, formalisieren und so zu neuen Begrifflichkeiten auf einer abstrakten Ebene gelangen, welche sich dann wiederum bei weiteren Beispielen in ganz anderen Bereichen verwenden lassen.
Zunächst müssen wir uns darüber im Klaren werden, was eine Addition bzw. eine Multiplikation eigentlich ist. Bei der Addition natürlicher Zahlen m und n ordnen wir diesen ihre Summe $m + n$ zu. In Abschnitt 3 haben wir gesehen, dass sich solche Zuordnungen mit Hilfe von Abbildungen formalisieren lassen. Da jeder Ausdruck der Form $m + n$ aus den beiden Summanden m und n entsteht, ordnen wir bei der Addition einem Paar (m, n) in $\mathbb{N}$, also einem Element in $\mathbb{N} \times \mathbb{N}$, das Element $m + n$ in $\mathbb{N}$ zu. Bei der Addition handelt es sich also um eine Abbildung

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N},\ (m, n) \mapsto m + n.$$

Wir werden nun Abbildungen von dieser Form systematisch studieren und ihnen deswegen eine eigene Bezeichnung verleihen.

(6.2) Definition (Verknüpfung)**.** Es sei eine Menge X gegeben. Eine *Verknüpfung* (oder *binäre algebraische Operation*) auf X ist eine Abbildung $m\colon X \times X \to X$. Für $(x, y) \in X \times X$ schreiben wir $x\, m\, y := m(x, y)$.

Da zu einer gegebenen Menge X die Start- und die Zielmenge einer Verknüpfung auf X eindeutig festgelegt sind ($X \times X$ bzw. X), lassen wir diese Angaben im Folgenden meist weg.

(6.3) Beispiel.

(a) Auf $\mathbb{N}$ haben wir die Verknüpfungen $(m, n) \mapsto m + n$ und $(m, n) \mapsto m \cdot n$.

(b) Auf $\mathbb{N}_0$ haben wir die Verknüpfungen $(m, n) \mapsto m + n$ und $(m, n) \mapsto m \cdot n$.

(c) Auf $\mathbb{Z}$ haben wir die Verknüpfungen $(x, y) \mapsto x + y$ und $(x, y) \mapsto x - y$ und $(x, y) \mapsto x \cdot y$.

(d) Auf $\mathbb{Q}$ haben wir die Verknüpfungen $(x, y) \mapsto x + y$ und $(x, y) \mapsto x - y$ und $(x, y) \mapsto x \cdot y$.

Verknüpfungen auf endlichen Mengen lassen sich durch *Verknüpfungstafeln* verbildlichen:

(6.4) Beispiel.

(a) Es seien verschiedene Objekte a, b, c gegeben. Auf $\{a, b, c\}$ haben wir eine Verknüpfung m, welche durch folgende Verknüpfungstafel gegeben ist:

m	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

(b) Es seien verschiedene Objekte a, b, c, d, e gegeben. Auf $\{a, b, c, d, e\}$ haben wir eine Verknüpfung m, welche durch folgende Verknüpfungstafel gegeben ist:

m	a	b	c	d	e
a	b	c	d	e	a
b	d	e	a	c	b
c	e	d	b	a	c
d	c	a	e	b	d
e	a	b	c	d	e

Natürlich gibt es auf $\mathbb{N}$ und den anderen Zahlbereichen noch viel mehr Verknüpfungen, doch diese beiden zeichnen sich durch besondere Eigenschaften aus, wie wir in Satz (6.1) gesehen haben. Wir wollen diese Eigenschaften nun für allgemeine Verknüpfungen studieren.

(6.5) Definition (Assoziativität, Kommutativität)**.** Es seien eine Menge X und eine Verknüpfung m auf X gegeben.

(a) Wir sagen, dass m *assoziativ* ist, wenn für $x, y, z \in X$ stets

$$x\, m\, (y\, m\, z) = (x\, m\, y)\, m\, z$$

gilt.

(b) Wir sagen, dass m *kommutativ* ist, wenn für $x, y \in X$ stets

$$x\, m\, y = y\, m\, x$$

gilt.

Die Aussagen aus Satz (6.1)(a)(i), (ii), (iii), (v) lassen sich nun auch kurz wie folgt formulieren:

(6.6) Beispiel. Die Verknüpfungen $(m, n) \mapsto m + n$ und $(m, n) \mapsto m \cdot n$ auf $\mathbb{N}$ sind assoziativ und kommutativ.

(6.7) Beispiel.

(a) Es seien verschiedene Objekte a, b, c gegeben und auf $\{a, b, c\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Dann ist m assoziativ und kommutativ.

(b) Es seien verschiedene Objekte a, b, c, d, e gegeben und auf $\{a, b, c, d, e\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c	d	e
a	b	c	d	e	a
b	d	e	a	c	b
c	e	d	b	a	c
d	c	a	e	b	d
e	a	b	c	d	e

Dann ist m nicht assoziativ und nicht kommutativ.

Beweis.

(a) Wegen

$$\begin{aligned}
&a\, m\, (a\, m\, a) = a\, m\, a = a = a\, m\, a = (a\, m\, a)\, m\, a,\\
&a\, m\, (a\, m\, b) = a\, m\, b = b = a\, m\, b = (a\, m\, a)\, m\, b,\\
&a\, m\, (a\, m\, c) = a\, m\, c = c = a\, m\, c = (a\, m\, a)\, m\, c,\\
&a\, m\, (b\, m\, a) = a\, m\, b = b = b\, m\, a = (a\, m\, b)\, m\, a,\\
&a\, m\, (b\, m\, b) = a\, m\, c = c = b\, m\, b = (a\, m\, b)\, m\, b,\\
&a\, m\, (b\, m\, c) = a\, m\, a = a = b\, m\, c = (a\, m\, b)\, m\, c,\\
&a\, m\, (c\, m\, a) = a\, m\, c = c = c\, m\, a = (a\, m\, c)\, m\, a,\\
&a\, m\, (c\, m\, b) = a\, m\, a = a = c\, m\, b = (a\, m\, c)\, m\, b,\\
&a\, m\, (c\, m\, c) = a\, m\, b = b = c\, m\, c = (a\, m\, c)\, m\, c,\\
&b\, m\, (a\, m\, a) = b\, m\, a = b = a\, m\, a = (b\, m\, a)\, m\, a,\\
&b\, m\, (a\, m\, b) = b\, m\, b = c = a\, m\, b = (b\, m\, a)\, m\, b,\\
&b\, m\, (a\, m\, c) = b\, m\, c = a = a\, m\, c = (b\, m\, a)\, m\, c,
\end{aligned}$$

$$b\,m\,(b\,m\,a) = b\,m\,b = c = b\,m\,a = (b\,m\,b)\,m\,a,$$
$$b\,m\,(b\,m\,b) = b\,m\,c = a = b\,m\,b = (b\,m\,b)\,m\,b,$$
$$b\,m\,(b\,m\,c) = b\,m\,a = b = b\,m\,c = (b\,m\,b)\,m\,c,$$
$$b\,m\,(c\,m\,a) = b\,m\,c = a = c\,m\,a = (b\,m\,c)\,m\,a,$$
$$b\,m\,(c\,m\,b) = b\,m\,a = b = c\,m\,b = (b\,m\,c)\,m\,b,$$
$$b\,m\,(c\,m\,c) = b\,m\,b = c = c\,m\,c = (b\,m\,c)\,m\,c,$$
$$c\,m\,(a\,m\,a) = c\,m\,a = c = c\,m\,a = (c\,m\,a)\,m\,a,$$
$$c\,m\,(a\,m\,b) = c\,m\,b = a = c\,m\,b = (c\,m\,a)\,m\,b,$$
$$c\,m\,(a\,m\,c) = c\,m\,c = b = c\,m\,c = (c\,m\,a)\,m\,c,$$
$$c\,m\,(b\,m\,a) = c\,m\,b = a = a\,m\,a = (c\,m\,b)\,m\,a,$$
$$c\,m\,(b\,m\,b) = c\,m\,c = b = a\,m\,b = (c\,m\,b)\,m\,b,$$
$$c\,m\,(b\,m\,c) = c\,m\,a = c = a\,m\,c = (c\,m\,b)\,m\,c,$$
$$c\,m\,(c\,m\,a) = c\,m\,c = b = b\,m\,a = (c\,m\,c)\,m\,a,$$
$$c\,m\,(c\,m\,b) = c\,m\,a = c = b\,m\,b = (c\,m\,c)\,m\,b,$$
$$c\,m\,(c\,m\,c) = c\,m\,b = a = b\,m\,c = (c\,m\,c)\,m\,c$$

ist m assoziativ.

Wegen

$$a\,m\,b = b = b\,m\,a,$$
$$a\,m\,c = c = c\,m\,a,$$
$$b\,m\,c = a = c\,m\,a$$

gilt $x\,m\,y = y\,m\,x$ für alle $x, y \in \{a, b, c\}$ mit $x \neq y$. Da für $x, y \in \{a, b, c\}$ mit $x = y$ ebenfalls $x\,m\,y = x\,m\,x = y\,m\,x$ gilt, ist m somit kommutativ.

(b) Wegen

$$b\,m\,(a\,m\,a) = b\,m\,b = e \neq c = d\,m\,a = (b\,m\,a)\,m\,a$$

ist m nicht assoziativ. Wegen

$$a\,m\,b = c \neq d = b\,m\,a$$

ist m nicht kommutativ. □

In Satz (6.1)(a)(iv) haben wir gesehen, dass dem Element $1 \in \mathbb{N}$ eine besondere Stellung bzgl. der Multiplikation von natürlichen Zahlen zukommt: Multipliziert man ein Element $n \in \mathbb{N}$ mit 1, egal von welcher Seite, so erhält man als Produkt das Element n zurück. Eine ganz ähnliche Rolle hat das Element $0 \in \mathbb{N}_0$ bzgl. der Addition von $\mathbb{N}_0$, siehe Satz (6.1)(b)(ii): Addiert man 0 zu einem Element $n \in \mathbb{N}_0$, so bekommt man als Summe wieder n. Wir abstrahieren wieder:

(6.8) Definition (neutrales Element)**.** Es seien eine Menge X und eine Verknüpfung m auf X gegeben. Ein *neutrales Element* (in X) bzgl. m ist ein Element e in X, welches

$$e\,m\,x = x\,m\,e = x$$

für alle $x \in X$ erfüllt.

(6.9) Beispiel. Es ist 1 ein neutrales Element bzgl. der Verknüpfung $(m, n) \mapsto m \cdot n$ auf $\mathbb{N}$.

(6.10) Beispiel.

(a) Es seien verschiedene Objekte a, b, c gegeben und auf $\{a, b, c\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Dann ist a ein neutrales Element in $\{a, b, c\}$ bzgl. m.

(b) Es seien verschiedene Objekte a, b, c, d, e gegeben und auf $\{a, b, c, d, e\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c	d	e
a	b	c	d	e	a
b	d	e	a	c	b
c	e	d	b	a	c
d	c	a	e	b	d
e	a	b	c	d	e

Dann ist e ein neutrales Element in $\{a, b, c, d, e\}$ bzgl. m.

Beweis.

(a) Wegen $a\, m\, x = x\, m\, a = x$ für alle $x \in \{a, b, c\}$ ist a ein neutrales Element bzgl. m.

(b) Wegen $e\, m\, x = x\, m\, e = x$ für alle $x \in \{a, b, c, d, e\}$ ist e ein neutrales Element bzgl. m. □

Wir werden nun sehen, dass es bzgl. einer Verknüpfung niemals mehrere neutrale Elemente geben kann.

(6.11) Bemerkung. Es seien eine Menge X und eine Verknüpfung m auf X gegeben. Dann gibt es höchstens ein neutrales Element bzgl. m.

Beweis. Es seien neutrale Elemente e und e' in X bzgl. m gegeben. Da e neutral ist, gilt $emx = x$ für alle $x \in X$, also insbesondere $e\, m\, e' = e'$. Da e' neutral ist, gilt $x\, m\, e' = x$ für alle $x \in X$, also insbesondere $e\, m\, e' = e$. Insgesamt haben wir

$$e = e\, m\, e' = e'.$$

□

Die Addition auf $\mathbb{N}$ liefert ein Beispiel für eine Verknüpfung bzgl. derer es kein neutrales Element gibt.
Das wesentliche Merkmal, was die ganzen Zahlen von den natürlichen Zahlen unterscheidet, ist das Hinzukommen von negativen Elementen. Diese haben die Eigenschaft, dass sie zu dem entsprechenden positiven Element addiert die Zahl 0, das neutrale Element bzgl. der Addition, ergeben. Ganz ähnlich liefert die Multiplikation mit einem inversen Element in $\mathbb{Q}$ die Zahl 1, das neutrale Element bzgl. der Multiplikation.
Wir abstrahieren von der konkreten Situation:

(6.12) Definition (inverses Element)**.** Es seien eine Menge X, eine Verknüpfung m auf X, ein neutrales Element e bzgl. m und ein $x \in X$ gegeben.

(a) Ein *linksinverses Element* (in X) zu x bzgl. m ist ein Element y in X, welches $y\, m\, x = e$ erfüllt.

(b) Ein *rechtsinverses Element* (in X) zu x bzgl. m ist ein Element y in X, welches $x\, m\, y = e$ erfüllt.

(c) Ein *inverses Element* (in X) zu x bzgl. m ist ein Element y in X, welches links- und rechtsinvers zu x bzgl. m ist.

(6.13) Beispiel. Es ist $\frac{4}{3}$ ein zu $\frac{3}{4}$ inverses Element bzgl. der Verknüpfung $(m, n) \mapsto m \cdot n$ auf $\mathbb{Q}$.

(6.14) Beispiel.

(a) Es seien verschiedene Objekte a, b, c gegeben und auf $\{a, b, c\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Dann ist b ein zu c inverses Element in $\{a, b, c\}$ bzgl. m.

(b) Es seien verschiedene Objekte a, b, c, d, e gegeben und auf $\{a, b, c, d, e\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c	d	e
a	b	c	d	e	a
b	d	e	a	c	b
c	e	d	b	a	c
d	c	a	e	b	d
e	a	b	c	d	e

Dann ist b ein zu b inverses Element in $\{a, b, c, d, e\}$ bzgl. m. Ferner ist c linksinvers zu a und d rechtsinvers zu a bzgl. m.

Beweis.

(a) Nach Beispiel (6.10)(a) ist a ein neutrales Element bzgl. m. Wegen $b\,m\,c = c\,m\,b = a$ ist daher b ein zu c inverses Element bzgl. m.

(b) Nach Beispiel (6.10)(b) ist e ein neutrales Element bzgl. m. Wegen $b\,m\,b = e$ ist daher b ein zu b inverses Element bzgl. m. Wegen $c\,m\,a = e$ ist ferner c linksinvers zu a bzgl. m und wegen $a\,m\,d = e$ ist d rechtsinvers zu a bzgl. m. □

Wir haben hier zwischen linksinversen, rechtsinversen und inversen Elementen unterschieden, da es Situationen gibt, in welchen ein Element ein linksinverses Element, aber kein rechtsinverses Element hat, und umgekehrt. Ist die betrachtete Verknüpfung assoziativ, so kann es jedoch nicht passieren, dass ein Element verschiedene links- und rechtsinverse Elemente hat:

(6.15) Bemerkung. Es seien eine Menge X, eine assoziative Verknüpfung m auf X und ein neutrales Element e bzgl. m gegeben. Ferner seien $x \in X$, ein linksinverses Element y und ein rechtsinverses Element y' zu x bzgl. m gegeben. Dann gilt

$$y = y'.$$

Beweis. Da e neutral bzgl. m ist, gilt $y\,m\,e = y$ und $e\,m\,y' = y'$. Da y linksinvers zu x bzgl. m ist, gilt $y\,m\,x = e$. Da y' rechtsinvers zu x bzgl. m ist, gilt $x\,m\,y' = e$. Unter Ausnutzung der Assoziativität von m erhalten wir

$$y = y\,m\,e = y\,m\,(x\,m\,y') = (y\,m\,x)\,m\,y' = e\,m\,y' = y'.$$ □

Man vergleiche den Beweis der vorangegangenen Bemerkung (6.15) mit dem Beweis von Bemerkung (3.19).

(6.16) Korollar. Es seien eine Menge X, eine assoziative Verknüpfung m auf X, ein neutrales Element e bzgl. m und ein $x \in X$ gegeben. Dann gibt es höchstens ein inverses Element zu x bzgl. m.

Beweis. Es seien inverse Elemente y und y' zu x gegeben. Dann ist y insbesondere linksinvers und y' insbesondere rechtsinvers zu x bzgl. m, so dass aus Bemerkung (6.15) bereits $y = y'$ folgt. □

Halbgruppen und Monoide

Als nächstes wollen wir uns davon lösen, Verknüpfungen als eigenständige Objekte zu betrachten. Wir wollen den Standpunkt einnehmen, dass Verknüpfungen „fest“ zu einer Menge dazugehören, und wollen die Menge zusammen mit den Verknüpfungen als eine gemeinsame „algebraische Struktur“ ansehen.
Obwohl wir auf $\mathbb{N}$ und $\mathbb{N}_0$ mehrere uns vertraute Verknüpfungen haben, begnügen wir uns zunächst mit „einfacheren“ Strukturen und studieren Mengen, die mit genau einer Verknüpfung versehen sind und einige der gerade eingeführten Eigenschaften erfüllen. Mengen, welche mit zwei miteinander verträglichen Verknüpfungen ausgestattet sind, werden dann später eingeführt.

(6.17) Definition (Halbgruppe, kommutative Halbgruppe, Monoid)**.**

(a) Eine *Halbgruppe* besteht aus einer Menge M zusammen mit einer assoziativen Verknüpfung m auf M. Unter Missbrauch der Notation bezeichnen wir sowohl die besagte Halbgruppe als auch die unterliegende Menge mit M. Die Verknüpfung m wird *Multiplikation* (oder *Halbgruppenverknüpfung*) von M genannt.

Für eine Halbgruppe M mit Multiplikation m schreiben wir $\cdot = \cdot^M := m$ und $xy = x \cdot y$ für $x, y \in M$.

(b) Eine Halbgruppe M heißt *kommutativ*, falls die Multiplikation von M kommutativ ist.

(c) Ein *Monoid* ist eine Halbgruppe M, welche ein neutrales Element bzgl. $\cdot^M$ besitzt. Die Halbgruppenverknüpfung eines Monoids M wird auch *Monoidverknüpfung* von M genannt. Das neutrale Element bzgl. der Multiplikation wird auch *Eins* (oder *Einselement*) von M genannt und als $1 = 1^M$ notiert.

Bei der Festlegung „$\cdot = \cdot^M := m$“ in Definition (6.17)(a) für die Multiplikation einer Halbgruppe handelt es sich um eine Notation, um in einer abstrakt (d.h. nicht in einem konkreten Beispiel) gegebenen Halbgruppe einfach von der Verknüpfung sprechen zu können und diese nicht immer explizit erwähnen zu müssen. In der Regel werden wir also von einer „Halbgruppe M“ anstatt von einer „Halbgruppe M mit Multiplikation m“ sprechen, die Multiplikation als implizit gegeben ansehen und diese dann mit dem Symbol $\cdot$ bezeichnen. Die Bezeichnung $\cdot^M$ werden wir nur dann verwenden, wenn wir explizit darauf hinweisen möchten, dass diese Multiplikation zu M gehört (etwa, wenn wir mehrere Halbgruppen auf einmal betrachten); in der Regel werden wir jedoch darauf verzichten.
Die Notationen „$\cdot$“ und „1“ sowie auch die Bezeichnungen „Multiplikation“ und „Eins“ sind von Beispielen wie dem der natürlichen Zahlen motiviert. Es gibt auch andere Beispiele, wo die Halbgruppenverknüpfung keine Multiplikation im vertrauten Sinne ist. In diesen konkret gegebenen Beispielen verwenden wir weiterhin die jeweils vorliegende Notation, die durch das Beispiel mitgebracht wird; siehe insbesondere Bemerkung (12.1).
Mit Hilfe der Standardnotation in einer Halbgruppe M liest sich die Assoziativität der Multiplikation wie folgt:

- *Assoziativität.* Für $x, y, z \in M$ ist $x(yz) = (xy)z$.

Ist eine Halbgruppe M kommutativ, so gilt neben der Assoziativität zusätzlich noch:

- *Kommutativität.* Für $x, y \in M$ ist $xy = yx$.

Mit Hilfe der Standardnotation in einem Monoid M lesen sich dessen *Axiome*, d.h. dessen definierende Eigenschaften, wie folgt:

- *Assoziativität.* Für $x, y, z \in M$ ist $x(yz) = (xy)z$.
- *Existenz der Eins.* Es existiert ein $e \in M$ derart, dass für $x \in M$ stets $ex = xe = x$ gilt. Dieses e ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für $x \in M$.

Da Monoide insbesondere Halbgruppen sind, erhalten wir auch den Begriff eines *kommutativen Monoids*.
Neben der Multiplikation auf den natürlichen Zahlen ist auch die Addition assoziativ und kommutativ. Für kommutative Halbgruppen, Monoide und Gruppen haben sich daher noch andere Bezeichnungen und Schreibweisen eingebürgert:

(6.18) Definition (abelsche Halbgruppe, abelsches Monoid)**.**

(a) Eine *abelsche Halbgruppe* ist eine kommutative Halbgruppe A mit Halbgruppenverknüpfung $+ = +^A$, genannt *Addition* von A.

(b) Ein *abelsches Monoid* ist eine abelsche Halbgruppe A, welche ein neutrales Element bzgl. $+^A$ besitzt. Das neutrale Element bzgl. der Addition wird auch *Null* (oder *Nullelement*) von A genannt und als $0 = 0^A$ notiert.

Eine abelsche Halbgruppe ist also strukturell gesehen das Gleiche wie eine kommutative Halbgruppe; wir verwenden lediglich in abstrakten abelschen Halbgruppen eine andere Standardnotation: Abstrakte Halbgruppen (die ggf. auch mal kommutativ sein dürfen, aber im Allgemeinen nicht müssen) werden multiplikativ geschrieben, abstrakte abelsche Halbgruppen werden additiv geschrieben.
Insbesondere gilt: Alle Aussagen über beliebige Halbgruppen und über kommutative Halbgruppen (in multiplikativer Notation geschrieben) bleiben auch für abelsche Halbgruppen (in additiver Notation geschrieben) korrekt. Umgekehrt bleiben alle Aussagen über abelsche Halbgruppen (in additiver Notation geschrieben) auch für kommutative Halbgruppen (in multiplikativer Notation geschrieben) korrekt. Bei der Verwendung solcher Aussagen muss gegebenenfalls nur die jeweilige Notation angepasst werden. In der Regel werden wir getroffene Aussagen über Halbgruppen nicht für abelsche Halbgruppen in additiver Notation wiederholen.
Mit Hilfe der Standardnotation in einer abelschen Halbgruppe A lesen sich deren Axiome wie folgt:

- *Assoziativität.* Für $x, y, z \in A$ ist $x + (y + z) = (x + y) + z$.

- *Kommutativität.* Für $x, y \in A$ ist $x + y = y + x$.

Die Axiome eines abelschen Monoids A sind die eines kommutativen Monoids in additiver Notation:

- *Assoziativität.* Für $x, y, z \in A$ ist $x + (y + z) = (x + y) + z$.
- *Existenz der Null.* Es existiert ein $n \in A$ derart, dass für $x \in A$ stets $n + x = x + n = x$ gilt. Dieses n ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 0 bezeichnet. Wir haben also $0 + x = x + 0 = x$ für $x \in A$.
- *Kommutativität.* Für $x, y \in A$ ist $x + y = y + x$.

Vom Rechnen in den natürlichen Zahlen sind wir es gewohnt, bei Produkten aus mehreren Faktoren bzw. Summen aus mehreren Summanden keine Klammern zu setzen. Dies ist durch die Assoziativität gerechtfertigt, da verschiedene Klammerungen zum selben Wert führen würden. Wir übertragen diese Konvention auf den allgemeinen Fall:

(6.19) Konvention. Wegen der Assoziativität der Multiplikation einer Halbgruppe bzw. der Addition einer abelschen Halbgruppe kommt es bei iterierter Bildung nicht auf die Klammerung an. Im Regelfall lassen wir daher die Klammern im Folgenden weg.

Nachdem wir alle in Satz (6.1)(a), (b) auftauchenden Phänomene analysiert und von den konkreten Beispielen $\mathbb{N}$ und $\mathbb{N}_0$ abstrahiert haben, lassen sich diese nun kurz wie folgt reformulieren.

(6.20) Beispiel.

(a) (i) Die Menge $\mathbb{N}$ zusammen mit der üblichen Addition ist eine abelsche Halbgruppe, aber kein abelsches Monoid.

(ii) Die Menge $\mathbb{N}$ zusammen mit der üblichen Multiplikation ist ein kommutatives Monoid. Die Eins von $\mathbb{N}$ ist die übliche Eins.

(b) (i) Die Menge $\mathbb{N}_0$ zusammen mit der üblichen Addition ist ein abelsches Monoid. Die Null von $\mathbb{N}_0$ ist die übliche Null.

(ii) Die Menge $\mathbb{N}_0$ zusammen mit der üblichen Multiplikation ist ein kommutatives Monoid. Die Eins von $\mathbb{N}_0$ ist die übliche Eins.

(6.21) Beispiel. Es gibt ein nicht-kommutatives Monoid mit genau drei Elementen, dessen Multiplikation durch folgende Verknüpfungstafel gegeben ist.

$\cdot$	1	c_1	c_2
1	1	c_1	c_2
c_1	c_1	c_1	c_1
c_2	c_2	c_2	c_2

Das Stringmonoid

Nach der bis hierher erfolgten abstrakten Begriffsbildung können wir nun das folgende Beispiel untersuchen, in welchem sich die soeben eingeführte Struktur eines Monoids erkennen lässt.

(6.22) Bemerkung. Es sei eine Menge X gegeben. Die Menge $\dot{\bigcup}_{k \in \mathbb{N}_0} X^k$ wird zu einem Monoid mit Monoidverknüpfung

$$((x_1, \ldots, x_k), (y_1, \ldots, y_l)) \mapsto (x_1, \ldots, x_k, y_1, \ldots, y_l)$$

und Einselement $( )$.

(6.23) Definition (Stringmonoid)**.** Es sei eine Menge X gegeben. Das Monoid mit unterliegender Menge $\dot{\bigcup}_{k \in \mathbb{N}_0} X^k$ und der Verknüpfung $((x_1, \ldots, x_k), (y_1, \ldots, y_l)) \mapsto (x_1, \ldots, x_k, y_1, \ldots, y_l)$ aus Bemerkung (6.22) wird *Stringmonoid* (oder *freies Monoid* oder *Wortmonoid*) über X genannt und als X^* notiert. Die Monoidverknüpfung von X^* wird *Konkatenation* (oder *Aneinanderhängung*) genannt. Ein Element von X^* wird *String* (oder *Zeichenkette*) in X genannt. Das Einselement von X^* wird *leerer String* in X genannt und als $\varepsilon := ( )$ notiert.
Für einen String $(x_1, \ldots, x_k)$ in X schreiben wir $x_1 \ldots x_k := (x_1, \ldots, x_k)$.

(6.24) Beispiel.

(a) Es sei ein Objekt a gegeben. Dann ist das Stringmonoid über $\{a\}$ gegeben durch

$$\{a\}^* = \{\varepsilon, a, aa, aaa, \dots\}.$$

(b) Es seien verschiedene Objekte a und b gegeben. Dann ist das Stringmonoid über $\{a, b\}$ gegeben durch

$$\{a, b\}^* = \{\varepsilon, a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, bab, bba, bbb, \dots\}.$$

Die Wichtigkeit des Stringmonoids, insbesondere in der (theoretischen) Informatik, ergibt sich durch die Betrachtung von Teilmengen:

(6.25) Definition (Sprache)**.** Es sei eine Menge X gegeben. Eine (*formale*) *Sprache* über X ist eine Teilmenge von X^*.
Es sei eine Sprache L über X gegeben. Die Menge X wird das *Alphabet* von L. Ein Element von X wird *Zeichen* (oder *Buchstabe*) in L genannt. Ein Element von L wird *Wort* in L genannt.

Da für eine Menge X auch das Stringmonoid X^* eine Sprache über X ist, werden die Strings in X, d.h. die Elemente von X^*, auch Wörter in X^* genannt.
Als Anwendungsbeispiel geben wir eine mögliche Formalisierung für die Sprache der Aussagenlogik, vgl. Definition (1.1), an:

(6.26) Anwendungsbeispiel. Das Alphabet der Aussagenlogik sei modelliert als Menge X gegeben durch

$$X = \{A_1, A_2, A_3, \dots\} \dot\cup \{0, 1, \neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\} \dot\cup \{(,)\}.$$

Die Sprache der Aussagenlogik lässt sich dann als (formale) Sprache über X auffassen.

Auch eine beliebige Programmiersprache, wie z.B. C, lässt sich als formale Sprache modellieren:

(6.27) Anwendungsbeispiel. Die Befehle und erlaubten Zeichen einer Programmiersprache seien als Elemente einer Menge X modelliert. Quelltexte für diese Programmiersprache lassen sich dann als Wörter einer Sprache über X auffassen.

Als kurzen Ausblick skizzieren wir das *Wortproblem*: Es sei eine Menge X gegeben. Für einen String x in X bezeichnen wir einen String x' in X als einen *Unterstring* (oder *Teilstring*) von x, falls es Strings p und s in X mit $x = px's$ gibt.
Ferner sei eine symmetrische Relation r auf X^* gegeben. Die bzgl. r in Relation stehenden Strings in X fassen wir als „Ersetzungsregeln“ im folgenden Sinn auf: Es seien Strings x und y in X gegeben. Wir sagen, dass x und y durch eine elementare Ersetzung auseinander hervorgehen, wenn es Strings p, s, x', y' in X mit $x = px's$, $y = py's$ und $x'\ r\ y'$ gibt, d.h. falls y durch Ersetzung des Unterstrings x' von x durch den Unterstring y' entsteht und umgekehrt.
Das Wortproblem ist nun folgendes: Es seien Strings x und y in X gegeben. Lässt sich überprüfen, ob x und y durch eine endliche Folge von elementaren Ersetzungen auseinander hervorgehen? In vielen Fällen ist dieses Problem nachweislich unentscheidbar.
Es sei L_x die bzgl. Inklusion kleinste Sprache, welche zum einen x enthält und welche zum anderen mit jedem Wort z in L_x auch alle diejenigen Strings in X enthält, die durch eine elementare Ersetzung aus z hervorgehen. ([1])
Mit Hilfe von L_x lässt sich das Wortproblem wie folgt umformulieren: Lässt sich überprüfen, ob y ein Wort von L_x ist?

[1] D.h. einerseits ist L_x eine Sprache derart, dass x in L_x enthalten ist, und so, dass mit jedem Wort z in L_x auch alle diejenigen Strings in X enthalten sind, welche durch eine elementare Ersetzung aus z hervorgehen, und andererseits gilt für jede Sprache L derart, dass x in L_x enthalten ist, und so, dass mit jedem Wort z in L_x auch alle diejenigen Strings in X enthalten sind, bereits, dass jedes Wort in L_x auch ein Wort von L ist.

Invertierbare Elemente

Wir legen eine Sprechweise für die Existenz eines inversen Elements bzgl. der Monoidverknüpfung in einem gegebenen Monoid fest:

(6.28) Definition (Invertierbarkeit)**.**

(a) Es sei ein Monoid M gegeben. Ein Element x in M heißt *invertierbar* in M (oder eine *Einheit* von M), falls es ein inverses Element zu x bzgl. $\cdot$ gibt. Das zu einem invertierbaren Element x in M bzgl. $\cdot$ inverse Element y wird auch das *Inverse* (oder das *inverse Element*) zu x in M genannt und als $x^{-1} = (x^{-1})^M := y$ notiert.

Die *Menge der invertierbaren Elemente* in M bezeichnen wir mit

$$M^\times = \{x \in M \mid x \text{ ist invertierbar}\}.$$

(b) Es sei ein abelsches Monoid A gegeben. Ein Element x in A heißt *negierbar* in A, falls es ein inverses Element zu x bzgl. $+^A$ gibt. Das zu einem negierbaren Element x in A bzgl. $+^A$ inverse Element y wird auch das *Negative* (oder das *negative Element*) zu x in A genannt und als $-x = (-x)^A := y$ notiert.

Die etwas ungewöhnlich aussehende Notation $(x^{-1})^M$ in Definition (6.28)(a) soll lediglich deutlich machen, in welchem Monoid wir das Inverse zu x bilden – nämlich gerade im Monoid M. Wir werden diese Notation nur dann verwenden, wenn wir explizit darauf hinweisen wollen, in welchem Monoid das Inverse gebildet wird.
Bei additiv geschriebenen abelschen Monoiden wird die Notation $M^\times$ in aller Regel nicht verwendet.

(6.29) Beispiel.

(a) Es ist ${\mathbb{N}_0}^\times = \{1\}$, d.h. das einzige invertierbare Element in $\mathbb{N}_0$ (bzgl. der üblichen Multiplikation) ist 1.

(b) Das einzige negierbare Element in $\mathbb{N}_0$ (bzgl. der üblichen Addition) ist 0.

(c) Für jede Menge X ist $(X^*)^\times = \{\varepsilon\}$.

Wir wollen einige einfache Eigenschaften von invertierbaren Elementen herleiten.

(6.30) Proposition. Es sei ein Monoid M gegeben.

(a) Für $x, y \in M^\times$ ist auch $xy \in M^\times$ mit $(xy)^{-1} = y^{-1}x^{-1}$.

(b) Es ist $1 \in M^\times$ mit $1^{-1} = 1$.

(c) Für $x \in M^\times$ ist auch $x^{-1} \in M^\times$ mit $(x^{-1})^{-1} = x$.

Beweis. Dies lässt sich analog zu Proposition (3.21) beweisen. Die Details seien dem Leser zur Übung überlassen. □

(6.31) Bemerkung. Es seien ein Monoid M und $a \in M^\times$, $b, x \in M$ gegeben.

(a) Genau dann gilt $ax = b$, wenn $x = a^{-1}b$ ist.

(b) Genau dann gilt $xa = b$, wenn $x = ba^{-1}$ ist.

Beweis.

(a) Wenn $ax = b$ gilt, dann auch

$$x = 1x = a^{-1}ax = a^{-1}b.$$

Umgekehrt, wenn $x = a^{-1}b$ ist, dann haben wir nach Proposition (6.30)(c) auch

$$b = (a^{-1})^{-1}x = ax.$$

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

(6.32) Korollar. Es sei ein Monoid M gegeben.

(a) Es seien $a \in M^\times$, $x, y \in M$ gegeben. Wenn $ax = ay$ oder $xa = ya$ gilt, dann ist $x = y$.

(b) Es seien $a \in M^\times$, $x \in M$ gegeben. Wenn $ax = a$ oder $xa = a$ gilt, dann ist $x = 1$.

Beweis.

(a) Es gelte $ax = ay$; der andere Fall wird analog bewiesen. Nach Bemerkung (6.31)(a) ist dann

$$x = a^{-1}ay = 1y = y.$$

(b) Es gelte $ax = a$; der andere Fall wird analog bewiesen. Dann haben wir $ax = a1$ und also $x = 1$ nach (a). □

Gruppen

Im abelschen Monoid der ganzen Zahlen $\mathbb{Z}$ zusammen mit der üblichen Addition ist jedes Element negierbar, vgl. Satz (6.1)(c)(iii). Für eine solche Situation benutzen wir einen neuen Begriff, den wir jetzt einführen wollen.

(6.33) Definition ((abelsche) Gruppe)**.**

(a) Eine *Gruppe* ist ein Monoid G, in welchem jedes Element von G invertierbar ist. Die Monoidverknüpfung einer Gruppe G wird auch *Gruppenverknüpfung* von G genannt.

(b) Eine *abelsche Gruppe* ist ein abelsches Monoid A, in welchem jedes Element von A negierbar ist.

Die Axiome einer Gruppe G in Standardnotation lesen sich insgesamt wie folgt:

- *Assoziativität.* Für $x, y, z \in G$ ist $x(yz) = (xy)z$.
- *Existenz der Eins.* Es existiert ein $e \in G$ derart, dass für $x \in G$ stets $ex = xe = x$ gilt. Dieses e ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für $x \in G$.
- *Existenz der Inversen.* Für jedes $x \in G$ existiert ein $y \in G$ mit $yx = xy = 1$. Dieses y ist nach Korollar (6.16) eindeutig bestimmt und wird mit x^{-1} bezeichnet. Wir haben also $x^{-1}x = xx^{-1} = 1$.

Ist G kommutativ, so gilt zusätzlich noch:

- *Kommutativität.* Für $x, y \in G$ ist $xy = yx$.

Die Axiome einer abelschen Gruppe A sind die einer kommutativen Gruppe in additiver Notation. Wir betonen noch einmal: Jede kommutative Gruppe lässt sich als abelsche Gruppe auffassen und umgekehrt – strukturell gesehen sind es die gleichen Objekte, wir bringen durch die unterschiedlichen Terminologien lediglich zum Ausdruck, welche Notation wir verwenden. Insbesondere bleiben alle Aussagen über Gruppen auch für abelsche Gruppen gültig, sie müssen nur in der Notation angepasst werden.
Wir fassen einige Eigenschaften aus Satz (6.1)(c), (d) mit Hilfe der neuen Terminologien noch einmal zusammen:

(6.34) Beispiel.

(a) (i) Die Menge $\mathbb{Z}$ zusammen mit der üblichen Addition ist eine abelsche Gruppe. Die Null von $\mathbb{Z}$ ist die übliche Null. Für $x \in \mathbb{Z}$ ist das Negative zu x in $\mathbb{Z}$ das übliche Negative.

(ii) Die Menge $\mathbb{Z}$ zusammen mit der üblichen Multiplikation ist ein kommutatives Monoid, aber keine Gruppe. Die Eins von $\mathbb{Z}$ ist die übliche Eins.

(b) (i) Die Menge $\mathbb{Q}$ zusammen mit der üblichen Addition ist eine abelsche Gruppe. Die Null von $\mathbb{Q}$ ist die übliche Null. Für $x \in \mathbb{Q}$ ist das Negative zu x in $\mathbb{Q}$ das übliche Negative.

(ii) Die Menge $\mathbb{Q}$ zusammen mit der üblichen Multiplikation ist ein kommutatives Monoid, aber keine Gruppe. Die Eins von $\mathbb{Q}$ ist die übliche Eins.

(iii) Die Menge $\mathbb{Q} \setminus \{0\}$ zusammen mit der üblichen Multiplikation ist eine kommutative Gruppe. Die Eins von $\mathbb{Q} \setminus \{0\}$ ist die übliche Eins. Für $x \in \mathbb{Q} \setminus \{0\}$ ist das Inverse zu x in $\mathbb{Q} \setminus \{0\}$ das übliche Inverse.

(6.35) Konvention. Wenn wir in Zukunft von der abelschen Gruppe $\mathbb{Z}$ sprechen, so meinen wir damit stets $\mathbb{Z}$ mit der üblichen Addition. Wenn wir vom kommutativen Monoid $\mathbb{Z}$ sprechen, so meinen wir damit stets $\mathbb{Z}$ mit der üblichen Multiplikation. Ähnlich für $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Q}$, $\mathbb{R}$.

(6.36) Beispiel. Es gibt eine nicht-kommutative Gruppe mit genau sechs Elementen, dessen Multiplikation durch folgende Verknüpfungstafel gegeben ist.

$\cdot$	1	τ_1	τ_2	τ_3	σ_1	σ_2
1	1	τ_1	τ_2	τ_3	σ_1	σ_2
τ_1	τ_1	1	σ_2	σ_1	τ_3	τ_2
τ_2	τ_2	σ_1	1	σ_2	τ_1	τ_3
τ_3	τ_3	σ_2	σ_1	1	τ_2	τ_1
σ_1	σ_1	τ_2	τ_3	τ_1	σ_2	1
σ_2	σ_2	τ_3	τ_1	τ_2	1	σ_1

Wie von den ganzen Zahlen bekannt, liefert die Existenz von negativen Elementen in einer abelschen Gruppe eine neue Verknüpfung:

(6.37) Definition (Subtraktion)**.** Es sei eine abelsche Gruppe A gegeben. Die Verknüpfung $(x, y) \mapsto x + (-y)$ auf A wird *Subtraktion* von A genannt und als $-$ notiert.

Wir betonen, dass die Addition einer abelschen Gruppe A ein Teil der Daten von A ist (d.h. A besteht aus der unterliegenden Menge, die unter Missbrauch der Notation ebenfalls mit A bezeichnet wird, und der Addition). Hingegen wird die Subtraktion mit Hilfe der Addition und den negativen Elementen definiert und ist insbesondere somit durch die Daten (unterliegende Menge und Addition) eindeutig festgelegt.
Da Gruppen (multiplikativ geschrieben) nicht kommutativ sein müssen, können wir die analoge Verknüpfung $(x, y) \mapsto x : y$, wie etwa aus dem Beispiel $\mathbb{Q} \setminus \{0\}$ bekannt, nicht bilden: für Gruppenelemente x und y muss im Allgemeinen nicht $xy^{-1} = y^{-1}x$ gelten. Genauer gesagt erhalten wir zwei Verknüpfungen, welche im Allgemeinen nicht übereinstimmen und für welche sich keine neue Notation eingebürgert hat.

Die Gruppe der invertierbaren Elemente

Während in einer Gruppe jedes Element invertierbar ist, haben wir in einem beliebigen Monoid auch nicht-invertierbare Elemente. In Beispiel (6.34)(b)(iii) haben wir gesehen, dass wir eine Gruppe erhalten, wenn wir die Multiplikation des Monoids $\mathbb{Q}$ auf die Menge der invertierbaren Elemente $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ einschränken. Dieses Resultat lässt sich auf beliebige Monoide verallgemeinern:

(6.38) Bemerkung. Für jedes Monoid M wird $M^\times$ eine Gruppe, wobei die Multiplikation auf $M^\times$ durch

$$x \cdot^{M^\times} y = x \cdot^{M} y$$

für $x, y \in M$ gegeben ist.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(6.39) Definition (Gruppe der invertierbaren Elemente)**.** Es sei ein Monoid M gegeben. Die Gruppe $M^\times$ mit der Multiplikation aus Bemerkung (6.38) heißt *Gruppe der invertierbaren Elemente* (oder *Einheitengruppe*) von M.

Ein Monoid G ist also genau dann eine Gruppe, wenn $G^\times = G$ ist.

(6.40) Beispiel.

(a) Es ist

$$\mathbb{Z}^\times = \{1, -1\}.$$

(b) Es ist

$$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}.$$

Ringe und Körper

Bei den uns vertrauten Strukturen spielen jeweils Addition und Multiplikation eine wichtige Rolle. Aus diesem Grund wollen wir als nächstes algebraische Strukturen betrachten, deren unterliegende Mengen mit zwei Verknüpfungen versehen sind.

(6.41) Definition (Ring, kommutativer Ring, Körper)**.**

(a) Ein *Ring* (genauer *unitärer Ring* oder *Ring mit Eins* oder *Ring mit Einselement*) besteht aus einer abelschen Gruppe R zusammen mit einer Verknüpfung m auf R so, dass die unterliegende Menge von R ein Monoid mit Multiplikation m wird und so, dass folgendes Axiom gilt.

- *Distributivität.* Für alle $x, y, z \in R$ ist

$$x\, m\, (y + z) = (x\, m\, y) + (x\, m\, z),$$
$$(x + y)\, m\, z = (x\, m\, z) + (y\, m\, z).$$

Unter Missbrauch der Notation bezeichnen wir sowohl den besagten Ring als auch die unterliegende abelsche Gruppe mit R. Die Verknüpfung m wird *Multiplikation* von R genannt.

Für einen Ring R mit Multiplikation m schreiben wir wie üblich $\cdot = \cdot^R := m$ und $xy = x \cdot y$ für $x, y \in R$.

(b) Ein Ring R heißt *kommutativ*, falls die Multiplikation von R kommutativ ist.

(c) Ein *Körper* ist ein kommutativer Ring K, in welchem $1 \neq 0$ gilt und in welchem jedes Element von $K \setminus \{0\}$ invertierbar (bzgl. der Multiplikation $\cdot^K$) ist.

(6.42) Konvention. In Ringen lassen wir die Klammern um Produkte meistens weg, d.h. es gelte *Punkt- vor Strichrechnung.*

Wir verwenden die in Definition (6.18)(a) bzw. Definition (6.17)(a) eingeführten Notationen für die Addition einer abelschen Halbgruppe (und also insbesondere einer abelschen Gruppe) bzw. für die Multiplikation einer Halbgruppe (und also insbesondere eines Monoids) auch weiterhin für Ringe. Ebenso verwenden wir die Notationen und Begriffe für die neutralen und inversen Elemente bzgl. dieser Verknüpfungen, vgl. Definition (6.28)(a) und Definition (6.37).
Die Axiome eines Rings R in Standardnotation lesen sich also wie folgt:

- *Assoziativität der Addition.* Für $x, y, z \in R$ ist $x + (y + z) = (x + y) + z$.
- *Existenz der Null.* Es existiert ein $n \in R$ derart, dass für $x \in R$ stets $n + x = x + n = x$ gilt. Dieses n ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 0 bezeichnet. Wir haben also $0 + x = x + 0 = x$ für alle $x \in R$.
- *Existenz der Negativen.* Für jedes $x \in R$ existiert ein $y \in R$ mit $y + x = x + y = 0$. Dieses y ist nach Korollar (6.16) eindeutig bestimmt und wird mit $-x$ bezeichnet. Wir haben also $(-x) + x = x + (-x) = 0$.
- *Kommutativität der Addition.* Für $x, y \in R$ ist $x + y = y + x$.
- *Assoziativität der Multiplikation.* Für $x, y, z \in R$ ist $x(yz) = (xy)z$.
- *Existenz der Eins.* Es existiert ein $e \in R$ derart, dass für $x \in R$ stets $ex = xe = x$ gilt. Dieses e ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für alle $x \in R$.
- *Distributivität.* Für $x, y, z \in R$ ist $x(y + z) = xy + xz$ und $(x + y)z = xz + yz$.

Ist R kommutativ, so gilt zusätzlich noch:

- *Kommutativität der Multiplikation.* Für $x, y \in R$ ist $xy = yx$.

Ist R ein Körper, so ist R kommutativ und es gilt ferner noch:

- *Existenz der Inversen.* Es ist $1 \neq 0$. Für jedes $x \in K \setminus \{0\}$ existiert ein $y \in K$ mit $yx = xy = 1$. Dieses y ist nach Korollar (6.16) eindeutig bestimmt und wird mit x^{-1} bezeichnet. Wir haben also $x^{-1}x = xx^{-1} = 1$.

Selbstverständlich bleiben alle Aussagen über (abelsche) Gruppen für die einem Ring unterliegende abelsche Gruppe, bestehend aus der unterliegenden Menge zusammen mit der Addition des Rings, sowie alle Aussagen über Monoide für das einem Ring unterliegende Monoid, bestehend aus der unterliegenden Menge zusammen mit der Multiplikation des Rings, gültig.
Mit Hilfe der Begriffe aus Definition (6.41) lassen sich die Aussagen aus Satz (6.1)(c), (d) noch knapper zusammenfassen:

(6.43) Beispiel.

(a) Die Menge $\mathbb{Z}$ zusammen mit der üblichen Addition und der üblichen Multiplikation ist ein kommutativer Ring, aber kein Körper. Die Null von $\mathbb{Z}$ ist die übliche Null und die Eins von $\mathbb{Z}$ ist die übliche Eins. Für $x \in \mathbb{Z}$ ist das Negative zu x in $\mathbb{Z}$ das übliche Negative.

(b) Die Menge $\mathbb{Q}$ zusammen mit der üblichen Addition und der üblichen Multiplikation ist ein Körper. Die Null von $\mathbb{Q}$ ist die übliche Null und die Eins von $\mathbb{Q}$ ist die übliche Eins. Für $x \in \mathbb{Q}$ ist das Negative zu x in $\mathbb{Q}$ das übliche Negative und für $x \in \mathbb{Q} \setminus \{0\}$ ist das Inverse zu x in $\mathbb{Q}$ das übliche Inverse.

(6.44) Konvention. Wenn wir in Zukunft vom (kommutativen) Ring $\mathbb{Z}$ sprechen, so meinen wir damit stets $\mathbb{Z}$ mit der üblichen Addition und der üblichen Multiplikation. Ähnlich für $\mathbb{Q}$ und $\mathbb{R}$.

(6.45) Beispiel. Es gibt einen Körper mit genau zwei Elementen, der Null 0 und der Eins 1, dessen Addition und Multiplikation durch folgende Verknüpfungstafeln gegeben sind.

$+$	0	1
0	0	1
1	1	0

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

(6.46) Beispiel. Es gibt einen nicht-kommutativen Ring mit genau acht Elementen, dessen Addition und Multiplikation durch folgende Verknüpfungstafeln gegeben sind.

$+$	0	1	e_1	e_2	n	u	s_1	s_2
0	0	1	e_1	e_2	n	u	s_1	s_2
1	1	0	e_2	e_1	u	n	s_2	s_1
e_1	e_1	e_2	0	1	s_1	s_2	n	u
e_2	e_2	e_1	1	0	s_2	s_1	u	n
n	n	u	s_1	s_2	0	1	e_1	e_2
u	u	n	s_2	s_1	1	0	e_2	e_1
s_1	s_1	s_2	n	u	e_1	e_2	0	1
s_2	s_2	s_1	u	n	e_2	e_1	1	0

$\cdot$	0	1	e_1	e_2	n	u	s_1	s_2
0	0	0	0	0	0	0	0	0
1	0	1	e_1	e_2	n	u	s_1	s_2
e_1	0	e_1	e_1	0	n	s_1	s_1	n
e_2	0	e_2	0	e_2	0	e_2	0	e_2
n	0	n	0	n	0	n	0	n
u	0	u	e_1	s_2	n	1	s_1	e_2
s_1	0	s_1	e_1	n	n	e_1	s_1	0
s_2	0	s_2	0	s_2	0	s_2	0	s_2

Eine Axiomatisierung der Eigenschaften von $\mathbb{N}_0$, welche Addition und Multiplikation involviert, wird manchmal *Halbring* genannt. Da eine solche Struktur für uns im Folgenden nur von untergeordnetem Interesse sein würde, werden wir solche Strukturen nicht einführen und genauer betrachten.
Im Folgenden halten wir einige elementare Eigenschaften von Ringen und Körpern fest.

(6.47) Proposition. Es sei ein Ring R gegeben.

(a) Für $a \in R$ gilt $a \cdot 0 = 0 \cdot a = 0$.

(b) Für $a, b \in R$ gilt $a(-b) = (-a)b = -ab$.

(c) Für $a, b \in R$ gilt $(-a)(-b) = ab$.

Beweis.

(a) Für $a \in R$ gilt

$$a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0$$

und damit $a \cdot 0 = 0$ nach Korollar (6.32)(b).

(b) Für $a, b \in R$ gilt

$$a(-b) + ab = a((-b) + b) = a \cdot 0 = 0$$

nach (a) und damit $-ab = a(-b)$. Die andere Gleichung zeigt man analog.

(c) Für $a, b \in R$ gilt

$$(-a)(-b) = -a(-b) = -(-ab) = ab$$

nach (b). □

Die Ringe $\mathbb{Z}$ und $\mathbb{Q}$ sind nullteilerfrei, eine Eigenschaft, welche nicht in jedem Ring gilt. Nullteilerfreie kommutative Ringe sind unter folgendem Namen bekannt:

(6.48) Definition (Integritätsbereich)**.** Ein *Integritätsbereich* ist ein kommutativer Ring R mit $1 \neq 0$ und so, dass folgende Eigenschaft gilt:

- *Nullteilerfreiheit.* Für $a, b \in R$ aus $ab = 0$ stets $a = 0$ oder $b = 0$ folgt.

(6.49) Beispiel. Es gibt einen kommutativen Ring mit genau vier Elementen, dessen Addition und Multiplikation durch folgende Verknüpfungstafeln gegeben sind, welcher kein Integritätsbereich ist.

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

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Der Ring aus Beispiel (6.46) liefert ein Beispiel für einen nicht-kommutativen Ring, welcher nicht nullteilerfrei ist, d.h. in welchem es zwei (nicht notwendigerweise verschiedene) von Null verschiedene Elemente gibt, deren Produkt Null ist.

(6.50) Proposition. Jeder Körper ist ein Integritätsbereich.

Beweis. Es seien ein Körper K und $a, b \in K$ mit $ab = 0$ gegeben. Ferner gelte $a \neq 0$. Dann ist $a \in K^\times$, nach Bemerkung (6.31)(a) und Proposition (6.47)(a) folgt also $b = a^{-1}0 = 0$. □

(6.51) Beispiel. Der Ring $\mathbb{Z}$ ist ein Integritätsbereich.

Beweis. Nach Proposition (6.50) ist $\mathbb{Q}$ als Körper ein Integritätsbereich, d.h. für $a, b \in \mathbb{Q}$ folgt aus $ab = 0$ stets $a = 0$ oder $b = 0$. Wegen $\mathbb{Z} \subseteq \mathbb{Q}$ folgt dann aber insbesondere für $a, b \in \mathbb{Z}$ aus $ab = 0$ stets $a = 0$ oder $b = 0$. Folglich ist auch $\mathbb{Z}$ ein Integritätsbereich. □

(6.52) Bemerkung. Es sei ein kommutativer Ring R mit $1 \neq 0$ gegeben. Die folgenden Bedingungen sind äquivalent:

(a) Es ist R ein Integritätsbereich.

(b) Für $a, x, y \in R$ folgt aus $ax = ay$ stets $a = 0$ oder $x = y$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

Sebastian Thomas

RWTH Aachen, WS 2016/17
17.11.2016

Diskrete Strukturen

Vorlesung 9 (vorläufig)

7 Ordnungsstrukturen

Ordnungen

(7.1) Definition (Präordnung, Ordnung, Totalordnung)**.** Es sei eine Menge X gegeben.

(a) Eine *Präordnung* (oder *Präordnungsrelation*) auf X ist eine Relation auf X, welche transitiv und reflexiv ist.

(b) Eine *Ordnung* (genauer *partielle Ordnung*, oder *Ordnungsrelation* oder *partielle Ordnungsrelation*) auf X ist eine antisymmetrische Präordnung auf X.

(c) Eine *Totalordnung* (oder *Totalordnungsrelation*) auf X ist eine vollständige Ordnung auf X.

Wir erinnern an die übliche Ordnung auf der Menge der natürlichen Zahlen $\mathbb{N}$: Für $m, n \in \mathbb{N}$ gilt genau dann $m \leq n$, wenn es ein $p \in \mathbb{N}_0$ mit $n = p + m$ gibt.

(7.2) Beispiel.

(a) Die Relation $\leq$ auf $\mathbb{N}$ ist eine Totalordnung.

(b) Es sei eine Menge X gegeben. Die Relation $\subseteq$ auf $\mathrm{Pot}(X)$ ist eine Ordnung.

(c) Die Relation $<$ auf $\mathbb{N}$ ist keine Präordnung.

Beweis.

(a) Es seien $m, n, p \in \mathbb{N}$ mit $m \leq n$ und $n \leq p$ gegeben. Dann gibt es $q, r \in \mathbb{N}_0$ mit $n = q + m$ und $p = r + n$. Es folgt $p = r + n = r + q + m$, also $m \leq p$. Folglich ist $\leq$ transitiv.

Für alle $m \in \mathbb{N}$ gilt $m = 0 + m$ und damit $m \leq m$. Folglich ist $\leq$ reflexiv.

Es seien $m, n \in \mathbb{N}$ mit $m \leq n$ und $n \leq m$ gegeben, so dass es ein $p, q \in \mathbb{N}_0$ mit $n = p + m$ und $m = q + n$ gibt. Dann folgt $m = q + n = q + p + m$, also $q + p = 0$. Dies impliziert aber $p = 0$ und damit $m = n$. Folglich ist $\leq$ antisymmetrisch.

Für $m, n \in \mathbb{N}$ gibt es ferner $p \in \mathbb{N}_0$ mit $n = p + m$ oder $m = p + n$, d.h. es gilt $m \leq n$ oder $n \leq m$. Folglich ist $\leq$ vollständig.

Insgesamt ist $\leq$ eine Totalordnung auf $\mathbb{N}$.

(b) Für $U, V, W \in \mathrm{Pot}(X)$ mit $U \subseteq V$ und $V \subseteq W$ gilt auch $U \subseteq W$. Folglich ist $\subseteq$ transitiv.

Für $U \in \mathrm{Pot}(X)$ gilt $U \subseteq U$. Folglich ist $\subseteq$ reflexiv.

Für $U, V \in \mathrm{Pot}(X)$ mit $U \subseteq V$ und $V \subseteq U$ gilt nach dem Gleichheitskriterium für Mengen (2.13) stets $U = V$. Folglich ist $\subseteq$ antisymmetrisch.

Insgesamt ist $\subseteq$ eine Ordnung auf $\mathrm{Pot}(X)$.

(c) Nach Beispiel (4.5) ist $<$ nicht reflexiv, also insbesondere keine Präordnung. □

(7.3) Beispiel. Es seien verschiedene Objekte a, b und c gegeben.

(a) Die Relation $\{(a,a), (b,b), (c,c), (a,b), (a,c)\}$ ist eine Ordnung auf $\{a, b, c\}$.

(b) Die Relation $\{(a,a), (b,b), (c,c), (a,c), (b,c)\}$ ist eine Ordnung auf $\{a, b, c\}$.

(c) Die Relation $\{(a,a), (b,b), (c,c), (b,a), (a,c), (b,c)\}$ ist eine Totalordnung auf $\{a, b, c\}$.

(d) Die Relation $\{(a,a), (b,b), (c,c), (a,b), (a,c), (b,c)\}$ ist eine Totalordnung auf $\{a, b, c\}$.

(e) Die Relation $\{(a,a), (b,b), (c,c), (a,b), (b,a), (a,c), (b,c)\}$ ist eine Präordnung auf $\{a, b, c\}$.

Geordnete Mengen

(7.4) Definition (prägeordnete Menge, geordnete Menge, total geordnete Menge)**.**

(a) Eine *prägeordnete Menge* besteht aus einer Menge X zusammen mit einer Präordnung o auf X. Unter Missbrauch der Notation bezeichnen wir sowohl die besagte prägeordnete Menge als auch die unterliegende Menge mit X. Die Präordnung o wird *Präordnung* von X genannt.

Für eine prägeordnete Menge X mit Präordnung o schreiben wir $\leq = \leq^X := o$.

(b) Eine *geordnete Menge* (genauer *partiell geordnete Menge*) ist eine prägeordnete Menge X derart, dass die Präordnung von X eine Ordnung auf der unterliegenden Menge von X ist. Die Präordnung einer geordneten Menge wird auch *Ordnung* von X genannt.

(c) Eine *totalgeordnete Menge* (oder *angeordnete Menge*) ist eine geordnete Menge X derart, dass die Ordnung von X eine Totalordnung auf der unterliegenden Menge von X ist. Die Ordnung einer totalgeordneten Menge wird auch *Totalordnung* von X genannt.

(7.5) Beispiel.

(a) Die Menge $\mathbb{N}$ zusammen mit der üblichen Ordnung ist eine totalgeordnete Menge.

(b) Es sei eine Menge X gegeben. Die Potenzmenge $\mathrm{Pot}(X)$ zusammen mit der Inklusionsrelation $\subseteq$ ist eine geordnete Menge.

(7.6) Konvention.

(a) Wenn wir in Zukunft von der geordneten Menge $\mathbb{N}$ sprechen, so meinen wir damit stets $\mathbb{N}$ mit der üblichen Ordnung. Ähnlich für $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

(b) Es sei eine Menge X gegeben. Wenn wir in Zukunft von der geordneten Menge $\mathrm{Pot}(X)$ sprechen, so meinen wir damit stets $\mathrm{Pot}(X)$ mit der Inklusionsrelation. Ähnlich für $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

(7.7) Definition (Striktordnung)**.** Es sei eine geordnete Menge X gegeben. Für $x, y \in X$ gelte genau dann $x < y$, wenn $x \leq y$ und $x \neq y$ ist. Die Relation $< = <^U$ auf X wird *Striktordnung* von X genannt.

(7.8) Bemerkung. Es seien eine prägeordnete Menge X und eine Teilmenge U von X gegeben. Die Menge U wird zu einer prägeordneten Menge mit Präordnung $\leq^U$ gegeben wie folgt. Für $u, v \in U$ gilt genau dann $u \leq^U v$ in U, wenn $u \leq^X v$ in X gilt. Wenn X eine geordnete Menge ist, dann wird U ebenfalls eine geordnete Menge. Wenn X eine total geordnete Menge ist, dann wird U ebenfalls eine total geordnete Menge.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(7.9) Beispiel.

(a) Für jedes $n \in \mathbb{N}_0$ wird $[1, n]$ eine totalgeordnete Menge.

(b) Es sei eine Menge X gegeben. Die Menge $\mathrm{Pot}(X) \setminus \{0\}$ wird eine geordnete Menge.

Extremale Elemente

Nun studieren wir Elemente von geordneten Mengen, welche extremal bzgl. der gegebenen Ordnung sind.

(7.10) Definition (minimales Element, kleinstes Element, maximales Element, größtes Element)**.** Es seien eine prägeordnete Menge X und ein $x \in X$ gegeben.

(a) (i) Wir sagen, dass x ein *minimales* Element in X ist, falls für alle $y \in X$ mit $y \leq x$ auch $x \leq y$ gilt.

(ii) Wir sagen, dass x ein *kleinstes* Element in X ist, falls $x \leq y$ für alle $y \in X$ gilt.

(b) (i) Wir sagen, dass x ein *maximales* Element in X ist, falls für alle $y \in X$ mit $x \leq y$ bereits $y \leq x$ gilt.

(ii) Wir sagen, dass x ein *größtes* Element in X ist, falls $y \leq x$ für alle $y \in X$ gilt.

(7.11) Beispiel.

(a) Es ist 1 ein minimales und kleinstes Element in $\mathbb{N}$. Maximale und größte Elemente gibt es in $\mathbb{N}$ nicht.

(b) Es sei eine Menge X gegeben. Dann ist $\emptyset$ ein minimales und kleinstes Element und X ein maximales und größtes Element in $\mathrm{Pot}(X)$.

(c) Die minimalen Elemente in $\mathrm{Pot}(\{1,2,3\}) \setminus \{\emptyset\}$ (bzgl. der Inklusionsrelation) sind die einelementigen Mengen $\{1\}$, $\{2\}$ und $\{3\}$. Kleinste Elemente gibt es in $\mathrm{Pot}(\{1,2,3\}) \setminus \{\emptyset\}$ nicht.

(d) Die maximalen Elemente in $\mathrm{Pot}(\{1,2,3\}) \setminus \{\{1,2,3\}\}$ (bzgl. der Inklusionsrelation) sind die zweielementigen Mengen $\{1,2\}$, $\{1,3\}$ und $\{2,3\}$. Größte Elemente gibt es in $\mathrm{Pot}(\{1,2,3\}) \setminus \{\{1,2,3\}\}$ nicht.

(7.12) Bemerkung. Es sei eine prägeordnete Menge X gegeben.

(a) Jedes kleinste Element in X ist auch minimal.

(b) Jedes größte Element in X ist auch maximal.

Beweis.

(a) Es sei ein kleinstes Element x in X gegeben, so dass $x \leq y$ für alle $y \in X$ gilt. Dann gilt aber insbesondere für alle $y \in X$ mit $y \leq x$ auch $x \leq y$. Folglich ist x minimal in X.

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

(7.13) Bemerkung. Es sei eine geordnete Menge X und ein $x \in X$ gegeben.

(a) Die folgenden Bedingungen sind äquivalent.

  (i) Das Element x ist minimal in X

  (ii) Für $y \in X$ gilt genau dann $y \leq x$, wenn $y = x$ gilt.

(b) Die folgenden Bedingungen sind äquivalent.

  (i) Das Element x ist maximal in X

  (ii) Für $y \in X$ gilt genau dann $x \leq y$, wenn $y = x$ gilt.

Beweis.

(a) Zunächst gelte Bedingung (i), d.h. x sei minimal in X. Für $y \in X$ mit $y \leq x$ gilt dann auch $x \leq y$ und damit $y = x$ auf Grund der Antisymmetrie der Ordnung $\leq$. Für $y \in X$ mit $y = x$ gilt hingegen auch $y \leq x$ auf Grund der Reflexivität von $\leq$. Somit gilt für $y \in X$ genau dann $y \leq x$, wenn $y = x$ gilt, d.h. es gilt Bedingung (ii).

  Umgekehrt gelte Bedingung (ii), d.h. für $y \in X$ gelte genau dann $y \leq x$, wenn $y = x$ gilt. Dann gilt insbesondere für $y \in X$ mit $y \leq x$ auch $y = x$, auf Grund der Reflexivität von $\leq$ also auch $x \leq y$. Folglich ist x minimal in X, d.h. es gilt Bedingung (i).

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

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

In Beispiel (7.11)(c) haben wir gesehen, dass es mehrere minimale Elemente bzgl. einer Ordnung geben kann. Nun werden wir zeigen, dass kleinste Elemente in geordneten Mengen hingegen stets eindeutig sind.

(7.14) Bemerkung. Es sei eine geordnete Menge X gegeben.

(a) Es seien ein kleinstes Element x und ein minimales Element y in X gegeben. Dann ist $x = y$.

(b) Es seien ein größtes Element x und ein maximales Element y in X gegeben. Dann ist $x = y$.

Beweis.

(a) Da x ein kleinstes Element in X ist, gilt insbesondere $x \leq y$. Die Minimalität von y impliziert nun aber bereits $x = y$ nach Bemerkung (a).

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

(7.15) Korollar. Es sei eine geordnete Menge X gegeben.

(a) Es gibt höchstens ein kleinstes Element in X.

(b) Es gibt höchstens ein größtes Element in X.

Beweis.

(a) Es seien x und x' kleinste Elemente in X. Dann ist x' auch minimal nach Bemerkung (7.12)(a) und daher $x = x'$ nach Bemerkung (7.14)(a).

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

(7.16) Proposition. Es seien eine total geordnete Menge X und ein $x \in X$ gegeben.

(a) Genau dann ist x minimal in X, wenn es ein kleinstes Element in X ist.

(b) Genau dann ist x maximal in X, wenn es ein größte Element in X ist.

Beweis.

(a) Zunächst sei x minimal in X. Nach Bemerkung (7.13)(a) gilt dann für alle $y \in X$ mit $y \leq x$ bereits $y = x$. Im Umkehrschluss bedeutet dies, dass für alle $y \in X \setminus \{x\}$ nicht $y \leq x$ ist. Die Vollständigkeit von $\leq$ impliziert dann aber bereits, dass $x \leq y$ für alle $y \in X \setminus \{x\}$ gilt. Andererseits gilt aber auch $x \leq x$ wegen der Reflexivität von $\leq$. Insgesamt ist also $x \leq y$ für alle $y \in X$, d.h. x ist ein kleinstes Element in X.

Umgekehrt, wenn x ein kleinstes Element in X ist, so ist x nach Bemerkung (7.12)(a) auch minimal.

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

Sebastian Thomas

RWTH Aachen, WS 2016/17
17.11.2016–23.11.2016

Diskrete Strukturen
Vorlesungen 9 und 10 (vorläufig)

8 Induktion und Rekursion

Induktion

Da uns die natürlichen Zahlen vertraut sind, haben wir auch ein intuitives Verständnis für die Gültigkeit des folgenden Satzes:

(8.1) Satz (Peano-Arithmetik)**.** Es sei $s\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto n+1$. Dann gilt:

(a) Es ist s injektiv.

(b) Es ist $1 \notin \operatorname{Im} s$.

(c) *Induktionsprinzip.* Für jede Teilmenge U von $\mathbb{N}$ mit $1 \in U$ und $s(U) \subseteq U$ (d.h. für alle $n \in U$ ist auch $s(n) = n+1 \in U$) gilt $U = \mathbb{N}$.

Die in Satz (8.1) aufgeführten Eigenschaften charakterisieren die natürlichen Zahlen bis auf Bijektion. Mit Hilfe dieser Eigenschaften lassen sich die Addition, die Multiplikation und die Ordnung auf $\mathbb{N}$ konstruieren.
Für uns von besonderem Interesse ist das Induktionsprinzip (8.1)(c) (auch *Prinzip der vollständigen Induktion* genannt), welches sich wie folgt äquivalent umformulieren lässt: Zum Beweis einer Aussage der Form

$$(\forall n \in \mathbb{N} : A(n)) := (\forall n : n \in \mathbb{N} \Rightarrow A(n))$$

können wir zeigen, dass die Aussage der Form

$$A(1) \wedge (\forall n \in \mathbb{N} : A(n) \Rightarrow A(n+1))$$

gültig ist, d.h. dass zum einen die Aussage der Form

$$A(1)$$

und zum anderen für jedes $n \in \mathbb{N}$ die Aussage der Form

$$A(n) \Rightarrow A(n+1)$$

gilt.
Um zu zeigen, dass dieses Beweisprinzip gültig ist, nehmen wir an, dass beide Bedingungen erfüllt sind, also dass die Aussage der Form $A(1)$ gilt und dass für jedes $n \in \mathbb{N}$ die Aussage der Form $A(n) \Rightarrow A(n+1)$ gilt. Ferner setzen wir $U := \{n \in \mathbb{N} \mid \text{die Aussage der Form } A(n) \text{ gilt}\}$. Dann ist die Gültigkeit der Aussage der Form $A(1)$ äquivalent zu $1 \in U$. Für alle $n \in U$ gilt ferner die Aussage der Form $A(n)$. Da für jedes $n \in U$ wegen $U \subseteq \mathbb{N}$ die Aussage der Form $A(n) \Rightarrow A(n+1)$ gilt, haben wir auch die Gültigkeit der Aussage der Form $A(n+1)$, d.h. für jedes $n \in U$ ist auch $n+1 \in U$. Nach dem Induktionsprinzip (8.1)(c) impliziert dies bereits $U = \mathbb{N}$, d.h. die Aussage der Form $A(n)$ gilt für alle $n \in \mathbb{N}$. Mit anderen Worten: die Aussage der Form $\forall n \in \mathbb{N} : A(n)$ ist gezeigt.
Wir illustrieren das Induktionsprinzip an einem Beispiel.

(8.2) Anwendungsbeispiel. Für jede ungerade natürliche Zahl m ist $2^m + 1$ ein Vielfaches von 3.

Beweis. Für jedes ungerade $m \in \mathbb{N}$ gibt es (genau) ein $n \in \mathbb{N}$ mit $m = 2n-1$. Wir wollen zeigen, dass $2^{2n-1}+1$ für alle $n \in \mathbb{N}$ ein Vielfaches von 3 ist. Hierzu führen wir Induktion nach n.
Induktionsanfang. Für $n = 1$ ist

$$2^{2n-1} + 1 = 2^{2\cdot 1-1} + 1 = 3 = 1 \cdot 3$$

ein Vielfaches von 3.
Induktionsvoraussetzung. Nun sei $n \in \mathbb{N}$ so gegeben, dass $2^{2n-1} + 1$ ein Vielfaches von 3 ist.
Induktionsschritt. Dann gibt es ein $q \in \mathbb{N}$ mit $2^{2n-1} + 1 = q \cdot 3$. Es folgt $2^{2n-1} = q \cdot 3 - 1$ und somit

$$\begin{aligned} 2^{2(n+1)-1} + 1 &= 2^{2n+2-1} + 1 = 4 \cdot 2^{2n-1} + 1 = 4 \cdot (q \cdot 3 - 1) + 1 = 4q \cdot 3 - 4 + 1 = 4q \cdot 3 - 3 \\ &= (4q - 1) \cdot 3. \end{aligned}$$

Insbesondere ist auch $2^{2(n+1)-1} + 1$ ein Vielfaches von 3.
Nach dem Induktionsprinzip ist $2^{2n-1} + 1$ für alle $n \in \mathbb{N}$ ein Vielfaches von 3. □

Im obigen Beispiel haben wir in der Induktionsvoraussetzung angenommen, dass ein (beliebiges) $n \in \mathbb{N}$ gegeben ist und dass die Aussage für dieses n gilt. Anschließend haben wir im Induktionsschritt gezeigt, dass die Aussage unter dieser Annahme auch für $n+1$ gilt. Äquivalent hätten wir in der Induktionsvoraussetzung natürlich auch annehmen können, dass ein (beliebiges) $n \in \mathbb{N}$ mit $n \geq 2$ gegeben ist und dass die Aussage für $n-1$ gilt, um im Induktionsschritt dann die Aussage für n zu zeigen.

Alternativer Beweis. Wir zeigen erneut durch Induktion nach n, dass $2^{2n-1} + 1$ für alle $n \in \mathbb{N}$ ein Vielfaches von 3 ist.
Induktionsanfang. Für $n = 1$ verfahren wir wie oben.
Induktionsvoraussetzung. Nun sei $n \in \mathbb{N}$ mit $n \geq 2$ so gegeben, dass $2^{2(n-1)-1} + 1$ ein Vielfaches von 3 ist.
Induktionsschritt. Dann gibt es ein $q \in \mathbb{N}$ mit $2^{2(n-1)-1} + 1 = q \cdot 3$. Es folgt $2^{2(n-1)-1} = q \cdot 3 - 1$ und somit

$$\begin{aligned} 2^{2n-1} + 1 &= 2^{2(n-1)+2-1} + 1 = 4 \cdot 2^{2(n-1)-1} + 1 = 4 \cdot (q \cdot 3 - 1) + 1 = 4q \cdot 3 - 4 + 1 = 4q \cdot 3 - 3 \\ &= (4q - 1) \cdot 3. \end{aligned}$$

Insbesondere ist auch $2^{2n-1} + 1$ ein Vielfaches von 3.
Nach dem Induktionsprinzip ist $2^{2n-1} + 1$ für alle $n \in \mathbb{N}$ ein Vielfaches von 3. □

Eine Variante des Induktionsprinzips lässt sich wie folgt formulieren. Um eine Aussage der Form $\forall n \in \mathbb{N} : A(n)$ zu beweisen, können wir die Aussage der Form

$$A(1) \wedge (\forall n \in \mathbb{N} : A(1) \wedge \ldots \wedge A(n) \Rightarrow A(n+1))$$

zeigen, d.h. zum einen die Aussage der Form

$$A(1)$$

und zum anderen für jedes $n \in \mathbb{N}$ die Aussage der Form

$$A(1) \wedge \ldots \wedge A(n) \Rightarrow A(n+1).$$

Um zu zeigen, dass auch diese Variante gültig ist, nehmen wir an, dass beide Bedingungen erfüllt sind, also dass die Aussage der Form $A(1)$ gilt und dass für jedes $n \in \mathbb{N}$ die Aussage der Form $A(1) \wedge \ldots \wedge A(n) \Rightarrow A(n+1)$ gilt. Dann gilt nach Beispiel (1.29) für jedes $n \in \mathbb{N}$ aber auch die Aussage der Form

$$A(1) \wedge \ldots \wedge A(n) \Rightarrow A(1) \wedge \ldots \wedge A(n) \wedge A(n+1),$$

so dass nach dem Induktionsprinzip die Aussage der Form $\forall n \in \mathbb{N} : A(1) \wedge \ldots \wedge A(n)$ gilt. Nach Beispiel (1.28)(a) gilt dann aber insbesondere die Aussage der Form $\forall n \in \mathbb{N} : A(n)$.
Wir wollen auch die Nützlichkeit dieses Induktionsprinzip an Hand eines Beispiels verdeutlichen.

(8.3) Anwendungsbeispiel. Jede natürliche Zahl ist ein Produkt ([1]) von Primzahlen.

[1] Genauer meinen wir hier ein Produkt aus einer endlichen Anzahl an Faktoren, wobei ein Produkt aus null Faktoren per Definition immer gleich 1 ist, vgl. Notation (8.7).

Beweis. Wir wollen zeigen, dass jedes $n \in \mathbb{N}$ ein Produkt aus Primzahlen ist. Hierzu führen wir Induktion nach n.
Induktionsanfang. Es ist $n = 1$ ein Produkt aus 0 Faktoren, vgl. Notation (8.7) unten, also insbesondere ein Produkt aus Primzahlen (bestehend aus null Faktoren).
Induktionsvoraussetzung. Nun sei $n \in \mathbb{N}$ gegeben und es sei angenommen, dass jedes $m \in \mathbb{N}$ mit $m < n$ ein Produkt aus Primzahlen ist.
Induktionsschritt. Wenn n eine Primzahl ist, so ist n insbesondere ein Produkt aus Primzahlen (bestehend aus einem Faktor). Andernfalls ist n zusammengesetzt, d.h. es gibt $l, m \in \mathbb{N}$ mit $l < n$, $m < n$ und $n = lm$. Nach Induktionsvoraussetzung sind l und m Produkte aus Primzahlen. Wegen $n = lm$ ist dann aber auch n ein Produkt aus Primzahlen.
Nach dem Induktionsprinzip ist jedes $n \in \mathbb{N}$ ein Produkt aus Primzahlen. □

Mit Hilfe eines abgewandelten Induktionsprinzips lassen sich auch Aussagen für ganze Zahlen ab einer bestimmten Grenze zeigen – das Beweisprinzip bleibt dasselbe, lediglich der Induktionsanfang bei 1 wird zu einem Induktionsanfang bei irgendeinem gegebenen $n_0 \in \mathbb{Z}$. Präzise formuliert: Um für ein $n_0 \in \mathbb{Z}$ eine Aussage der Form $\forall n \in \mathbb{Z} : n \geq n_0 \Rightarrow A(n)$ zu beweisen, können wir die Aussage der Form

$$A(n_0) \wedge (\forall n \in \mathbb{Z} : n \geq n_0 \Rightarrow (A(n) \Rightarrow A(n+1)))$$

zeigen, d.h. zum einen die Aussage der Form

$$A(n_0)$$

und zum anderen für jedes $n \in \mathbb{Z}$ mit $n \geq n_0$ die Aussage der Form

$$A(n) \Rightarrow A(n+1).$$

Um zu zeigen, dass auch diese Variante gültig ist, nehmen wir an, dass beide Bedingungen erfüllt sind, also dass die Aussage der Form $A(n_0)$ gilt und dass für jedes $n \in \mathbb{Z}$ mit $n \geq n_0$ die Aussage der Form $A(n) \Rightarrow A(n+1)$ gilt. Da $\mathbb{N} \to \{n \in \mathbb{Z} \mid n \geq n_0\}$, $m \mapsto n_0 - 1 + m$ eine wohldefinierte Bijektion ist, gilt dann die Aussage der Form

$$A(n_0 - 1 + 1)$$

sowie für jedes $m \in \mathbb{N}$ die Aussage der Form

$$A(n_0 - 1 + m) \Rightarrow A(n_0 - 1 + m + 1).$$

Nach dem Induktionsprinzip ist dann aber die Gültigkeit der Aussage der Form $\forall m \in \mathbb{N} : A(n_0 - 1 + m)$ nachgewiesen, so dass aus der Bijektion die Gültigkeit der Aussage der Form $\forall n \in \mathbb{Z} : n \geq n_0 \Rightarrow A(n)$ folgt.
Diese Variante des Induktionsprinzips lässt sich zum Beispiel zum Beweis der folgenden Aussage verwenden.

(8.4) Anwendungsbeispiel. Für jedes $n \in \mathbb{N}$ mit $n \geq 4$ gilt $n^2 > 2n + 7$.

Beweis. Wir führen Induktion nach n.
Induktionsanfang. Für $n = 4$ gilt

$$n^2 = 4^2 = 16 > 15 = 2 \cdot 4 + 7 = 2n + 7.$$

Induktionsvoraussetzung. Nun sei $n \in \mathbb{N}$ mit $n \geq 4$ so gegeben, dass $n^2 > 2n + 7$ gilt.
Induktionsschritt. Dann folgt auch

$$(n+1)^2 = n^2 + 2n + 1 > 2n + 7 + 2n + 1 > 2n + 7 + 2 = 2n + 2 + 7 = 2(n+1) + 7.$$

Nach dem Induktionsprinzip gilt $n^2 > 2n + 7$ für alle $n \in \mathbb{N}$ mit $n \geq 4$. □

Rekursion

Auf Grund des Induktionsprinzips lassen sich Folgen, also Familien über $\mathbb{N}$, rekursiv definieren:

(8.5) Proposition (Rekursionssatz)**.** Für jede Menge X, jede Abbildung $t\colon X \to X$ und jedes $a \in X$ gibt es genau eine Folge $x = (x_n)_{n\in\mathbb{N}}$ in X mit $x_1 = a$ und $x_{n+1} = t(x_n)$ für $n \in \mathbb{N}$.

(8.6) Beispiel. Für jedes $a \in \mathbb{R}$ gibt es genau eine Folge $x = (x_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ mit $x_1 = a$ und $x_{n+1} = ax_n$ für $n \in \mathbb{N}$.

Beweis. Es sei $a \in \mathbb{R}$ gegeben und es sei $t\colon \mathbb{R} \to \mathbb{R}$, $y \mapsto ay$. Nach dem Rekursionssatz (8.5) gibt es genau eine Folge $x = (x_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ mit $x_1 = a$ und $x_{n+1} = t(x_n) = ax_n$. □

Produkt- und Summennotation

Mit Hilfe von Rekursion führen wir die Produkt- bzw. Summenschreibweise ein:

(8.7) Notation.

(a) Es sei ein Monoid M gegeben. Für jedes $n \in \mathbb{N}_0$ und alle $x \in M^n$ mit $x_i x_j = x_j x_i$ für $i, j \in [1, n]$ notieren wir rekursiv

$$\prod_{i\in[1,n]} x_i = \begin{cases} 1, & \text{falls } n = 0, \\ (\prod_{i\in[1,n-1]} x_i)\, x_n, & \text{falls } n > 0. \end{cases}$$

(b) Es sei ein abelsches Monoid A gegeben. Für jedes $n \in \mathbb{N}_0$ und alle $x \in A^n$ notieren wir rekursiv

$$\sum_{i\in[1,n]} x_i := \begin{cases} 0, & \text{falls } n = 0, \\ \sum_{i\in[1,n-1]} x_i + x_k, & \text{falls } n > 0. \end{cases}$$

Wie skizzieren einen Beweis für die Wohldefiniertheit des in Notation (8.7)(a) definierten Objekts: Es sei

$$t\colon \dot{\bigcup_{n\in\mathbb{N}_0}} \operatorname{Map}(M^n, M) \to \dot{\bigcup_{n\in\mathbb{N}_0}} \operatorname{Map}(M^n, M)$$

gegeben durch

$$t(f)\colon M^{n+1} \to M,\ x \mapsto f((x_i)_{i\in[1,n]}) \cdot x_{n+1}$$

für $f \in \operatorname{Map}(M^n, M)$, $n \in \mathbb{N}_0$. Nach dem Rekursionssatz (8.5) ([2]) gibt es genau eine durch $\mathbb{N}_0$ indizierte Folge $(p_n)_{n\in\mathbb{N}_0}$ in $\dot{\bigcup}_{n\in\mathbb{N}_0} \operatorname{Map}(M^n, M)$ mit $p_0\colon M^0 \to M$, $x \mapsto 1$ und mit $p_n = t(p_{n-1})$ für $n \in \mathbb{N}_0$. Nach dem Induktionsprinzip ist dann p_n für jedes $n \in \mathbb{N}_0$ eine Abbildung von M^n nach M. Für $n \in \mathbb{N}_0$, $x \in M^n$ mit $x_i x_j = x_j x_i$ für $i, j \in [1, n]$ schreiben wir

$$\prod_{i\in[1,n]} x_i = p_n(x),$$

dann gilt

$$\prod_{i\in[1,n]} x_i = p_n(x) = \left\{ \begin{cases} 1, & \text{falls } n = 0, \\ (t(p_{n-1}))(x), & \text{falls } n > 0 \end{cases} \right\} = \left\{ \begin{cases} 1, & \text{falls } n = 0, \\ p_{n-1}((x_i)_{i\in[1,n-1]}) \cdot x_n, & \text{falls } n > 0 \end{cases} \right\}$$
$$= \begin{cases} 1, & \text{falls } n = 0, \\ (\prod_{i\in[1,n-1]} x_i) \cdot x_n, & \text{falls } n > 0. \end{cases}$$

(8.8) Bemerkung. Es seien ein Monoid M, eine endliche Menge I und ein $x \in M^I$ so gegeben, dass $x_i x_j = x_j x_i$ für $i, j \in I$ gilt. Für Abzählungen $e, e'\colon [1, |I|] \to I$ gilt

$$\prod_{k\in[1,|I|]} x_{e(k)} = \prod_{k\in[1,|I|]} x_{e'(k)}.$$

Beweisidee. Dies folgt aus der Assoziativität von M. □

Die vorangegangene Bemerkung erlaubt uns, die Produkt- und Summenschreibweise auf beliebige endliche Indexmengen zu verallgemeinern:

(8.9) Notation. Es sei eine endliche Menge I gegeben. Wir wählen eine Abzählung $e\colon [1, |I|] \to I$.

(a) Es seien ein Monoid M und ein $x \in M^I$ so gegeben, dass $x_i x_j = x_j x_i$ für $i, j \in I$ gilt. Wir setzen

$$\prod_{i\in I} x_i := \prod_{k\in[1,|I|]} x_{e(k)}.$$

[2] Genau genommen benutzen wir eine Variante für $\mathbb{N}_0$ statt $\mathbb{N}$.

(b) Es seien ein abelsches Monoid A und ein $x \in A^I$ gegeben. Wir setzen

$$\sum_{i \in I} x_i := \sum_{k \in [1,|I|]} x_{e(k)}.$$

(8.10) Notation. Es seien ein Monoid M und eine Menge I gegeben. Wir setzen

$$M^{(I)} := \{x \in M^I \mid \{i \in I \mid x_i \neq 1\} \text{ ist endlich}\}.$$

(8.11) Notation. Es sei eine Menge I gegeben.

(a) Es seien ein Monoid M und ein $x \in M^{(I)}$ so gegeben, dass $x_i x_j = x_j x_i$ für $i, j \in I$ gilt. Wir setzen

$$\prod_{i \in I} x_i := \prod_{\substack{i \in I \\ x_i \neq 1}} x_i := \prod_{i \in \{j \in I \mid x_j \neq 1\}} x_i.$$

(b) Es seien ein abelsches Monoid A und ein $x \in A^{(I)}$ gegeben. Wir setzen

$$\sum_{i \in I} x_i := \sum_{\substack{i \in I \\ x_i \neq 0}} x_i := \sum_{i \in \{j \in I \mid x_j \neq 0\}} x_i.$$

Wir kommen zum Spezialfall, bei welchem alle indizierten Elemente gleich sind:

(8.12) Notation.

(a) Es seien ein Monoid M und $x \in M$ gegeben. Für $k \in \mathbb{N}_0$ setzen wir

$$x^k := \prod_{i \in [1,k]} x.$$

Wenn x invertierbar in M ist, so setzen wir

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

für $k \in \mathbb{N}$.

(b) Es seien ein abelsches Monoid A und $x \in A$ gegeben. Für $k \in \mathbb{N}_0$ setzen wir

$$kx = k \cdot x := \sum_{i \in [1,k]} x.$$

Wenn x negierbar in A ist, so setzen wir

$$(-k)x := k(-x)$$

für $k \in \mathbb{N}$.

(8.13) Proposition (Potenzgesetze)**.** Es sei ein Monoid M gegeben.

(a) Für $x \in M$, $k, l \in \mathbb{N}_0$ gilt

$$x^k x^l = x^{k+l}.$$

Für $x \in M^\times$, $k, l \in \mathbb{Z}$ gilt

$$x^k x^l = x^{k+l}.$$

(b) Für $x \in M$, $k, l \in \mathbb{N}_0$ gilt

$$(x^k)^l = x^{kl}.$$

Für $x \in M^\times$, $k, l \in \mathbb{Z}$ gilt

$$(x^k)^l = x^{kl}.$$

(c) Es sei M kommutativ. Für $x, y \in M$, $k \in \mathbb{N}_0$ gilt

$$x^k y^k = (xy)^k.$$

Für $x, y \in M^\times$, $k \in \mathbb{Z}$ gilt

$$x^k y^k = (xy)^k.$$

Beweis.

(a) Es seien $x \in M$, $k \in \mathbb{N}_0$ gegeben. Um $x^k x^l = x^{k+l}$ für alle $l \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach l. Für $l = 0$ gilt

$$x^k x^l = x^k x^0 = x^k \cdot 1 = x^k = x^{k+0}.$$

Es sei also $l > 0$ und gelte $x^k x^{l-1} = x^{k+l-1}$. Dann ist auch $k + l \geq l > 0$ und somit

$$x^k x^l = x^k (x^{l-1} x) = (x^k x^{l-1}) x = x^{k+l-1} x = x^{k+l}.$$

Nach dem Induktionsprinzip haben wir $x^k x^l = x^{k+l}$ für alle $l \in \mathbb{N}_0$.

Um $x^k x^l = x^{k+l}$ für alle $x \in M^\times$, $k, l \in \mathbb{Z}$ zu zeigen, unterscheiden wir drei Fälle. Zuerst verifizieren wir die Gleichung für den Spezialfall $x \in M^\times$, $k \in \mathbb{Z}$, $l = 1$, danach für $x \in M^\times$, $k \in \mathbb{Z}$, $l \geq 0$ mittels Induktion nach l, und schließlich für $x \in M^\times$, $k \in \mathbb{Z}$, $l < 0$.

Zum ersten Fall. Es seien $x \in M^\times$, $k \in \mathbb{Z}$, $l = 1$. Für $k \geq 0$ ist $k+1 > 0$ und damit $x^{k+1} = x^{(k+1)-1} x = x^k x$ nach Definition. Für $k < 0$ gilt aber $-k > 0$ und damit ebenfalls

$$\begin{aligned} x^k x^1 &= (x^{-1})^{-k} x = ((x^{-1})^{-k-1} x^{-1}) x = (x^{-1})^{-k-1} (x^{-1} x) = (x^{-1})^{-(k+1)} \cdot 1 = (x^{-1})^{-(k+1)} \\ &= \left.\begin{cases} (x^{-1})^0, & \text{falls } k = -1, \\ x^{-(-(k+1))}, & \text{falls } k < -1 \end{cases}\right\} = \left\{\begin{cases} 1, & \text{falls } k = -1, \\ x^{k+1}, & \text{falls } k < -1 \end{cases}\right\} = x^{k+1}. \end{aligned}$$

Zum zweiten Fall. Es seien $x \in M^\times$, $k \in \mathbb{Z}$. Um $x^k x^l = x^{k+l}$ für $l \in \mathbb{Z}$, $l \geq 0$ zu zeigen, führen wir Induktion nach l (wobei dies völlig analog zum Beweis für $x \in M$, $k, l \in \mathbb{N}_0$ geht): Für $l = 0$ gilt

$$x^k x^l = x^k x^0 = x^k \cdot 1 = x^k = x^{k+0}.$$

Es seien also $l > 0$ und es gelte $x^k x^{l-1} = x^{k+l-1}$. Unter Benutzung des ersten Falls erhalten wir dann auch

$$x^k x^l = x^k (x^{l-1} x) = (x^k x^{l-1}) x = x^{k+l-1} x = x^{k+l}.$$

Nach dem Induktionsprinzip haben wir $x^k x^l = x^{k+l}$ für alle $l \geq 0$.

Zum dritten Fall. Schließlich seien $x \in M^\times$, $k, l \in \mathbb{Z}$, $l < 0$. Dann ist $-l > 0$, also

$$x^{k+l} x^{-l} = x^{k+l+(-l)} = x^k$$

nach dem zweiten Fall und damit $x^{k+l} = x^k (x^{-l})^{-1}$. Nun haben wir aber

$$x^{-l} x^l = ((x^{-1})^{-1})^{-l} (x^{-1})^{-l} = (x^{-1})^{-(-l)} (x^{-1})^{-l} = (x^{-1})^l (x^{-1})^{-l} = (x^{-1})^{l+(-l)} = (x^{-1})^0 = 1$$

unter Benutzung des zweiten Falls, also $(x^{-l})^{-1} = x^l$ nach Bemerkung (6.15) und damit auch in diesem Fall

$$x^k x^l = x^k (x^{-l})^{-1} = x^{k+l}.$$

(b) Es seien $x \in M$, $k \in \mathbb{N}_0$ gegeben. Um $(x^k)^l = x^{kl}$ für alle $l \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach l. Für $l = 0$ gilt

$$(x^k)^0 = 1 = x^0 = x^{k \cdot 0}.$$

Es sei also $l > 0$ und gelte $(x^k)^{l-1} = x^{k(l-1)}$. Mit (a) folgt

$$(x^k)^l = (x^k)^{l-1}x^k = x^{k(l-1)}x^k = x^{k(l-1)+k} = x^{kl}$$

Nach dem Induktionsprinzip haben wir $(x^k)^l = x^{kl}$ für alle $l \in \mathbb{N}_0$.

Um $(x^k)^l = x^{kl}$ für alle $x \in M^\times$, $k, l \in \mathbb{Z}$, unterscheiden wir drei Fälle. Zuerst verifizieren wir die Gleichung für $k \geq 0$, $l \geq 0$, danach für $k < 0$, $l \geq 0$, und schließlich für $k \in \mathbb{Z}$, $l < 0$.

Zum ersten Fall. Wir haben bereits bewiesen, dass $(x^k)^l = x^{kl}$ für alle $x \in M$, $k, l \in \mathbb{N}_0$ gilt, also insbesondere für $x \in M^\times$, $k, l \in \mathbb{Z}$, $k \geq 0$, $l \geq 0$.

Zum zweiten Fall. Es seien $x \in M^\times$, $k, l \in \mathbb{Z}$, $k < 0$, $l \geq 0$. Dann ist $-k > 0$ und $-kl > 0$, also

$$(x^k)^l = ((x^{-1})^{-k})^l = (x^{-1})^{(-k)l} = (x^{-1})^{-kl} = x^{kl}$$

nach dem ersten Fall.

Zum dritten Fall. Es seien $x \in M^\times$, $k, l \in \mathbb{Z}$, $k \in \mathbb{Z}$, $l < 0$. Dann ist $-l > 0$, also

$$(x^k)^{-l} = x^{k(-l)}$$

nach dem ersten oder zweiten Fall. Nun ist aber $(x^k)^l\,(x^k)^{-l} = (x^k)^0 = 1$ und $x^{k(-l)}x^{kl} = x^0 = 1$ nach (a), also $((x^k)^{-l})^{-1} = (x^k)^l$ und $(x^{k(-l)})^{-1} = x^{kl}$ nach Bemerkung (6.15). Wir erhalten also auch in diesem Fall

$$(x^k)^l = ((x^k)^{-l})^{-1} = (x^{k(-l)})^{-1} = x^{kl}.$$

(c) Es seien $x, y \in M$ gegeben. Um $x^k y^k = (xy)^k$ für alle $k \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach k. Für $k = 0$ gilt

$$x^k y^k = x^0 y^0 = 1 \cdot 1 = 1 = (xy)^0.$$

Es sei also $k > 0$ und gelte $x^{k-1}y^{k-1} = (xy)^{k-1}$. Dann ist auch

$$x^k y^k = (x^{k-1}x)(y^{k-1}y) = (x^{k-1}y^{k-1})(xy) = (xy)^{k-1}\,(xy) = (xy)^k.$$

Nach dem Induktionsprinzip haben wir $x^k y^k = (xy)^k$ für alle $k \in \mathbb{N}_0$.

Nun seien $x, y \in M^\times$, $k \in \mathbb{Z}$, $k < 0$. Dann ist $-k > 0$, also

$$x^k y^k = (x^{-1})^{-k}(y^{-1})^{-k} = (x^{-1}y^{-1})^{-k} = (y^{-1}x^{-1})^{-k} = ((xy)^{-1})^{-k} = (xy)^k$$

nach Proposition (6.30)(a). □

Jeder Ring R hat eine unterliegende abelsche Gruppe. Folglich haben wir für jedes $x \in R$, $k \in \mathbb{Z}$ den Ausdruck $kx = k \cdot x \in R$ definiert, vgl. Notation (8.12)(b).

(8.14) Notation. Es sei ein Ring R gegeben. Für $k \in \mathbb{Z}$ schreiben wir auch

$$k = k^R := k \cdot 1^R.$$

Wir betonen, dass die vorangegangene Vereinbarung konform mit unserer Notation für das Nullelement und das Einselement in einem Ring R ist. Sie besagt unter anderem, dass wir $2^R = 2 \cdot 1^R = 1^R + 1^R$, $3^R = 3 \cdot 1^R = 2 \cdot 1^R + 1^R = 2^R + 1^R$, etc., setzen.
Hin und wieder werden wir außerdem folgende Schreibweise antreffen:

(8.15) Notation (Kronecker-Delta)**.** Es seien ein Ring R, eine Menge I und $i, j \in I$ gegeben. Das *Kronecker-Delta* ist definiert als

$$\delta_{i,j} := \begin{cases} 1^R & \text{falls } i = j, \\ 0^R & \text{falls } i \neq j. \end{cases}$$

Rekursionsgleichungen

(8.16) Beispiel. Es sei $f \in \mathbb{R}^{\mathbb{N}_0}$ gegeben durch

$$f_k = \begin{cases} 0, & \text{für } k = 0, \\ 1, & \text{für } k = 1, \\ f_{k-2} + f_{k-1}, & \text{für } k \in \mathbb{N}_0 \text{ mit } k \geq 2. \end{cases}$$

Dann gilt

$$f_k = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^k - (\frac{1-\sqrt{5}}{2})^k)$$

für $k \in \mathbb{N}_0$.

Beweis. Wir führen Induktion nach k. Für $k = 0$ gilt

$$f_k = f_0 = 0 = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^0 - (\frac{1-\sqrt{5}}{2})^0).$$

Für $k = 1$ gilt

$$f_k = f_1 = 1 = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^1 - (\frac{1-\sqrt{5}}{2})^1).$$

Für $k \in \mathbb{N}_0$ mit $k \geq 2$ und $f_{k-2} = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-2} - (\frac{1-\sqrt{5}}{2})^{k-2})$ und $f_{k-1} = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-1})$ gilt auch

$$\begin{aligned}
f_k = f_{k-2} + f_{k-1} &= \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-2} - (\frac{1-\sqrt{5}}{2})^{k-2}) + \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-1}) \\
&= \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-2} - (\frac{1-\sqrt{5}}{2})^{k-2} + (\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-1}) \\
&= \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{k-2} + (\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-2} - (\frac{1-\sqrt{5}}{2})^{k-1}) \\
&= \frac{1}{\sqrt{5}}(\frac{2^2(1+\sqrt{5})^{k-2} + 2(1+\sqrt{5})^{k-1}}{2^k} - \frac{2^2(1-\sqrt{5})^{k-2} + 2(1-\sqrt{5})^{k-1}}{2^k}) \\
&= \frac{1}{\sqrt{5}}(\frac{(4+2(1+\sqrt{5}))(1+\sqrt{5})^{k-2}}{2^k} - \frac{(4+2(1-\sqrt{5}))(1-\sqrt{5})^{k-2}}{2^k}) \\
&= \frac{1}{\sqrt{5}}(\frac{(4+2+2\sqrt{5})(1+\sqrt{5})^{k-2}}{2^k} - \frac{(4+2-2\sqrt{5})(1-\sqrt{5})^{k-2}}{2^k}) \\
&= \frac{1}{\sqrt{5}}(\frac{(1+2\sqrt{5}+(\sqrt{5})^2)(1+\sqrt{5})^{k-2}}{2^k} - \frac{(1-2\sqrt{5}+(\sqrt{5})^2)(1-\sqrt{5})^{k-2}}{2^k}) \\
&= \frac{1}{\sqrt{5}}(\frac{(1+\sqrt{5})^2\,(1+\sqrt{5})^{k-2}}{2^k} - \frac{(1-\sqrt{5})^2\,(1-\sqrt{5})^{k-2}}{2^k}) = \frac{1}{\sqrt{5}}(\frac{(1+\sqrt{5})^k}{2^k} - \frac{(1-\sqrt{5})^k}{2^k}).
\end{aligned}$$

Nach dem Induktionsprinzip gilt $f_k = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^k - (\frac{1-\sqrt{5}}{2})^k)$ für alle $k \in \mathbb{N}_0$. □

(8.17) Beispiel. Es seien ein Monoid M, $a \in M$ und $x \in M^{\mathbb{N}_0}$ mit

$$x_{k+1} = ax_k$$

für $k \in \mathbb{N}_0$ gegeben. Dann ist

$$x_k = a^k x_0$$

für $k \in \mathbb{N}_0$.

Beweis. Wir führen Induktion nach k. Für $k = 0$ gilt

$$x_0 = 1x_0 = a^0 x_0.$$

Für $k \in \mathbb{N}_0$ mit $x_k = a^k x_0$ gilt auch

$$x_{k+1} = ax_k = aa^k x_0 = a^{k+1} x_0.$$

Nach dem Induktionsprinzip gilt also in der Tat $x_k = a^k x_0$ für alle $k \in \mathbb{N}_0$. □

(8.18) Beispiel. Es seien ein Monoid M, $a \in M^{\mathbb{N}}$ und $x \in M^{\mathbb{N}_0}$ mit

$$x_{k+1} = a_{k+1} x_k$$

für $k \in \mathbb{N}_0$ gegeben. Dann ist

$$x_k = (\prod_{i \in [1,k]} a_i) x_0$$

für $k \in \mathbb{N}_0$.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(8.19) Beispiel. Es sei $x \in \mathbb{R}^{\mathbb{N}_0}$ mit

$$x_{k+1} = x_k + k + 1$$

für $k \in \mathbb{N}_0$ gegeben. Dann ist

$$x_k = \frac{(k+1)k}{2} + x_0$$

für $k \in \mathbb{N}_0$.

(8.20) Beispiel. Es sei $x \in \mathbb{R}^{\mathbb{N}_0}$ mit

$$x_{k+1} = 2x_k + 2^{k+1}$$

für $k \in \mathbb{N}_0$ gegeben. Dann ist

$$x_k = 2^k(k + x_0)$$

für $k \in \mathbb{N}_0$.

Beweis. Für $k = 0$ gilt

$$x_0 = 2^0 \cdot (0 + x_0) = 2^k(k + x_0).$$

Für $k \in \mathbb{N}_0$ mit $x_k = 2^k(k + x_0)$ gilt auch

$$\begin{aligned} x_{k+1} &= 2x_k + 2^{k+1} = 2 \cdot 2^k(k + x_0) + 2^{k+1} = 2^{k+1}(k + x_0) + 2^{k+1} = 2^{k+1}(k + x_0 + 1) \\ &= 2^{k+1}(k + 1 + x_0). \end{aligned}$$

Nach dem Induktionsprinzip gilt $x_k = 2^k(k + x_0)$ für alle $k \in \mathbb{N}_0$. □

(8.21) Beispiel. Es sei $x \in \mathbb{R}^{\mathbb{N}_0}$ mit

$$x_k = 2x_{\lfloor \frac{k}{2} \rfloor} + k$$

für $k \in \mathbb{N}$ gegeben. Dann ist

$$x_k = \sum_{i \in [0, \lfloor \log_2(k) \rfloor]} \lfloor \frac{k}{2^i} \rfloor \, 2^i + 2^{\lfloor \log_2(k) \rfloor + 1} x_0$$

für $k \in \mathbb{N}$.

Beweis. Für $k = 1$ gilt

$$\sum_{i\in[0,\lfloor\log_2(k)\rfloor]} \lfloor\frac{k}{2^i}\rfloor\, 2^i + 2^{\lfloor\log_2(k)\rfloor+1}x_0 = \sum_{i\in[0,\lfloor\log_2(1)\rfloor]} \lfloor\frac{1}{2^i}\rfloor\, 2^i + 2^{\lfloor\log_2(1)\rfloor+1}x_0 = \sum_{i\in[0,0]} \lfloor\frac{1}{2^i}\rfloor\, 2^i + 2^{0+1}x_0$$
$$= 1 + 2x_0,$$

also

$$x_k = x_1 = 2x_0 + 1 = \sum_{i\in[0,\lfloor\log_2(k)\rfloor]} \lfloor\frac{k}{2^i}\rfloor\, 2^i + 2^{\lfloor\log_2(k)\rfloor+1}x_0.$$

Für $k \in \mathbb{N}$ mit $k > 1$ gilt

$$\begin{aligned} x_k &= 2x_{\lfloor\frac{k}{2}\rfloor} + k = 2\Big(\sum_{i\in[0,\lfloor\log_2(k)\rfloor]} \lfloor\frac{\lfloor\frac{k}{2}\rfloor}{2^i}\rfloor\, 2^i + 2^{\lfloor\log_2(\lfloor\frac{k}{2}\rfloor)\rfloor+1}x_0\Big) + k \\ &= 2\Big(\sum_{i\in[0,\lfloor\log_2(k)\rfloor]} \lfloor\frac{k}{2^{i+1}}\rfloor\, 2^i + 2^{\lfloor\log_2(\frac{k}{2})\rfloor+1}x_0\Big) + k = \sum_{i\in[0,\lfloor\log_2(k)\rfloor]} \lfloor\frac{k}{2^{i+1}}\rfloor\, 2^{i+1} + 2^{\lfloor\log_2(k)-1\rfloor+1+1}x_0 + k \\ &= k + \sum_{i\in[1,\lfloor\log_2(k)\rfloor+1]} \lfloor\frac{k}{2^i}\rfloor\, 2^i + 2^{\lfloor\log_2(k)\rfloor+1}x_0 = \sum_{i\in[0,\lfloor\log_2(k)\rfloor]} \lfloor\frac{k}{2^i}\rfloor\, 2^i + 2^{\lfloor\log_2(k)\rfloor+1}x_0. \end{aligned}$$

Nach dem Induktionsprinzip gilt $x_k = \sum_{i\in[0,\lfloor\log_2(k)\rfloor]} \lfloor\frac{k}{2^i}\rfloor\, 2^i + 2^{\lfloor\log_2(k)\rfloor+1}x_0$ für alle $k \in \mathbb{N}$. □

(8.22) Beispiel. Es sei $x \in \mathbb{R}^{\mathbb{N}_0}$ mit

$$x_k = 2x_{\lfloor\frac{k}{2}\rfloor} + k$$

für $k \in \mathbb{N}$ gegeben. Dann ist

$$x_{2^l} = 2^l(l + 2x_0 + 1)$$

für $l \in \mathbb{N}_0$. Mit anderen Worten: Für $k \in 2^{\mathbb{N}_0}$ gilt

$$x_k = k(\log_2(k) + 2x_0 + 1).$$

Beweis. Für $k \in \mathbb{N}$ gilt $x_k = 2x_{\lfloor\frac{k}{2}\rfloor} + k$, also insbesondere

$$x_{2k} = 2x_{\lfloor\frac{2k}{2}\rfloor} + 2k = 2x_k + 2k.$$

Für $l \in \mathbb{N}_0$ folgt

$$x_{2^{l+1}} = x_{2\cdot 2^l} = 2x_{2^l} + 2 \cdot 2^l = 2x_{2^l} + 2^{l+1},$$

und damit

$$x_{2^l} = 2^l(l + x_{2^0}) = 2^l(l + x_1) = 2^l(l + 2x_0 + 1)$$

nach Beispiel (8.20). □

Mache Wertetabelle:

(8.23) Definition (ungefähr gleich schnelles asymptotisches Wachstum)**.** Es seien $x, y \in \mathbb{R}_{\geq 0}^{\mathbb{N}_0}$ gegeben. Wir sagen, dass x *ungefähr so schnell* wie y *wächst*, wenn es $c, d \in \mathbb{R}_{>0}$ und ein $k_0 \in \mathbb{N}_0$ derart gibt, dass für $k \in \mathbb{N}_0$ mit $k \geq k_0$ stets

$$cy_k \leq x_k \leq dy_k$$

gilt.

(8.24) Beispiel. Es seien $x, y \in \mathbb{R}_{\geq 0}^{\mathbb{N}_0}$ mit

$$x_k = 2x_{\lfloor \frac{k}{2} \rfloor} + k,$$
$$y_k = k \log_2(k)$$

für $k \in \mathbb{N}$ gegeben. Dann wächst x ungefähr so schnell wie y.

Beweis. Zunächst zeigen wir durch Induktion nach k, dass für $k \in \mathbb{N}_0$ mit $k \geq 2$ stets $x_k \leq 2(x_0 + 1)y_k$ gilt. Für $k = 2$ gilt

$$\begin{aligned} x_k = x_2 &= 2x_1 + 2 = 2(2x_0 + 1) + 2 = 4x_0 + 4 = 2(x_0 + 1) \cdot 2 = 2(x_0 + 1) \cdot 2\log_2(2) = 2(x_0 + 1)y_2 \\ &= 2(x_0 + 1)y_k. \end{aligned}$$

Für $k = 3$ gilt

$$\begin{aligned} x_k = x_3 &= 2x_1 + 3 = 2(2x_0 + 1) + 3 = 4x_0 + 5 \leq 6x_0 + 6 = 2(x_0 + 1) \cdot 3 \leq 2(x_0 + 1) \cdot 3\log_2(3) \\ &= 2(x_0 + 1)y_3 = 2(x_0 + 1)y_k. \end{aligned}$$

Für $k \in \mathbb{N}_0$ mit $k \geq 4$ gilt

$$\begin{aligned} x_k &= 2x_{\lfloor \frac{k}{2} \rfloor} + k \leq 2 \cdot 2(x_0 + 1)y_{\lfloor \frac{k}{2} \rfloor} + k = 4(x_0 + 1)\lfloor \frac{k}{2} \rfloor \log_2(\lfloor \frac{k}{2} \rfloor) + k \leq 4(x_0 + 1)\frac{k}{2}\log_2(\frac{k}{2}) + k \\ &= 2(x_0 + 1)k(\log_2(k) - 1) + k = 2(x_0 + 1)k\log_2(k) - 2(x_0 + 1)k + k = 2(x_0 + 1)y_k - (2x_0 + 1)k \\ &\leq 2(x_0 + 1)y_k. \end{aligned}$$

Nach dem Induktionsprinzip gilt $x_k \leq 2(x_0 + 1)y_k$ für alle $k \in \mathbb{N}_0$ mit $k \geq 2$. □

Sebastian Thomas

RWTH Aachen, WS 2016/17
23.11.2016–24.11.2016

Diskrete Strukturen

Vorlesungen 10 und 11

9 Der Polynomring

In diesem Abschnitt führen wir Polynome mit Koeffizienten in einem Körper ein. Da sich Polynome addieren und multiplizieren lassen, erhalten wir so für jeden Körper einen kommutativen Ring.
Im Folgenden, bis zum Ende des Abschnitts und mit Ausnahme einiger Beispiele, sei stets ein Körper K gegeben.

Begriffsbildung

Wir beginnen mit der Einführung von Polynomen, wobei wir auf eine Rückführung auf bekannte Konzepte verzichten. Ein Polynom in X soll ein Ausdruck der Form $\sum_{i\in[0,n]} a_i X^i = a_0 + a_1 X + \ldots + a_n X^n$ für ein beliebiges $n \in \mathbb{N}_0$ sein. Führen wir triviale Summanden mit, so können alle Polynome gleich behandelt werden, unabhängig von der Anzahl ihrer jeweiligen nicht-trivialen Summanden. Hierzu betrachten wir im Folgenden die Menge

$$\begin{aligned} K^{(\mathbb{N}_0)} &= \{a \in K^{\mathbb{N}_0} \mid \{i \in \mathbb{N}_0 \mid a_i \neq 0\} \text{ ist endlich}\} \\ &= \{a \in K^{\mathbb{N}_0} \mid \text{es gibt ein } n \in \mathbb{N}_0 \text{ mit } a_i = 0 \text{ für alle } i > n\}. \end{aligned}$$

(9.1) Vorstellung (Polynomring)**.**

(a) Es sei $a \in K^{(\mathbb{N}_0)}$ gegeben. Wir nennen

$$f = \sum_{i\in\mathbb{N}_0} a_i X^i$$

ein *Polynom* in X über K. Die Familie a wird *Koeffizientenfolge*. Für $i \in I$ wird a_i der *Koeffizient* von f an der Stelle i genannt.

(b) Polynome $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ und $g = \sum_{i\in\mathbb{N}_0} b_i X^i$, wobei $a, b \in K^{(\mathbb{N}_0)}$, sind *gleich*, geschrieben $f = g$, falls $a = b$ gilt.

(c) Das Polynom $X = \sum_{i\in\mathbb{N}_0} \delta_{1,i} X^i$ wird *Unbestimmte* genannt.

(d) Der kommutative Ring gegeben durch die Menge der Polynome

$$K[X] := \{\sum_{i\in\mathbb{N}_0} a_i X^i \mid a \in K^{(\mathbb{N}_0)}\}$$

in X über K mit Addition und Multiplikation gegeben durch

$$\begin{aligned} \sum_{i\in\mathbb{N}_0} a_i X^i + \sum_{i\in\mathbb{N}_0} b_i X^i &= \sum_{i\in\mathbb{N}_0} (a_i + b_i) X^i, \\ (\sum_{i\in\mathbb{N}_0} a_i X^i)(\sum_{j\in\mathbb{N}_0} b_j X^j) &= \sum_{k\in\mathbb{N}_0} (\sum_{\substack{i,j\in\mathbb{N}_0 \\ i+j=k}} a_i b_j) X^k \end{aligned}$$

für $a, b \in K^{(\mathbb{N}_0)}$ wird *Polynomring* in X über K genannt.

(e) Wir identifizieren K mit der Teilmenge $\{aX^0 \mid a \in K\}$ von $K[X]$. Das heißt, unter Missbrauch der Notation notieren wir aX^0 für $a \in K$ auch durch a.

Für $a, b \in K^{(\mathbb{N}_0)}$ sind die Polynome $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ und $g = \sum_{i\in\mathbb{N}_0} b_i X^i$ in X über K genau dann gleich, wenn $a = b$ gilt, d.h. wenn $a_i = b_i$ für alle $i \in \mathbb{N}_0$ gilt.

(9.2) Beispiel. Es seien $f, g \in \mathbb{Q}[X]$ gegeben durch $f = X^2 - 1$ und $g = -X^3 + 2X^2 + X + 1$. Dann ist

$$\begin{aligned} f + g &= -X^3 + 3X^2 + X, \\ fg &= -X^5 + 2X^4 + 2X^3 - X^2 - X - 1, \\ -2f &= -2X^2 + 2. \end{aligned}$$

Polynomfunktionen

Die wesentliche Eigenschaft eines Polynoms $f \in K[X]$ ist die Möglichkeit, Elemente von K in f „einzusetzen". Hierdurch können wir Polynome als Funktionen auffassen.

(9.3) Definition (Polynomfunktion)**.** Es seien $f \in K[X]$ und $a \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ gegeben. Die Abbildung

$$K \to K,\ x \mapsto \sum_{i\in\mathbb{N}_0} a_i x^i$$

heißt *Polynomfunktion* zu f und wird unter Missbrauch der Notation wieder als f notiert.

(9.4) Beispiel. Es sei $f \in \mathbb{Q}[X]$ gegeben durch $f = X^2 - 1$. Dann ist $f(5) = 24$.

Beweis. Es gilt $f(5) = 5^2 - 1 = 24$. □

Wir betonen, dass Polynome keine Funktionen *sind*, sondern nur zugehörige Polynomfunktionen *liefern*. So gibt es etwa über dem Körper $\mathbb{F}_2$ unendlich viele Polynome, aber lediglich vier Polynomfunktionen (alle vier Funktionen von $\mathbb{F}_2$ nach $\mathbb{F}_2$ sind Polynomfunktionen).

Grad eines Polynoms

Es seien $f \in K[X]\setminus\{0\}$ und $a \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ gegeben. Wegen $f \neq 0$ ist $a \neq 0$ und wegen $a \in K^{(\mathbb{N}_0)}$ gibt es ein $n \in \mathbb{N}_0$ mit $a_n \neq 0$ und $a_i = 0$ für $i > n$. Somit ist

$$f = \sum_{i\in[0,n]} a_i X^i.$$

Wir wollen nun etwas Terminologie für diese endliche Darstellung eines Polynoms festlegen.

(9.5) Definition (Grad, Leitkoeffizient, normiertes Polynom)**.** Es seien $f \in K[X] \setminus \{0\}$ und $a \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ gegeben.

(a) Der *Grad* von f ist definiert als

$$\deg f := \max\{i \in \mathbb{N}_0 \mid a_i \neq 0\}.$$

(b) Der Koeffizient $\mathrm{lc}(f) := a_{\deg f}$ von f heißt *Leitkoeffizient* von f.

(c) Wir sagen, dass f ein *normiertes* Polynom ist, falls $\mathrm{lc}(f) = 1$ ist.

Wir betonen, dass das Nullpolynom keinen Grad hat.

(9.6) Beispiel.

(a) Das Polynom $X^2 - 1$ über $\mathbb{Q}$ hat den Grad 2 und den Leitkoeffizienten 1 und ist daher normiert.

(b) Das Polynom $-X^3 + 2X^2 + X + 1$ über $\mathbb{Q}$ hat den Grad 3 und den Leitkoeffizienten -1 und ist daher nicht normiert.

(9.7) Bemerkung. Es seien $f, g \in K[X] \setminus \{0\}$ gegeben.

(a) Wenn $f + g \neq 0$ ist, gilt

$$\deg(f+g) \leq \max(\deg f, \deg g).$$

Wenn $\deg f \neq \deg g$ ist, gilt

$$\deg(f+g) = \max(\deg f, \deg g).$$

(b) Es gilt $fg \neq 0$ und

$$\deg(fg) = \deg f + \deg g.$$

Beweis. Es seien $a, b \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ und $g = \sum_{i\in\mathbb{N}_0} b_i X^i$ gegeben.

(a) Es ist $f + g = \sum_{i\in\mathbb{N}_0}(a_i + b_i)X^i$. Für $i \in \mathbb{N}_0$ mit $a_i + b_i \neq 0$ gilt auch $a_i \neq 0$. Folglich ist

$$\deg(f+g) = \max\{i \in \mathbb{N}_0 \mid a_i + b_i \neq 0\} \leq \max\{i \in \mathbb{N}_0 \mid a_i \neq 0\} = \deg f.$$

Analog lässt sich $\deg(f+g) \leq \deg g$ zeigen.

Nun gelte $\deg f \neq \deg g$. Wir nehmen o.B.d.A. an, dass $\deg f < \deg g$ ist. Für $i \in \mathbb{N}_0$ mit $i \geq \deg g$ gilt dann $a_i = 0$ und damit

$$a_i + b_i = \begin{cases} b_{\deg g}, & \text{falls } i = \deg g, \\ 0, & \text{falls } i > \deg g. \end{cases}$$

Folglich ist $\deg(f+g) = \deg g = \max(\deg f, \deg g)$.

(b) Es ist $fg = \sum_{k\in\mathbb{N}_0}(\sum_{\substack{i,j\in\mathbb{N}_0 \\ i+j=k}} a_i b_j)X^k$. Für $k \in \mathbb{N}_0$ mit $k \geq \deg f + \deg g$ gilt dann

$$\sum_{\substack{i,j\in\mathbb{N}_0 \\ i+j=k}} a_i b_j = \begin{cases} a_{\deg f} b_{\deg g}, & \text{falls } k = \deg f + \deg g, \\ 0, & \text{falls } i > \deg f + \deg g. \end{cases}$$

Folglich ist $fg \neq 0$ und $\deg(fg) = \deg f + \deg g$. □

(9.8) Korollar. Es ist

$$K[X]^\times = K^\times.$$

Beweis. Für $f \in K[X]^\times$ gilt

$$\deg f + \deg f^{-1} = \deg(ff^{-1}) = \deg 1 = 0,$$

also $\deg f = \deg f^{-1} = 0$ und damit $f, f^{-1} \in K^\times$. Folglich ist $K[X]^\times \subseteq K^\times$. Da jedes in K invertierbare Element insbesondere in $K[X]$ invertierbar ist, gilt umgekehrt auch $K^\times \subseteq K[X]^\times$. Insgesamt ist also $K[X]^\times = K^\times$. □

(9.9) Korollar. Der Polynomring $K[X]$ ist ein Integritätsbereich.

Beweis. Dies gilt nach Bemerkung (9.7)(b). □

Manchmal betrachten wir nur Polynome bis zum einem gegebenen Grad n. Wir legen eine Schreibweise fest:

(9.10) Notation. Für $n \in \mathbb{N}_0$ setzen wir

$$K[X]_{<n} := \{f \in K[X] \mid f = 0 \text{ oder } \deg f < n\}.$$

(9.11) Bemerkung. Für $n \in \mathbb{N}_0$ ist

$$K[X]_{<n} = \{\sum_{i\in[0,n-1]} a_i X^i \mid a \in K^{[0,n-1]}\}.$$

Insbesondere gilt $K[X]_{<0} = \{0\}$ und $K[X]_{<1} = K$.

(9.12) Definition (konstantes Polynom, lineares Polynom)**.** Es sei $f \in K[X]$ gegeben.

(a) Wir nennen f ein *konstantes* Polynom, falls $f = 0$ oder $\deg f = 0$ ist.

(b) Wir nennen f ein *lineares* Polynom, falls $\deg f = 1$ ist.

(9.13) Beispiel.

(a) Das Polynom 2 über $\mathbb{Q}$ ist konstant.

(b) Das Polynom $2X + 3$ über $\mathbb{Q}$ ist linear.

Nullstellen

Unter allen Körperelementen, die man in ein gegebenes Polynom einsetzen kann, sind diejenigen von besonderem Interesse, welche die Null als Wert annehmen:

(9.14) Definition (Nullstelle)**.** Es sei $f \in K[X]$ gegeben. Eine *Nullstelle* von f ist ein $a \in K$ mit

$$f(a) = 0.$$

(9.15) Beispiel. Es sei $f \in \mathbb{Q}[X]$ gegeben durch $f = X^2 - 1$. Dann sind 1 und -1 Nullstellen von f.

Beweis. Es gilt $f(1) = 1^2 - 1 = 0$ und $f(-1) = (-1)^2 - 1 = 0$. Folglich sind 1 und -1 Nullstellen von f. □

(9.16) Definition (algebraisch abgeschlossen)**.** Wir nennen K *algebraisch abgeschlossen*, falls jedes Polynom über K, welches nicht konstant ist, eine Nullstelle hat.

(9.17) Beispiel. Der Körper der reellen Zahlen $\mathbb{R}$ ist nicht algebraisch abgeschlossen.

Beweis. Für alle $a \in \mathbb{R}$ gilt $a^2 + 1 \geq 0 + 1 = 1 > 0$ und damit insbesondere $a^2 + 1 \neq 0$, d.h. das Polynom $X^2 + 1$ über $\mathbb{R}$ hat keine Nullstelle. Folglich ist $\mathbb{R}$ nicht algebraisch abgeschlossen. □

Der *Fundamentalsatz der Algebra*, welchen wir im Rahmen dieser Vorlesung nicht beweisen können, besagt, dass der Körper der komplexen Zahlen $\mathbb{C}$, siehe Definition (11.25), algebraisch abgeschlossen ist.

Sebastian Thomas

RWTH Aachen, WS 2016/17
24.11.2016–30.11.2016

Diskrete Strukturen

Vorlesungen 11 und 12 (vorläufig, wird fortgesetzt)

10 Teilbarkeitslehre

Ziel dieses Abschnitts ist es zu sehen, dass es starke formale Ähnlichkeiten zwischen dem Ring der ganzen Zahlen $\mathbb{Z}$ und dem Polynomring $K[X]$ über einem Körper K gibt.

Division mit Rest

Wir beginnen mit der (zumindest in Spezialfällen aus der Schule bekannten) Division mit Rest, für welche es sowohl eine Version für ganze Zahlen als auch für Polynome mit Koeffizienten in einem Körper gibt.

(10.1) Satz (Ganzzahldivision, Polynomdivision)**.**

(a) Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gegeben. Ferner seien Folgen $(q_i)_{i\in\mathbb{N}_0}$ und $(r_i)_{i\in\mathbb{N}_0}$ in $\mathbb{Z}$ rekursiv definiert durch

$$q_i := \begin{cases} 0, & \text{für } i = 0, \\ q_{i-1} + (\operatorname{sgn} r_{i-1})(\operatorname{sgn} b), & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \notin [0, |b| - 1], \\ q_{i-1}, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \in [0, |b| - 1], \end{cases}$$

$$r_i := \begin{cases} a, & \text{für } i = 0, \\ r_{i-1} - (\operatorname{sgn} r_{i-1})|b|, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \notin [0, |b| - 1], \\ r_{i-1}, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \in [0, |b| - 1]. \end{cases}$$

(i) Für alle $i \in \mathbb{N}_0$ gilt

$$a = q_i b + r_i.$$

(ii) Es existiert ein $n \in [0, \max(0, |a| - |b| + 1)]$ mit $r_n \in [0, |b| - 1]$ und $q_i = q_n$, $r_i = r_n$ für $i \in \mathbb{N}_0$ mit $i \geq n$.

(b) Es seien ein Körper K und $f \in K[X]$, $g \in K[X] \setminus \{0\}$ gegeben. Ferner seien Folgen $(q_i)_{i\in\mathbb{N}_0}$ und $(r_i)_{i\in\mathbb{N}_0}$ in $K[X]$ rekursiv definiert durch

$$q_i := \begin{cases} 0, & \text{für } i = 0, \\ q_{i-1} + \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g}, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \notin K[X]_{<\deg g}, \\ q_{i-1}, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \in K[X]_{<\deg g}, \end{cases}$$

$$r_i := \begin{cases} f, & \text{für } i = 0, \\ r_{i-1} - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \notin K[X]_{<\deg g}, \\ r_{i-1}, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \in K[X]_{<\deg g}. \end{cases}$$

(i) Für alle $i \in \mathbb{N}_0$ gilt

$$f = q_i g + r_i.$$

(ii) Es existiert ein $n \in \mathbb{N}_0$ mit $r_n \in K[X]_{<\deg g}$ und $q_i = q_n$, $r_i = r_n$ für $i \in \mathbb{N}_0$ mit $i \geq n$. Wenn $f \neq 0$ ist, dann kann $n \in \mathbb{N}_0$ so gewählt werden, dass zusätzlich $n \leq \max(0, \deg f - \deg g + 1)$ gilt.

Beweis.

(a) (i) Wir führen Induktion nach i. Für $i = 0$ gilt

$$q_i b + r_i = q_0 b + r_0 = 0 \cdot b + a = a.$$

Nun sei $i \in \mathbb{N}$ so gegeben, dass $a = q_{i-1} b + r_{i-1}$ gilt. Dann erhalten wir auch

$$\begin{aligned} q_i b + r_i &= \begin{Bmatrix} (q_{i-1} + (\operatorname{sgn} r_{i-1})(\operatorname{sgn} b))b + r_{i-1} - (\operatorname{sgn} r_{i-1})|b|, & \text{falls } r_{i-1} \notin [0, |b| - 1], \\ q_{i-1} b + r_{i-1}, & \text{falls } r_{i-1} \in [0, |b| - 1] \end{Bmatrix} \\ &= \begin{Bmatrix} q_{i-1} b + (\operatorname{sgn} r_{i-1})(\operatorname{sgn} b)b + r_{i-1} - (\operatorname{sgn} r_{i-1})|b|, & \text{falls } r_{i-1} \notin [0, |b| - 1], \\ q_{i-1} b + r_{i-1}, & \text{falls } r_{i-1} \in [0, |b| - 1] \end{Bmatrix} \\ &= q_{i-1} b + r_{i-1} = a. \end{aligned}$$

Nach dem Induktionsprinzip gilt $a = q_i b + r_i$ für alle $i \in \mathbb{N}_0$.

(ii) Zunächst sei $i \in \mathbb{N}$ mit $r_{i-1} \notin [0, |b| - 1]$ gegeben. Dann gilt

$$\begin{aligned} |r_i| = |r_{i-1} - (\operatorname{sgn} r_{i-1})|b|| &= \begin{Bmatrix} |r_{i-1} - |b||, & \text{falls } r_{i-1} > 0, \\ |r_{i-1} + |b||, & \text{falls } r_{i-1} < 0 \end{Bmatrix} = \begin{Bmatrix} r_{i-1} - |b|, & \text{falls } r_{i-1} > 0, \\ -(r_{i-1} + |b|), & \text{falls } r_{i-1} < 0 \end{Bmatrix} \\ &= \begin{Bmatrix} r_{i-1} - |b|, & \text{falls } r_{i-1} > 0, \\ -r_{i-1} - |b|, & \text{falls } r_{i-1} < 0 \end{Bmatrix} = |r_{i-1}| - |b| < |r_{i-1}|. \end{aligned}$$

Für $i \in \mathbb{N}$ mit $r_{i-1} \in [0, |b| - 1]$ gilt hingegen $r_i = r_{i-1}$ und damit $r_i \in [0, |b| - 1]$.
Falls $a \notin [0, |b| - 1]$ ist, erhalten wir induktiv $r_{|a|-|b|+1} \in [0, |b| - 1]$. Falls hingegen $a \in [0, |b| - 1]$ ist, gilt $r_0 = a \in [0, |b| - 1]$. Es sei $n := \min\{i \in \mathbb{N}_0 \mid r_i \in [0, |b| - 1]\}$. Per Induktion folgt $q_i = q_n$ und $r_i = r_n$ für $i \in \mathbb{N}_0$ mit $i \geq n$. Wenn $a \notin [0, |b| - 1]$ ist, gilt $n \leq |a| - |b| + 1$, und wenn $a \in [0, |b| - 1]$ ist, gilt $n = 0$. Insgesamt gilt also stets $n \leq \max(0, |a| - |b| + 1)$ und damit $n \in [0, \max(0, |a| - |b| + 1)]$.

(b) (i) Wir führen Induktion nach i. Für $i = 0$ gilt

$$q_i g + r_i = q_0 g + r_0 = 0 \cdot g + f = f.$$

Nun sei $i \in \mathbb{N}$ so gegeben, dass $f = q_{i-1} g + r_{i-1}$ gilt. Dann erhalten wir auch

$$\begin{aligned} q_i g + r_i &= \begin{Bmatrix} (q_{i-1} + \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g})g \\ \qquad + r_{i-1} - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g, & \text{falls } r_{i-1} \notin K[X]_{<\deg g}, \\ q_{i-1} g + r_{i-1}, & \text{falls } r_{i-1} \in K[X]_{<\deg g} \end{Bmatrix} \\ &= \begin{Bmatrix} q_{i-1} g + \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g \\ \qquad + r_{i-1} - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g, & \text{falls } r_{i-1} \notin K[X]_{<\deg g}, \\ q_{i-1} g + r_{i-1}, & \text{falls } r_{i-1} \in K[X]_{<\deg g} \end{Bmatrix} \\ &= q_{i-1} g + r_{i-1} = f. \end{aligned}$$

Nach dem Induktionsprinzip gilt $f = q_i g + r_i$ für alle $i \in \mathbb{N}_0$.

(ii) Zunächst sei $i \in \mathbb{N}$ mit $r_{i-1} \notin K[X]_{<\deg g}$ gegeben. Dann gilt

$$\begin{aligned} \deg(\operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g) &= \deg X^{\deg r_{i-1} - \deg g} + \deg g \\ &= \deg r_{i-1} - \deg g + \deg g = \deg r_{i-1} \end{aligned}$$

nach Bemerkung (9.7)(b) und damit $r_i = 0$ oder $r_i \neq 0$ und

$$\begin{aligned} \deg r_i &= \deg(r_{i-1} - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g) \\ &\leq \max(\deg r_{i-1}, \deg(\operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g)) = \deg r_{i-1} \end{aligned}$$

nach Bemerkung (9.7)(a). Da der Koeffizient von $r_i = r_{i-1} - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g$ an der Stelle $\deg r_{i-1}$ durch $\operatorname{lc}(r_{i-1}) - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} \operatorname{lc}(g) = 0$ gegeben ist, gilt sogar $r_i = 0$ oder $r_i \neq 0$ und $\deg r_i < \deg r_{i-1}$, d.h. es ist $r_i \in K[X]_{<\deg r_{i-1}}$.

Für $i \in \mathbb{N}$ mit $r_{i-1} \in K[X]_{<\deg g}$ gilt hingegen $r_i = r_{i-1}$ und damit $r_i \in K[X]_{<\deg g}$.
Falls $f \notin K[X]_{<\deg g}$ ist, erhalten wir induktiv $r_{\deg f - \deg g + 1} \in K[X]_{<\deg g}$. Falls hingegen $f \in K[X]_{<\deg g}$ ist, gilt $r_0 = f \in K[X]_{<\deg g}$. Es sei $n := \min\{i \in \mathbb{N}_0 \mid r_i \in K[X]_{<\deg g}\}$. Per Induktion folgt $q_i = q_n$ und $r_i = r_n$ für $i \in \mathbb{N}_0$ mit $i \geq n$. Wenn $f \notin K[X]_{<\deg g}$ ist, gilt $n \leq \deg f - \deg g + 1$, und wenn $f \in K[X]_{<\deg g} \setminus \{0\}$ ist, gilt $n = 0$. Insgesamt gilt also, sofern $f \neq 0$ ist, stets $n \leq \max(0, \deg f - \deg g + 1)$. □

(10.2) Satz (Division mit Rest)**.**

(a) Für alle $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gibt es eindeutige $q \in \mathbb{Z}$, $r \in [0, |b| - 1]$ mit

$$a = qb + r.$$

(b) Es sei ein Körper K gegeben. Für alle $f \in K[X]$, $g \in K[X] \setminus \{0\}$ gibt es eindeutige $q \in K[X]$, $r \in K[X]_{<\deg g}$ mit

$$f = qg + r.$$

Beweis.

(a) Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gegeben. Nach Satz (10.1)(a) gibt es $q \in \mathbb{Z}$, $r \in [0, |b| - 1]$ mit $a = qb + r$. Für die Eindeutigkeit seien $q, q' \in \mathbb{Z}$, $r, r' \in [0, |b| - 1]$ mit $x = qb + r = q'b + r'$ gegeben. Dann ist

$$|q - q'|\,|b| = |(q - q')b| = |qb - q'b| = |r' - r| < |b|.$$

Wegen $b \neq 0$ impliziert dies $|q - q'| < 1$, also $|q - q'| = 0$. Folglich ist $q - q' = 0$, d.h. es gilt $q = q'$ und damit auch $r = a - qb = a - q'b = r'$.

(b) Es seien $f \in K[X]$, $g \in K[X] \setminus \{0\}$ gegeben. Nach Satz (10.1)(b) gibt es $q \in K[X]$, $r \in K[X]_{<\deg g}$ mit $f = qg + r$. Für die Eindeutigkeit seien $q, q' \in K[X]$, $r, r' \in K[X]_{<\deg g}$ mit $f = qg + r = q'g + r'$ gegeben. Dann ist

$$(q - q')g = qg - q'g = r' - r \in K[X]_{<\deg g}$$

und damit $(q - q')g = 0$ nach Bemerkung (9.7)(b). Wegen $g \neq 0$ impliziert dies aber bereits $q - q' = 0$, d.h. es gilt $q = q'$ und damit auch $r = f - qg = f - q'g = r'$. □

(10.3) Definition (ganzer Anteil, Rest)**.**

(a) Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gegeben und es seien $q \in \mathbb{Z}$, $r \in [0, |b| - 1]$ die eindeutigen ganzen Zahlen mit $a = qb + r$. Dann heißt $a \operatorname{div} b := q$ der *ganzzahlige Anteil* (oder der *ganze Anteil*) und $a \bmod b := r$ der *Rest* bei der *Ganzzahldivision* von a durch b.

(b) Es seien ein Körper K sowie $f \in K[X]$, $g \in K[X] \setminus \{0\}$ gegeben und es seien $q, r \in K[X]$ die eindeutigen Polynome mit $f = qg + r$ und mit $r = 0$ oder $r \neq 0$, $\deg r < \deg g$. Dann heißt $f \operatorname{div} g := q$ der *ganze Anteil* und $f \bmod g := r$ der *Rest* bei der *Polynomdivision* von f durch g.

(10.4) Beispiel.

(a) In $\mathbb{Z}$ ist $(-47) \operatorname{div} 9 = -6$ und $(-47) \bmod 9 = 7$.

(b) In $\mathbb{Q}[X]$ ist $(6X^3 + X^2 + 7) \operatorname{div} (2X^2 + X - 3) = 3X - 1$ und $(6X^3 + X^2 + 7) \bmod (2X^2 + X - 3) = 10X + 4$.

Beweis.

(a) Eine Ganzzahldivision liefert

$$\begin{aligned} -47 &= 0 \cdot 9 + (-47) = (-1) \cdot 9 + (-38) = (-2) \cdot 9 + (-29) = (-3) \cdot 9 + (-20) = (-4) \cdot 9 + (-11) \\ &= (-5) \cdot 9 + (-2) = (-6) \cdot 9 + 7. \end{aligned}$$

Folglich ist $(-47) \operatorname{div} 9 = -6$ und $(-47) \bmod 9 = 7$.

(b) Eine Polynomdivision liefert

$$\begin{aligned} 6X^3 + X^2 + 7 &= 0 \cdot (2X^2 + X - 3) + 6X^3 + X^2 + 7 = 3X \cdot (2X^2 + X - 3) + (-2X^2 + 9X + 7) \\ &= (3X - 1) \cdot (2X^2 + X - 3) + (10X + 4). \end{aligned}$$

Folglich ist $(6X^3 + X^2 + 7) \operatorname{div} (2X^2 + X - 3) = 3X - 1$ und $(6X^3 + X^2 + 7) \bmod (2X^2 + X - 3) = 10X + 4$. □

Teilbarkeit

Als nächstes studieren wir die Teilbarkeitsrelation in $\mathbb{Z}$ und in $K[X]$ für einen Körper K.

(10.5) Definition (Teilbarkeit)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben. Wir sagen a *teilt* b (oder dass a ein *Teiler* von b ist oder dass a ein *Faktor* von b ist oder dass b ein *Vielfaches* von a ist), geschrieben $a \mid b$, falls ein $q \in R$ mit $b = qa$ existiert. Wenn a kein Teiler von b ist, so schreiben wir $a \nmid b$.

(10.6) Beispiel.

(a) In $\mathbb{Z}$ gilt $3 \mid 6$ und $4 \nmid 6$.

(b) In $\mathbb{Q}[X]$ gilt $X - 1 \mid X^2 - 1$ und $X \nmid X^2 - 1$.

Beweis.

(a) Es gilt $6 = 2 \cdot 3$, also $3 \mid 6$. Wegen $6 = 1 \cdot 4 + 2$ gibt es nach dem Satz über die Division mit Rest (10.2)(a) kein $q \in \mathbb{Z}$ mit $6 = q \cdot 4$, so dass $4 \nmid 6$ folgt.

(b) Es gilt $X^2 - 1 = (X + 1)(X - 1)$, also $X - 1 \mid X^2 - 1$. Wegen $X^2 - 1 = X \cdot X + (-1)$ gibt es nach dem Satz über die Division mit Rest (10.2)(b) kein $q \in \mathbb{Q}[X]$ mit $X^2 - 1 = q \cdot X$, so dass $X \nmid X^2 - 1$ folgt. □

(10.7) Bemerkung. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a \in R \setminus \{0\}$, $b \in R$ gegeben. Genau dann gilt $a \mid b$, wenn $b \bmod a = 0$ ist.

Beweis. Wenn $a \mid b$ gilt, dann gibt es ein $q \in R$ mit $b = qa = qa + 0$ und nach dem Satz über die Division mit Rest (10.2) folgt $b \bmod a = 0$. Gilt umgekehrt $b \bmod a = 0$, so folgt $b = (b \operatorname{div} a)a + (b \bmod a) = (b \operatorname{div} a)a$ und damit $a \mid b$. □

(10.8) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Die Teilbarkeitsrelation $\mid$ auf R ist eine Präordnung.

Beweis. Es seien $a, b, c \in R$ mit $a \mid b$ und $b \mid c$ gegeben, d.h. es gebe $p, q \in R$ mit $b = pa$ und $c = qb$. Dann folgt

$$c = qb = q(pa) = (qp)a,$$

also $a \mid c$. Folglich ist $\mid$ transitiv.
Für $a \in R$ gilt $a = 1 \cdot a$, also $a \mid a$. Folglich ist $\mid$ reflexiv.
Insgesamt ist $\mid$ eine Präordnung auf R. □

Wir studieren weitere Eigenschaften der Teilbarkeitsrelation.

(10.9) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K.

(a) Für $a, b, c \in R$ gilt: Wenn $a \mid b$ und $a \mid c$, dann auch $a \mid b + c$.

(b) Für $a \in R$ gilt $a \mid 0$.

(c) Für $a, b, c \in R$ gilt: Wenn $a \mid b$, dann auch $a \mid cb$.

Beweis.

(a) Es seien $a, b, c \in R$ mit $a \mid b$ und $a \mid c$ gegeben, d.h. es gebe $p, q \in R$ mit $b = pa$ und $c = qa$. Dann folgt

$$b + c = pa + qa = (p + q)a,$$

also $a \mid b + c$.

(b) Für $a \in R$ gilt $0 = 0 \cdot a$, also $a \mid 0$.

(c) Es seien $a, b, c \in R$ gegeben und es gelte $a \mid b$. Da auch $b \mid cb$ gilt, folgt $a \mid cb$ nach Proposition (10.8). □

Assoziiertheit

Nach Proposition (10.8) ist die Teilbarkeitsrelation | eine Präordnung auf $\mathbb{Z}$ bzw. auf $K[X]$ für einen Körper K. Im Allgemeinen gilt jedoch keine Antisymmetrie, es kann in diesen Ringen Elemente a und b mit $a \mid b$ und $b \mid a$ und $a \neq b$ geben. Wir vergeben folgende Terminologie:

(10.10) Definition (assoziierte Elemente)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben. Wir sagen, dass a *assoziiert* zu b ist, wenn $a \mid b$ und $b \mid a$ gilt.

(10.11) Beispiel.

(a) In $\mathbb{Z}$ ist 3 assoziiert zu -3.

(b) In $\mathbb{Q}[X]$ ist $X - 1$ assoziiert zu $2X - 2$.

Beweis.

(a) Wegen $-3 = (-1) \cdot 3$ gilt $3 \mid -3$ und wegen $3 = (-1) \cdot (-3)$ gilt $-3 \mid 3$. Folglich ist 3 assoziiert zu -3.

(b) Wegen $2X - 2 = 2(X - 1)$ gilt $X - 1 \mid 2X - 2$ und wegen $X - 1 = \frac{1}{2}(2X - 2)$ gilt $-3 \mid 3$. Folglich ist $X - 1$ assoziiert zu $2X - 2$. □

(10.12) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben. Die folgenden Aussagen sind äquivalent.

(a) Es ist a assoziiert zu b.

(b) Es gibt ein $u \in R^\times$ mit $b = ua$.

(c) Im Fall $R = \mathbb{Z}$ gilt $|a| = |b|$. Im Fall $R = K[X]$ gilt entweder $a = b = 0$ oder $\mathrm{lc}(a)^{-1}a = \mathrm{lc}(b)^{-1}b$.

Beweis. Zunächst gelte Bedingung (a), d.h. es sei a assoziiert zu b. Dann gilt $a \mid b$ und $b \mid a$, d.h. es gibt $p, q \in R$ mit $b = pa$ und $a = qb$. Wir erhalten

$$a = qb = q(pa) = (qp)a.$$

Da R nach Beispiel (6.51) bzw. nach Korollar (9.9) ein Integritätsbereich ist, folgt $a = 0$ oder $qp = 1$ nach Bemerkung (6.52). Wenn $a = 0$ ist, dann ist $b = pa = 0 = 1 \cdot a$ und es ist $1 \in R^\times$ nach Proposition (6.30)(b) auf Grund der Kommutativität des Rings R. Wenn $qp = 1$ ist, dann ist $p \in R^\times$. In jedem Fall gibt es ein $u \in R^\times$ mit $b = ua$, d.h. es gilt Bedingung (b).
Umgekehrt, wenn Bedingung (b) gilt, d.h. wenn es ein $u \in R^\times$ mit $b = ua$ gibt, dann gilt auch $a = u^{-1}b$ und damit $a \mid b$ und $b \mid a$, d.h. auch Bedingung (a) gilt.
Wir haben gezeigt, dass Bedingung (a) und Bedingung (b) äquivalent sind.
Um zu zeigen, dass Bedingung (b) und Bedingung (c) äquivalent sind, betrachten wir zunächst den Fall $R = \mathbb{Z}$. Dann ist $R^\times = \mathbb{Z}^\times = \{1, -1\}$. Folglich gibt es genau dann ein $u \in R^\times$ mit $b = ua$, wenn $|a| = |b|$ gilt, d.h. Bedingung (b) und Bedingung (c) sind in diesem Fall äquivalent.
Schließlich betrachten wir den Fall $R = K[X]$ für einen Körper K. Dann ist $R^\times = K[X]^\times = K^\times$. Folglich gibt es genau dann ein $u \in R^\times$ mit $b = ua$, wenn $a = b = 0$ oder $\mathrm{lc}(a)^{-1}a = \mathrm{lc}(b)^{-1}b$ gilt, d.h. Bedingung (b) und Bedingung (c) sind auch in diesem Fall äquivalent.
Wir haben gezeigt, dass Bedingung (b) und Bedingung (c) äquivalent sind.
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

Teilbarkeit und Nullstellen von Polynomen

Mit Hilfe der Teilbarkeitsrelation lassen sich Nullstellen von Polynomen über einem Körper charakterisieren:

(10.13) Definition (Linearfaktor)**.** Es seien ein Körper K und ein $f \in K[X]$ gegeben. Ein *Linearfaktor* von f ist ein lineares Polynom über K, welches ein Teiler von f ist.

Ein Linearfaktor eines Polynoms f über einem Körper K ist also ein Polynom von der Form $aX + b$ für gewisse $a \in K \setminus \{0\} = K^\times$, $b \in K$.

(10.14) Proposition. Es seien ein Körper K, $f \in K[X]$ und $a \in K$ gegeben. Genau dann ist a eine Nullstelle von f, wenn $X - a$ ein Linearfaktor von f ist.

Beweis. Es sei $q := f \operatorname{div} (X - a)$ und $r := f \bmod (X - a)$. Dann gilt

$$f = (f \operatorname{div} (X - a)) \cdot (X - a) + f \bmod (X - a) = q \cdot (X - a) + r$$

und damit

$$f(a) = q(a) \cdot (a - a) + r(a) = r(a).$$

Wegen $\deg(X - a) = 1$ ist $r \in K[X]_{<\deg(X-a)} = K[X]_{<1} = K$, also $r = r(a) = f(a)$. Somit ist a genau dann eine Nullstelle von f, wenn $r = 0$ ist, d.h. wenn $X - a$ ein Linearfaktor von f ist. □

Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

Als nächstes thematisieren wir die aus der Schule bekannten Begriffe des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen, wobei wir diese über die Teilbarkeitsrelation definieren.

(10.15) Definition (gemeinsamer Teiler, gemeinsames Vielfaches)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben.

(a) Ein *gemeinsamer Teiler* von a und b ist ein $d \in R$ so, dass $d \mid a$ und $d \mid b$ gilt.

(b) Ein *gemeinsames Vielfaches* von a und b ist ein $m \in R$ so, dass $a \mid m$ und $b \mid m$ gilt.

(10.16) Beispiel.

(a) (i) In $\mathbb{Z}$ sind 1, 2, -6 gemeinsame Teiler von 12 und 18.

(ii) In $\mathbb{Q}[X]$ sind 1, $X + 1$, $2X + 2$ gemeinsame Teiler von $X^2 - 1$ und $X^2 + 2X + 1$.

(b) (i) In $\mathbb{Z}$ sind 12 und -24 gemeinsame Vielfache von 4 und 6.

(ii) In $\mathbb{Q}[X]$ sind $X^3 - X^2 - X + 1$ und $-\frac{1}{2}X^4 + X^3 - X + \frac{1}{2}$ gemeinsame Vielfache von $X^2 - 2X + 1$ und $X^2 - 1$.

Beweis.

(a) (i) Wegen $12 = 12 \cdot 1$ gilt $1 \mid 12$ und wegen $18 = 18 \cdot 1$ gilt $1 \mid 18$. Folglich ist 1 ein gemeinsamer Teiler von 12 und 18.
Wegen $12 = 6 \cdot 2$ gilt $2 \mid 12$ und wegen $18 = 9 \cdot 2$ gilt $2 \mid 18$. Folglich ist 2 ein gemeinsamer Teiler von 12 und 18.
Wegen $12 = (-2) \cdot (-6)$ gilt $-6 \mid 12$ und wegen $18 = (-3) \cdot (-6)$ gilt $-6 \mid 18$. Folglich ist -6 ein gemeinsamer Teiler von 12 und 18.

(ii) Wegen $X^2 - 1 = (X^2 - 1) \cdot 1$ gilt $1 \mid X^2 - 1$ und wegen $X^2 + 2X + 1 = (X^2 + 2X + 1) \cdot 1$ gilt $1 \mid X^2 + 2X + 1$. Folglich ist 1 ein gemeinsamer Teiler von $X^2 - 1$ und $X^2 + 2X + 1$.
Wegen $X^2 - 1 = (X - 1)(X + 1)$ gilt $X + 1 \mid X^2 - 1$ und wegen $X^2 + 2X + 1 = (X + 1)(X + 1)$ gilt $X + 1 \mid X^2 + 2X + 1$. Folglich ist 1 ein gemeinsamer Teiler von $X^2 - 1$ und $X^2 + 2X + 1$.
Wegen $X^2 - 1 = (\frac{1}{2}X - \frac{1}{2})(2X + 2))$ gilt $2X + 2 \mid X^2 - 1$ und wegen $X^2 + 2X + 1 = (\frac{1}{2}X + \frac{1}{2})(2X + 2)$ gilt $2X + 2 \mid X^2 + 2X + 1$. Folglich ist 1 ein gemeinsamer Teiler von $X^2 - 1$ und $X^2 + 2X + 1$.

(b) (i) Wegen $12 = 3 \cdot 4$ gilt $4 \mid 12$ und wegen $12 = 2 \cdot 6$ gilt $6 \mid 12$. Folglich ist 12 ein gemeinsames Vielfaches von 4 und 6.
Wegen $-24 = (-6) \cdot 4$ gilt $4 \mid -24$ und wegen $-24 = (-4) \cdot 6$ gilt $6 \mid -24$. Folglich ist -24 ein gemeinsames Vielfaches von 4 und 6.

(ii) Wegen $X^3 - X^2 - X + 1 = (X + 1) \cdot (X^2 - 2X + 1)$ gilt $X^2 - 2X + 1 \mid X^3 - X^2 - X + 1$ und wegen $X^3 - X^2 - X + 1 = (X - 1) \cdot (X^2 - 1)$ gilt $X^2 - 1 \mid X^3 - X^2 - X + 1$. Folglich ist $X^3 - X^2 - X + 1$ ein gemeinsames Vielfaches von $X^2 - 2X + 1$ und $X^2 - 1$.
Wegen $-\frac{1}{2}X^4 + X^3 - X + \frac{1}{2} = (-\frac{1}{2}X^2 + \frac{1}{2}) \cdot (X^2 - 2X + 1)$ gilt $X^2 - 2X + 1 \mid -\frac{1}{2}X^4 + X^3 - X + \frac{1}{2}$ und wegen $-\frac{1}{2}X^4 + X^3 - X + \frac{1}{2} = (-\frac{1}{2}X^2 + X - \frac{1}{2}) \cdot (X^2 - 1)$ gilt $X^2 - 1 \mid -\frac{1}{2}X^4 + X^3 - X + \frac{1}{2}$. Folglich ist $-\frac{1}{2}X^4 + X^3 - X + \frac{1}{2}$ ein gemeinsames Vielfaches von $X^2 - 2X + 1$ und $X^2 - 1$. □

(10.17) Definition (größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben.

(a) Ein *größter gemeinsamer Teiler* von a und b ist ein gemeinsamer Teiler g von a und b derart, dass jeder gemeinsame Teiler d von a und b auch ein Teiler von g ist.

(b) Ein *kleinstes gemeinsames Vielfaches* von a und b ist ein gemeinsames Vielfaches l von a und b derart, dass jedes gemeinsame Vielfache m von a und b auch ein Vielfaches von l ist.

Ein größter gemeinsamer Teiler ist also ein größtes Element in der prägeordneten Menge der gemeinsamen Teiler zusammen mit der Teilbarkeitsrelation, vgl. Definition (7.10)(b)(ii).

(10.18) Beispiel.

(a) In $\mathbb{Z}$ ist -6 ein größter gemeinsamer Teiler von 12 und 18.

(b) In $\mathbb{Z}$ ist 12 ein kleinstes gemeinsames Vielfaches von 4 und 6.

Beweis.

(a) Es sei $T := \{d \in \mathbb{Z} \mid d \mid 12 \text{ und } d \mid 18\}$ die Menge der gemeinsamen Teiler von 12 und 18. Nach Beispiel (10.16)(a)(i) ist $-6 \in T$. Da für $a \in \mathbb{Z}$ aus $a \mid 12$ stets $|a| \leq |12| = 12$ folgt, gilt ferner $T \subseteq [-12, 12]$. Durch Ausrechnen ergibt sich

$$T = \{-6, -3, -2, -1, 1, 2, 3, 6\}.$$

Da für alle $d \in T$ auch $d \mid -6$ gilt, ist -6 somit ein größter gemeinsamer Teiler von 12 und 18.

(b) Es sei $I := \{m \in \mathbb{Z} \mid 4 \mid m \text{ und } 6 \mid m\}$ die Menge der gemeinsamen Vielfache von 4 und 6. Nach Beispiel (10.16)(b)(i) ist $12 \in I$. Es sei ein beliebiges gemeinsames Vielfaches m von 4 und 6 gegeben. Dann gilt $4 \mid m$ und $6 \mid m$, nach Proposition (10.9)(a) also auch $4 \mid m - (m \operatorname{div} 12) \cdot 12 = m \bmod 12$ und $6 \mid m - (m \operatorname{div} 12) \cdot 12 = m \bmod 12$. Folglich ist $m \bmod 12 \in I$. Durch Ausrechnen ergibt sich ferner $[0, 11] \cap I = \{0\}$, so dass $m \bmod 12 = 0$ folgt. Somit ist m ein Vielfaches von 12. Insgesamt ist 12 daher ein kleinstes gemeinsames Vielfaches von 4 und 6. □

Im Beweis von Beispiel (10.18) haben wir an entscheidender Stelle benutzt, dass die ganzzahligen Intervalle $[-12, 12]$ bzw. $[0, 11]$ endliche Mengen sind. Eine effizientere Methode zur Berechnung von größten gemeinsamen Teilern, welche sich auch für Polynome über Körpern eignet, werden wir in Satz (10.24) kennenlernen. Unter Ausnutzung von Satz (10.22) wird dies auch eine Möglichkeit zur effizienten Berechnung von kleinsten gemeisamen Vielfachen liefern.

(10.19) Bemerkung. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben.

(a) Es sei ein größter gemeinsamer Teiler g von a und b sowie $g' \in R$ gegeben. Genau dann ist g' ein größter gemeinsamer Teiler von a und b, wenn g assoziiert zu g' ist.

(b) Es sei ein kleinstes gemeinsames Vielfaches l von a und b sowie $l' \in R$ gegeben. Genau dann ist l' ein kleinstes gemeinsames Vielfaches von a und b, wenn l assoziiert zu l' ist.

Beweis.

(a) Zunächst sei g' ein größter gemeinsamer Teiler von a und b. Dann ist g' insbesondere ein gemeinsamer Teiler von a und b und g ein größter gemeinsamer Teiler von a und b, wir haben also $g' \mid g$. Andererseits ist aber auch g ein gemeinsamer Teiler von a und b und g' ein größter gemeinsamer Teiler von a und b, wir haben also auch $g \mid g'$. Folglich ist g assoziiert zu g'.

Umgekehrt sei nun $g' = ug$ für ein $u \in R^\times$. Nach Proposition (10.12) ist mit g dann auch $g' = ug$ ein gemeinsamer Teiler von a und b, und für jeden gemeinsamen Teiler d von a und b folgt aus $d \mid g$ auch $d \mid ug$. Insgesamt ist g' ein größter gemeinsamer Teiler von a und b.

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

(10.20) Lemma (Lemma von Bézout)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben.

(a) Es sei $I := \{d \in R \mid \text{es gibt } x, y \in R \text{ mit } d = xa + yb\}$.

(i) Falls $(a, b) = (0, 0)$, sei $g = 0$. Falls $(a, b) \neq (0, 0)$ sei $g \in I$ so, dass folgendes gilt: Im Fall $R = \mathbb{Z}$ gelte

$$|g| = \min\{|d| \mid d \in I \setminus \{0\}\}.$$

Im Fall $R = K[X]$ für einen Körper K gelte

$$\deg g = \min\{\deg d \mid d \in I \setminus \{0\}\}.$$

Dann ist g ein größter gemeinsamer Teiler von a und b. Insbesondere existiert ein größter gemeinsamer Teiler von a und b.

(ii) Es sei $g \in R$ ein größter gemeinsamer Teiler von a und b. Dann ist $g \in I$.

(b) Es sei $I := \{m \in R \mid \text{es gibt } x, y \in R \text{ mit } m = xa \text{ und } m = yb\}$.

(i) Falls $(a, b) = (0, 0)$, sei $l = 0$. Falls $(a, b) \neq (0, 0)$ sei $l \in I$ so, dass folgendes gilt: Im Fall $R = \mathbb{Z}$ gelte

$$|l| = \min\{|m| \mid m \in I \setminus \{0\}\}.$$

Im Fall $R = K[X]$ für einen Körper K gelte

$$\deg l = \min\{\deg m \mid m \in I \setminus \{0\}\}.$$

Dann ist l ein kleinstes gemeinsames Vielfaches von a und b. Insbesondere existiert ein kleinstes gemeinsames Vielfaches von a und b.

(ii) Es sei $l \in R$ ein kleinstes gemeinsames Vielfaches von a und b. Dann ist $l \in I$.

Beweis.

(a) (i) Wenn $(a, b) = (0, 0)$ ist, so ist $g = 0$ ein größter gemeinsamer Teiler von a und b. Im Folgenden sei daher $(a, b) \neq (0, 0)$, so dass auch $g \neq 0$ gilt. Da $g \in I$ ist, gibt es $x, y \in R$ mit $g = xa + yb$. Folglich ist

$$a \bmod g = a - (a \operatorname{div} g)g = a - (a \operatorname{div} g)(xa + yb) = (1 - (a \operatorname{div} g)x)a + (a \operatorname{div} g)yb \in I,$$

also $a \bmod g = 0$ nach Wahl von g. Somit ist g ein Teiler von a. Analog lässt sich zeigen, dass g ein Teiler von b ist. Ferner ist jeder gemeinsame Teiler d von a und b nach Proposition (10.9)(a), (c) auch ein Teiler von $xa + yb = g$. Insgesamt ist g daher ein größter gemeinsamer Teiler von a und b.

(ii) Nach (i) gibt es einen größten gemeinsamen Teiler g' von a und b mit $g' \in I$, also derart, dass $g' = x'a + y'b$ für gewisse $x', y' \in R$. Da sowohl g als auch g' ein größter gemeinsamer Teiler von a und b ist, sind g und g' nach Bemerkung (10.19)(a) zueinander assoziiert. Nach Proposition (10.12) gibt es ein $u \in R^\times$ mit

$$g = ug' = u(x'a + y'b) = (ux')a + (uy')b.$$

Folglich ist auch $g \in I$. □

(b) (i) Wenn $(a, b) = (0, 0)$ ist, so ist $l = 0$ ein kleinstes gemeinsames Vielfaches von a und b. Im Folgenden sei daher $(a, b) \neq (0, 0)$. Da $l \in I$ ist, gibt es $x, y \in R$ mit $l = xa = yb$, d.h. l ist ein gemeinsames Vielfaches von a und b. Es sei ein beliebiges gemeinsames Vielfaches m von a und b gegeben. Dann gilt $a \mid m$ und $b \mid m$, nach Proposition (10.9)(a), (c) also auch $a \mid m - (m \operatorname{div} l)l = m \bmod l$ und $b \mid m - (m \operatorname{div} l)l = m \bmod l$. Folglich ist $m \bmod l \in I$, also $m \bmod l = 0$ nach Wahl von l. Somit ist m ein Vielfaches von l. Insgesamt ist l daher ein kleinstes gemeinsames Vielfaches von a und b.

(ii) Da l als kleinstes gemeinsames Vielfaches von a und b insbesondere ein gemeinsames Vielfaches von a und b ist, gibt es $x, y \in R$ mit $l = xa = yb$. Folglich ist $l \in I$.

Nach dem Lemma von Bézout (10.20) gibt es für jedes Paar ganzer Zahlen bzw. von Polynomen über einem Körper einen größten gemeinsamen Teiler sowie ein kleinstes gemeinsames Vielfaches, und nach Bemerkung (10.19) sind diese eindeutig bis auf Assoziiertheit. Im Folgenden geben wir einem ausgezeichneten größten gemeinsamen Teiler und einem ausgezeichneten kleinsten gemeinsamen Vielfachen eine feste Bezeichnung.

(10.21) Definition (größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches)**.**

(a) (i) Es seien $a, b \in \mathbb{Z}$ gegeben. Wir bezeichnen mit $\gcd(a, b)$ den eindeutig bestimmten nicht-negativen größten gemeinsamen Teiler von a und b.

(ii) Es seien ein Körper K und $f, g \in K[X]$ gegeben. Falls $(f, g) = (0, 0)$, so setzen wir $\gcd(f, g) := 0$. Andernfalls bezeichnen wir mit $\gcd(f, g)$ den eindeutig bestimmten normierten größten gemeinsamen Teiler von f und g.

(b) (i) Es seien $a, b \in \mathbb{Z}$ gegeben. Wir bezeichnen mit $\operatorname{lcm}(a, b)$ das eindeutig bestimmte nicht-negative kleinste gemeinsame Vielfache von a und b.

(ii) Es seien ein Körper K und $f, g \in K[X]$ gegeben. Falls $(f, g) = (0, 0)$, so setzen wir $\operatorname{lcm}(f, g) := 0$. Andernfalls bezeichnen wir mit $\operatorname{lcm}(f, g)$ das eindeutig bestimmte normierte kleinste gemeinsame Vielfache von f und g.

Wir haben also in den Fällen $R = \mathbb{Z}$ und $R = K[X]$ für einen Körper K wohldefinierte Abbildungen

$$\gcd\colon R \times R \to R,$$
$$\operatorname{lcm}\colon R \times R \to R$$

konstruiert.

(10.22) Satz. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben. Dann ist ab assoziiert zu $\gcd(a, b) \operatorname{lcm}(a, b)$.

Beweis. Zunächst gelte $\gcd(a, b) = 1$. Nach dem Lemma von Bézout (10.20) gibt es dann $x, y \in R$ mit $1 = xa + yb$. Da $\operatorname{lcm}(a, b)$ ein gemeinsames Vielfaches von a und b ist, gibt es ferner $p, q \in R$ mit $\operatorname{lcm}(a, b) = pa = qb$. Es folgt

$$(xq + yp)ab = xqab + ypab = qbxa + payb = \operatorname{lcm}(a, b)xa + \operatorname{lcm}(a, b)yb = \operatorname{lcm}(a, b)(xa + yb) = \operatorname{lcm}(a, b),$$

also $ab \mid \operatorname{lcm}(a, b)$. Andererseits ist aber auch ab ein gemeinsames Vielfaches von a und b, und da $\operatorname{lcm}(a, b)$ ein kleinstes gemeinsames Vielfaches von a und b ist, folgt $\operatorname{lcm}(a, b) \mid ab$. Folglich ist ab assoziiert zu $\operatorname{lcm}(a, b) = \gcd(a, b) \operatorname{lcm}(a, b)$.
Nun sei $\gcd(a, b)$ beliebig. Wenn $(a, b) = (0, 0)$ ist, so gilt

$$ab = 0 \cdot 0 = \gcd(a, b) \operatorname{lcm}(a, b).$$

Es sei also im Folgenden $(a, b) \neq (0, 0)$, so dass $\gcd(a, b) \neq 0$ ist. Da $\gcd(a, b)$ ein gemeinsamer Teiler von a und b ist, gibt es $p, q \in R$ mit $a = p \gcd(a, b)$ und $b = q \gcd(a, b)$. Es gilt $\gcd(p, q) = 1$ und $\operatorname{lcm}(a, b) = \gcd(a, b) \operatorname{lcm}(p, q)$. Nach dem bereits bewiesenen Spezialfall ist pq assoziiert zu $\gcd(p, q) \operatorname{lcm}(p, q) = \operatorname{lcm}(p, q)$. Folglich ist auch $ab = p \gcd(a, b)\, q \gcd(a, b) = \gcd(a, b)^2\, pq$ assoziiert zu $\gcd(a, b)^2 \operatorname{lcm}(p, q) = \gcd(a, b) \operatorname{lcm}(a, b)$. □

Alternativer Beweis von Beispiel (10.18)(b). Es sei $T := \{d \in \mathbb{Z} \mid d \mid 4 \text{ und } d \mid 6\}$ die Menge der gemeinsamen Teiler von 4 und 6. Wegen $4 = 2 \cdot 2$ und $6 = 3 \cdot 2$ ist $2 \in T$. Da für $a \in \mathbb{Z}$ aus $a \mid 6$ stets $|a| \leq |6| = 6$ folgt, gilt ferner $T \subseteq [-6, 6]$. Durch Ausrechnen ergibt sich

$$T = \{-2, -1, 1, 2\}.$$

Da für alle $d \in T$ auch $d \mid 2$ gilt und $2 \geq 0$ gilt, ist somit $\gcd(4, 6) = 2$.
Nach Satz (10.22) folgt

$$\operatorname{lcm}(4, 6) = \frac{4 \cdot 6}{\gcd(4, 6)} = \frac{4 \cdot 6}{2} = 12.$$ □

Der euklidische Algorithmus

Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Nach dem Lemma von Bézout (10.20)(a)(ii) wissen wir, dass es für $a, b \in R$ stets $x, y \in R$ mit $\gcd(a, b) = xa + yb$ gibt. Wir wollen nun einen Algorithmus herleiten, welcher zum einen $\gcd(a, b)$ und zum anderen eine solche Darstellung $(x, y) \in R \times R$ berechnet.

(10.23) Lemma. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Für $a \in R$, $b \in R \setminus \{0\}$ ist

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

Beweis. Es seien $a, b \in R$ gegeben. Für $d \in R$ mit $d \mid b$ gilt nach Proposition (10.9)(a), (c) genau dann $d \mid a$, wenn $d \mid a - (a \operatorname{div} b)b = a \bmod b$ gilt. Somit sind die gemeinsamen Teiler von a und b genau die gemeinsamen Teiler von b und $a \bmod b$. Als größte Elemente in der prägeordneten Menge der gemeinsamen Teiler von a und b mit der Teilbarkeitsrelation sind dann aber auch die größten gemeinsamen Teiler von a und b genau die größten gemeinsamen Teiler von b und $a \bmod b$. Folglich gilt auch $\gcd(a, b) = \gcd(b, a \bmod b)$. □

(10.24) Satz (erweiterter euklidischer Algorithmus)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a \in R$, $b \in R \setminus \{0\}$ gegeben. Es seien Folgen $(r_i)_{i\in\mathbb{N}_0}$, $(x_i)_{i\in\mathbb{N}_0}$, $(y_i)_{i\in\mathbb{N}_0}$ in R rekursiv definiert durch

$$r_i := \begin{cases} a, & \text{für } i = 0, \\ b, & \text{für } i = 1, \\ r_{i-2} \bmod r_{i-1}, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} \neq 0, \\ 0, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} = 0, \end{cases}$$

$$x_i := \begin{cases} 1, & \text{für } i = 0, \\ 0, & \text{für } i = 1, \\ x_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})x_{i-1}, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} \neq 0, \\ 0, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} = 0, \end{cases}$$

$$y_i := \begin{cases} 0, & \text{für } i = 0, \\ 1, & \text{für } i = 1, \\ y_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})y_{i-1}, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} \neq 0, \\ 0, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} = 0. \end{cases}$$

(a) Für alle $i \in \mathbb{N}_0$ gilt

$$r_i = x_i a + y_i b.$$

(b) Es existiert ein $n \in \mathbb{N}$ so, dass r_n assoziiert zu $\gcd(a, b)$ ist und $r_i = 0$ für $i > n$ gilt. Im Fall $R = \mathbb{Z}$ kann $n \in \mathbb{N}$ so gewählt werden, dass $n \leq |b| + 1$ gilt. Im Fall $R = K[X]$ für einen Körper K kann $n \in \mathbb{N}$ so gewählt werden, dass $n \leq \deg b + 2$ gilt.

Beweis.

(a) Um $x_i a + y_i b = r_i$ für alle $i \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach i. Zunächst gilt

$$x_0 a + y_0 b = 1 \cdot a + 0 \cdot b = a = r_0,$$
$$x_1 a + y_1 b = 0 \cdot a + 1 \cdot b = b = r_1,$$

also $x_i a + y_i b = r_i$ für $i \in \{0, 1\}$. Es sei also ein $i \in \mathbb{N}_0$ mit $i \geq 2$ gegeben und gelte $x_{i-2}a + y_{i-2}b = r_{i-2}$ sowie $x_{i-1}a + y_{i-1}b = r_{i-1}$. Wenn $r_{i-1} \neq 0$ ist, erhalten wir

$$\begin{aligned} x_i a + y_i b &= (x_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})x_{i-1})a + (y_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})y_{i-1})b \\ &= x_{i-2}a - (r_{i-2} \operatorname{div} r_{i-1})x_{i-1}a + y_{i-2}b - (r_{i-2} \operatorname{div} r_{i-1})y_{i-1}v \\ &= x_{i-2}a + y_{i-2}b - (r_{i-2} \operatorname{div} r_{i-1})(x_{i-1}a + y_{i-1}b) = r_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})r_{i-1} = r_i. \end{aligned}$$

Wenn $r_{i-1} = 0$ ist, erhalten wir ebenfalls

$$x_i a + y_i b = 0 \cdot a + 0 \cdot b = 0 = r_i.$$

Nach dem Induktionsprinzip gilt $x_i a + y_i b = r_i$ für alle $i \in \mathbb{N}_0$.

(b) Im Fall $R = \mathbb{Z}$ gilt für $i \geq 2$ stets $r_i = 0$ oder $r_i \neq 0$, $|r_i| = |r_{i-2} \bmod r_{i-1}| < |r_{i-1}|$, per Induktion also $r_{|b|+1} = 0$. Im Fall $R = K[X]$ für einen Körper K gilt für $i \geq 2$ stets $r_i = 0$ oder $r_i \neq 0$, $\deg r_i = \deg(r_{i-2} \bmod r_{i-1}) < \deg r_{i-1}$, per Induktion also $r_{(\deg b)+2} = 0$.

Wir setzen $n := \min\{i \in \mathbb{N} \mid r_i = 0\} - 1$. Dann ist $r_{n+1} = 0$, induktiv also $r_i = 0$ für alle $i \in \mathbb{N}_0$ mit $i > n$. Nach Lemma (10.23) gilt ferner

$$\gcd(r_{i-2}, r_{i-1}) = \gcd(r_{i-1}, r_{i-2} \bmod r_{i-1}) = \gcd(r_{i-1}, r_i)$$

für $i \in \mathbb{N}_0$, $i \geq 2$ mit $r_{i-1} \neq 0$. Induktiv erhalten wir

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_n, r_{n+1}) = \gcd(r_n, 0).$$

Nun ist aber r_n assoziiert zu $\gcd(r_n, 0) = \gcd(a, b)$. □

(10.25) Beispiel.

(a) In $\mathbb{Z}$ ist $\gcd(2238, 168) = 6$ und

$$6 = (-3) \cdot 2238 + 40 \cdot 168.$$

(b) In $\mathbb{Q}[X]$ ist $\gcd(X^3 + X^2 - X - 1, X^2 - 2X + 1) = X - 1$ und

$$X - 1 = \frac{1}{4}(X^3 + X^2 - X - 1) + (-\frac{1}{4}X - \frac{3}{4})(X^2 - 2X + 1).$$

Beweis.

(a) Wir berechnen $\gcd(2238, 168)$ mittels euklidischem Algorithmus:

$$\begin{aligned} 2238 &= 13 \cdot 168 + 54, \\ 168 &= 3 \cdot 54 + 6, \\ 54 &= 9 \cdot 6 + 0. \end{aligned}$$

Nach Satz (10.24)(b) ist $\gcd(2238, 168) = 6$. Wir setzen

$$\begin{aligned} r_0 &:= 2238, & & \\ r_1 &:= 168, & q_1 &:= 13, \\ r_2 &:= 54, & q_2 &:= 3, \\ r_3 &:= 6, & q_3 &:= 9, \end{aligned}$$

und berechnen $x_i, y_i \in \mathbb{Z}$ für $i \in \{0, 1, 2, 3\}$ mit dem erweiterten euklidischen Algorithmus:

$$\begin{aligned} x_0 &:= 1, & y_0 &:= 0, \\ x_1 &:= 0, & y_1 &:= 1, \\ x_2 &:= x_0 - q_1 x_1 = 1 - 13 \cdot 0 = 1, & y_2 &:= y_0 - q_1 y_1 = 0 - 13 \cdot 1 = -13, \\ x_3 &:= x_1 - q_2 x_2 = 0 - 3 \cdot 1 = -3, & y_3 &:= y_1 - q_2 y_2 = 1 - 3 \cdot (-13) = 40. \end{aligned}$$

Nach Satz (10.24)(b) ist

$$6 = r_3 = x_3 \cdot 2238 + y_3 \cdot 168 = (-3) \cdot 2238 + 40 \cdot 168.$$

(b) Wir berechnen $\gcd(X^3 + X^2 - X - 1, X^2 - 2X + 1)$ mittels euklidischem Algorithmus:

$$\begin{aligned} X^3 + X^2 - X - 1 &= (X + 3)(X^2 - 2X + 1) + 4X - 4, \\ X^2 - 2X + 1 &= (\frac{1}{4}X - \frac{1}{4})(4X - 4) + 0. \end{aligned}$$

Nach Satz (10.24)(b) ist $\gcd(X^3 + X^2 - X - 1, X^2 - 2X + 1) = X - 1$. Wir setzen

$$\begin{aligned} r_0 &:= X^3 + X^2 - X - 1, \\ r_1 &:= X^2 - 2X + 1, & q_1 &:= X + 3, \\ r_2 &:= 4X - 4, & q_2 &:= \frac{1}{4}X - \frac{1}{4}, \end{aligned}$$

und berechnen $h_i, k_i \in \mathbb{Q}[X]$ für $i \in \{0, 1, 2\}$ mit dem erweiterten euklidischen Algorithmus:

$$\begin{aligned} h_0 &:= 1, & k_0 &:= 0, \\ h_1 &:= 0, & k_1 &:= 1, \\ h_2 &:= h_0 - q_1 h_1 = 1 - (X + 3) \cdot 0 = 1, & k_2 &:= k_0 - q_1 k_1 = 0 - (X + 3) \cdot 1 = -X - 3. \end{aligned}$$

Nach Satz (10.24)(b) ist

$$4X - 4 = r_2 = h_2 f_2 + k_2 g_2 = 1(X^3 + X^2 - X - 1) + (-X - 3)(X^2 - 2X + 1)$$

und damit

$$X - 1 = \frac{1}{4}(4X - 4) = \frac{1}{4}(X^3 + X^2 - X - 1) + (-\frac{1}{4}X - \frac{3}{4})(X^2 - 2X + 1). \qquad \square$$