

# **Grundlagen und Diskrete Mathematik**

# Inhaltsverzeichnis

<b>1</b>	<b>Grundbegriffe und elementare Logik</b>	<b>3</b>
1.1	Aussagen, Prädikate und Quantoren . . . . .	4
1.2	Grundlegende Beweistechniken . . . . .	13
<b>2</b>	<b>Syntax und Semantik am Beispiel der formalen Aussagenlogik</b>	<b>18</b>
2.1	Syntax der Aussagenlogik . . . . .	20
2.2	Semantik der Aussagenlogik . . . . .	21
<b>3</b>	<b>Mengen, Relationen und Funktionen</b>	<b>35</b>
3.1	Der Mengenbegriff und grundlegende Definitionen . . . . .	37
3.2	Relationen, Funktionen und Graphen . . . . .	47
3.2.1	Funktionen . . . . .	53
3.2.2	Grössenvergleiche von unendlichen Mengen . . . . .	57
3.2.3	Ordnungs- und Äquivalenzrelationen . . . . .	68
<b>4</b>	<b>Rekursive Strukturen und die natürlichen Zahlen</b>	<b>86</b>
4.1	Die grundlegende Struktur der natürlichen Zahlen . . . . .	87
4.2	Vom Induktionsbeweis zum rekursiven Algorithmus . . . . .	93
4.3	Rekursive Definitionen . . . . .	96
<b>5</b>	<b>Elementare Zahlentheorie</b>	<b>101</b>
5.1	Teilbarkeit und Euklidischer Algorithmus . . . . .	103
5.2	Primzahlen . . . . .	110
5.3	Modulare Arithmetik . . . . .	113
5.3.1	Chinesischer Restsatz . . . . .	118

# 1 Grundbegriffe und elementare Logik

Am Anfang aller Logik steht...

Wenn “Doken” stets “derig” sind und wenn es “Raken” gibt die auch “Doken” sind, dann gibt es derige Raken und alle underigen Raken sind keine Doken.

...die Erkenntnis, dass gewisse Argumente unabhängig von deren Inhalt aber aufgrund ihrer Struktur als eindeutig schlüssig/korrekt identifizierbar sind. Dieses Kapitel gibt Ihnen eine informelle Einführung in die Prädikatenlogik.

## Beispiele für Anwendungen in der Informatik

- Grundlage für die Entwicklung einer soliden “Theorie der Informatik”.
- Künstliche Intelligenz, Wissensrepräsentation, Expertensysteme.
- Allgegenwärtig in der Programmierung (z.B. “if ... then ... else...”-Befehle).
- Formale Verifikation der Korrektheit von Programmen.

## Lernziele

Sie kennen die Konzepte von

- Aussagen und Prädikaten.
- universeller und existenzieller Quantifikation.

Sie verstehen wie

- durch Implikation, Äquivalenz, Negation, Konjunktion und Disjunktion neue Aussagen und Prädikate aus bereits bestehenden gewonnen werden.
- durch Quantifikation von Prädikaten neue Aussagen und Prädikate gewonnen werden.

Sie sind in der Lage

- natürlichsprachliche (mathematische) Aussagen in der Sprache der Prädikatenlogik zu formalisieren.
- mittels Fallunterscheidung, Widerspruchsargumenten und Kontraposition einfache mathematische Tatsachen zu beweisen.

Sie bewerten

- einfache Beweise und Argumente bezüglich ihrer Korrektheit und Stringenz.

### Literatur und Links

Ergänzende Literatur:

- [3] Kapitel 1.2 bis 1.4.
- [2] Kapitel 2.
- [1] Kapitel 2.

Weiterführende Literatur:

- [5] ganzes Buch.

Nützliche Links:

- [http://de.wikipedia.org/wiki/Pr%C3%A4dikatenlogik\\_erster\\_Stufe](http://de.wikipedia.org/wiki/Pr%C3%A4dikatenlogik_erster_Stufe)
- <https://openlogicproject.org/>

### 1.1 Aussagen, Prädikate und Quantoren

Wir werden im folgenden Abschnitt auf pragmatische Art und Weise die grundlegenden Konzepte der Logik und Mathematik kennenlernen. Um nicht nur langweilige Beispiele machen zu können, werden wir in diesem Kapitel auf gewisse mathematische Begriffe wie z.b. “natürliche Zahlen” ( $0, 1, 2, \dots$ ) oder “Primzahlen” ( $2, 3, 5, 7, 11 \dots$ ) zurückgreifen, ohne diese vorher sauber eingeführt zu haben. Die Anschauung, welche Sie von der Schule mitbringen, sollte aber ausreichen um die Beispiele zu verstehen.

**Definition 1.** Unter einer *Aussage* wollen wir ein “sprachliches Gebilde” oder Ausdruck verstehen, welchem ein Wahrheitswert “wahr” oder “falsch” zugeordnet werden kann.

**Bemerkung 1.** Obwohl nach Definition jede Aussage einen eindeutigen Wahrheitswert besitzt, bedeutet dies nicht, dass dieser bekannt sein muss. Der Satz “es gibt unendlich viele Primzahlen” war beispielsweise bereits eine Aussage, bevor man wusste, dass er wahr ist.

**Beispiel 1.** Einige Beispiele für Aussagen mit ihren Wahrheitswerten:

- a) “ $3 + 4 = 106$ ” (falsch)
- b) “Jede natürliche Zahl ist entweder durch 2 oder durch 3 teilbar.” (falsch)
- c) “Es gibt unendlich viele natürliche Zahlen.” (wahr)

**Bemerkung 2.** Wir sagen, dass eine Variable  $x$  frei in einem Ausdruck  $A$  vorkommt, falls  $x$  weder für einen noch für eine Menge von konkreten Werten steht, sondern einen reinen “Platzhalter” darstellt. Beispiele in denen die Variable  $x$  frei vorkommt sind: “ $x < 3$ ” oder “ $x$  ist ein Tisch”. Im Gegensatz dazu kommt  $x$  in “alle  $x$ , die durch 4 teilbar sind, sind gerade” nicht frei vor, weil in dieser Aussage die Gesamtheit (Menge) aller möglichen Belegungen von  $x$  betrachtet wird. In einem Ausdruck können beliebig viele Variablen frei vorkommen und wir schreiben  $A(x, y, z, \dots)$ , um anzuzeigen, dass in einem Ausdruck  $A$  die Variablen  $x, y, z, \dots$  frei vorkommen.

**Definition 2.** Es sei  $n$  eine natürliche Zahl. Ein Ausdruck, in dem  $n$  viele Variablen frei vorkommen und der bei Belegung aller freien Variablen in eine Aussage übergeht, nennen wir ein  $n$ -stelliges Prädikat.

**Bemerkung 3.** Aussagen sind 0-stellige Prädikate.

**Bemerkung 4.** Ist  $A(x)$  ein Prädikat und ist  $y$  ein mathematisches Objekt (z.B.  $y = 17$ ) so, dass  $A(y)$  eine wahre Aussage ist, dann sagen wir, dass das Prädikat (manchmal auch die Eigenschaft)  $A$  auf  $y$  zutrifft. Das Prädikat  $x > 100$  trifft zum Beispiel auf die Zahl 232 zu, weil  $232 > 100$  eine wahre Aussage ist.

**Beispiel 2.** Einige Beispiele<sup>1</sup> für Prädikate:

- a)  $P(p) := “p \text{ ist eine Primzahl.}”$
- b)  $T(x) := “x \text{ ist eine durch 21 teilbare ganze Zahl.}”$
- c)  $G(r) := “r > 0”$
- d)  $Q(x, y) := “x^2 + 14x - 15 = y”$

Die Aussagen

$$\begin{array}{ccc} T(42) & P(7) & Q(2, 17) \\ T(357) & P(2) & Q(1, 0) \end{array}$$

sind alle wahr. Deshalb können wir, entsprechend der vorhergehenden Bemerkung, z.B. “ $T$  trifft auf 42” zu oder auch “7 hat die Eigenschaft  $P$ ” sagen.

**Beispiel 3.** Weitere Beispiele für Prädikate:

- $A(x, y) := x + y < 10$  ist ein zweistelliges Prädikat mit den freien Variablen  $x$  und  $y$ .
- $B(x, y, z) := x + y < z$  ist ein dreistelliges Prädikat.
- Wenn wir die Variable  $y$  in  $B$  mit dem Wert 10 belegen, dann erhalten wir das zweistellige Prädikat  $B(x, y, 10)$ , welches gleichbedeutend mit dem Prädikat  $A$  ist.

---

<sup>1</sup>Die Zeichenfolge “:=” steht für “ist definiert als” oder “ist per Definition gleich”.

### Junktoren

Aus gegebenen Aussagen lassen sich durch Verknüpfung neue komplexere Aussagen gewinnen. Betrachten wir zum Beispiel die Aussagen

$A := \text{“78 ist keine Primzahl”}$

und

$B := \text{“15 ist keine Primzahl”},$

so können wir eine neue Aussage, nennen wir sie  $C$ , betrachten.  $C$  soll ausdrücken, dass sowohl  $A$  als auch  $B$  wahr ist, d.h.

$C := \text{“78 ist keine Primzahl und 15 ist keine Primzahl”}$

oder etwas anders formuliert (aber mit gleichem Wahrheitswert)

$C := \text{“weder die 15 noch die 78 ist eine Primzahl”}.$

Wir werden nun einige abkürzende Schreibweisen einführen um bequem über solche zusammengesetzten Aussagen sprechen zu können.

**Definition 3.** Es seien  $A$  und  $B$  beliebige Prädikate. Wir führen folgende abkürzende Schreibweisen ein:

- $\neg A$  (gesprochen: Nicht  $A$ ) ist das Prädikat, welches (für jede Belegung) genau dann wahr ist, wenn  $A$  falsch ist.
- $A \wedge B$  (gesprochen:  $A$  und  $B$ ) ist das Prädikat, welches (für jede Belegung) genau dann wahr ist, wenn sowohl  $A$  als auch  $B$  wahr sind.
- $A \vee B$  (gesprochen:  $A$  oder  $B$ ) ist das Prädikat, welches (für jede Belegung) genau dann wahr ist, wenn  $A$  wahr ist oder  $B$  wahr ist (oder beide wahr sind).
- $A \Rightarrow B$  (gesprochen:  $A$  impliziert  $B$ ) ist das Prädikat, welches (für jede Belegung) genau dann wahr ist, wenn  $\neg A \vee B$  wahr ist.
- $A \Leftrightarrow B$  (gesprochen:  $A$  äquivalent  $B$ ) ist das Prädikat, welches (für jede Belegung) genau dann wahr ist, wenn  $A \Rightarrow B$  und  $B \Rightarrow A$  wahr sind.

Die Zeichen  $\neg, \Rightarrow, \wedge$  und  $\vee$  nennen wir *Junktoren*.

**Bemerkung 5.** Das Prädikat  $A \Rightarrow B$  besagt, dass in jedem Fall in dem  $A$  wahr ist auch  $B$  wahr sein muss. Die Äquivalenz zweier Prädikate besagt also, dass diese stets denselben Wahrheitswert haben. Umgangssprachlich wird oft vorausgesetzt, dass zwischen den

Prädikaten  $A$  und  $B$  ein “inhaltlicher Zusammenhang” bestehen muss, damit  $A \Rightarrow B$  gelten kann. Dies ist in der mathematischen Logik nicht der Fall. Die Aussagen

*Es gibt Einhörner  $\Rightarrow$  8 ist eine Primzahl*

und

*Spinat ist grün  $\Rightarrow$  2 ist eine Primzahl*

sind beispielsweise beide (mathematisch gesehen) wahr.

**Beispiel 4.** Gegeben sind die Aussagen  $A$  und  $B$ :

$A$  := “Alle Hasen haben lange Ohren.”

$B$  := “Es gibt Hasen mit kurzen Beinen.”

Es gilt:

- a)  $\neg A$  entspricht “Es gibt mindestens einen Hasen, der keine langen Ohren hat.”
- b)  $A \wedge \neg B$  entspricht “Alle Hasen haben lange Ohren und keine kurzen Beine.”
- c)  $A \Rightarrow B$  entspricht “Wenn alle Hasen lange Ohren haben, dann gibt es Hasen mit kurzen Beinen.”

**Übung 1.** Negieren Sie umgangssprachlich folgende Aussagen (so präzise wie möglich).

- a) Alle Autos haben vier Räder.
- b) Zwillinge haben stets die identische Haarfarbe.
- c) Es gibt flugunfähige Vögel.
- d) Alle Dinosaurier sind ausgestorben.

**Lösung.**

Wir werden nun einige Umformungsregeln betrachten, die unterschiedlich zusammengesetzte Aussagen, rein aufgrund ihrer logischen Struktur, als äquivalent deklarieren. Wir werden diese Regeln als evident betrachten und sie ohne Beweis übernehmen. Diese Regeln werden es uns erlauben mit Aussagen und Prädikaten zu “rechnen”.

**Bemerkung 6** (Junktorenregeln). Seien  $A, B$  und  $C$  beliebige Aussagen. Es gelten folgende Äquivalenzen

- Regel der doppelten Negation:

$$\neg\neg A \Leftrightarrow A$$

- Kommutativität:

$$A \wedge B \Leftrightarrow B \wedge A$$

$$A \vee B \Leftrightarrow B \vee A$$

- Assoziativität:

$$(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$$

$$(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$$

- Distributivität:

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

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

- Regeln von De Morgan:

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

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

**Beispiel 5** (Kontraposition). Wir können die eben aufgestellten Rechenregeln dazu verwenden um wiederum neue Tatsachen abzuleiten. Unter anderem folgt daraus das sogenannte Prinzip der *Kontraposition*. Dieses Prinzip besagt, dass  $A \Rightarrow B$  äquivalent ist zu  $\neg B \Rightarrow \neg A$ . Wollen wir dies nun mit unseren Rechenregeln nachvollziehen, so beginnen wir mit  $A \Rightarrow B$  und wenden nacheinander verschiedene Regeln an um schlussendlich  $\neg B \Rightarrow \neg A$  zu erhalten:

$$\begin{aligned} & A \Rightarrow B \\ \Leftrightarrow & \neg A \vee B && \text{(Definition von } A \Rightarrow B) \\ \Leftrightarrow & B \vee \neg A && \text{(Kommutativität)} \\ \Leftrightarrow & \neg\neg B \vee \neg A && \text{(Doppelte Negation)} \\ \Leftrightarrow & \neg B \Rightarrow \neg A && \text{(Definition von } \neg B \Rightarrow \neg A) \end{aligned}$$



## Quantoren

Quantoren sind Symbole anhand derer wir aus Prädikaten neue Prädikate oder Aussagen gewinnen können. Wir betrachten das Beispiel des Prädikates

$$A(x) := \text{“}x \text{ ist eine Primzahl und } x \text{ ist ein Teiler von 24“}$$

und die Aussage

$$B := \text{“es gibt eine Primzahl welche ein Teiler von 24 ist“}$$

mit anderen Worten,

$$B := \text{“es **existiert** ein } x \text{ mit } A(x)\text{“}.$$

Wir sagen, dass  $B$  aus  $A(x)$  durch existenzielle Quantifizierung über  $x$  entsteht.

Andererseits können wir aus dem Prädikat  $A(x)$  aber auch die (offensichtlich falsche) Aussage

$$C := \text{“alle Zahlen sind Primzahlen und ein Teiler von 24“}$$

konstruieren. Diese ist gleichbedeutend mit

$$C := \text{“**alle** Zahlen } x \text{ erfüllen } A(x)\text{“}.$$

Wir sagen, dass  $C$  aus  $A(x)$  durch universelle Quantifizierung entsteht<sup>2</sup>.

**Definition 4.** Es sei  $M$  eine Menge. Ist  $A(x)$  ein Prädikat, dann können wie folgt neue Prädikate geformt werden:

- $\forall x A(x)$  (gesprochen: Für alle  $x$  gilt  $A(x)$ ) trifft genau dann zu, wenn  $A$  auf jedes (mathematische) Objekt zutrifft.
- $\forall x \in M A(x)$  (gesprochen: Für alle  $x$  aus  $M$  gilt  $A(x)$ ) trifft genau dann zu, wenn  $A$  auf jedes Element aus  $M$  zutrifft.
- $\exists x A(x)$  (gesprochen: Es gibt ein  $x$  mit  $A(x)$ ) trifft genau dann zu, wenn es (mindestens) ein Objekt gibt, auf welches  $A$  zutrifft.
- $\exists x \in M A(x)$  (gesprochen: Es gibt ein  $x$  aus  $M$  mit  $A(x)$ ) trifft genau dann zu, wenn es (mindestens) ein Element aus  $M$  gibt, auf welches  $A$  zutrifft.

Die Symbole  $\forall$  und  $\exists$  heissen *Allquantor* und *Existenzquantor*.

**Bemerkung 7.** Prädikate von der Form  $\forall x \forall y A(x, y)$  und  $\exists x \exists y A(x, y)$  kürzen wir mit  $\forall x, y A(x, y)$  und  $\exists x, y A(x, y)$  ab.

---

<sup>2</sup>Obwohl in den Aussagen  $B$  und  $C$  formal die Variable  $x$  vorkommt, steht sie nicht als Platzhalter für ein einzusetzendes Objekt, sondern “läuft” über die Gesamtheit aller möglichen Objekte. Wir sagen, dass die Variable nicht frei sondern durch einen Quantor gebunden ist.

**Bemerkung 8.** Ein  $n$ -stelliges Prädikat wird durch Quantifizierung (einer freien Variable) zu einem neuen  $n - 1$  stelligen Prädikat.

**Beispiel 6.** Einige quantifizierte Aussagen mit ihren Wahrheitswerten:

- a) Es sei  $S$  die Menge aller Schweine und  $R(x)$  das Prädikat “ $x$  ist rosa”. Es gilt

$$“\exists x \in S R(x)” \Leftrightarrow “\text{es gibt rosa Schweine}”.$$

Diese Aussage ist offensichtlich wahr. Wenn wir nun die Allquantifizierung betrachten, so erhalten wir

$$“\forall x \in S R(x)” \Leftrightarrow “\text{alle Schweine sind rosa}”.$$

Dies ist eine falsche Aussage, da etwa Wildschweine einerseits Elemente von  $S$  sind aber andererseits  $R$  nicht erfüllen, da sie nicht rosa sind.

- b) Wir wollen nun die Aussage

$$A := “\text{alle Informatiker können programmieren}”$$

mit Quantoren ausdrücken. Wir definieren dazu zuerst das Prädikat

$$B(x) := “x \text{ kann programmieren}”.$$

Wir haben nun zwei mögliche Vorgehensweisen. Einerseits können wir die Menge  $I$  aller Informatiker betrachten und kommen dann mittels der Aussage

$$\forall x \in I B(x)$$

zum Ziel. Andererseits können wir auch  $A$  umformulieren als “alles was ein Informatiker ist kann programmieren” und erhalten die gewünschte Aussage mit einem uneingeschränkten Quantor

$$\forall x (x \in I \Rightarrow B(x)).$$

Diesen Zusammenhang zwischen eingeschränkten und uneingeschränkten Quantoren werden wir in der nächsten Bemerkung zu “Rechenregeln für Quantoren” allgemein formulieren.

**Bemerkung 9** (Quantorenregeln). Ist  $A(x)$  ein Prädikat und  $K$  eine Menge, so gelten folgende Äquivalenzen:

- a) Vertauschungsregel für unbeschränkte Quantoren

$$\forall x A(x) \Leftrightarrow \neg \exists x \neg A(x)$$

- b) Vertauschungsregel für beschränkte Quantoren

$$\forall x \in K A(x) \Leftrightarrow \neg \exists x \in K \neg A(x)$$

c) Beschränkter und unbeschränkter Allquantor

$$\forall x \in K A(x) \Leftrightarrow \forall x(x \in K \Rightarrow A(x))$$

d) Beschränkter und unbeschränkter Existenzquantor

$$\exists x \in K A(x) \Leftrightarrow \exists x(x \in K \wedge A(x))$$

**Beispiel 7.** Mit den Rechenregeln für Quantoren und den Rechenregeln für Junktoren können wir wieder neue Tatsachen (=Wahrheitswerte neuer Aussagen) herleiten. Als Beispiel betrachten wir das Duale zur Vertauschungsregel für unbeschränkte Quantoren, nämlich:

$$\exists x A(x) \Leftrightarrow \neg \forall x \neg A(x)$$

Wir beginnen also mit  $\exists x A(x)$  und erhalten durch Anwenden der Rechenregeln  $\neg \forall x \neg A(x)$ .

$$\begin{aligned} & \exists x A(x) \\ \Leftrightarrow & \neg \neg \exists x A(x) && \text{(Doppelte Negation)} \\ \Leftrightarrow & \neg(\neg \exists x A(x)) \\ \Leftrightarrow & \neg(\neg \exists x \neg(\neg A(x))) && \text{(Doppelte Negation)} \\ \Leftrightarrow & \neg(\forall x \neg A(x)) && \text{(Vertauschungsregel)} \end{aligned}$$

**Warnung.** Wir haben keine Distributionsregel mit Quantoren und Junktoren. Die Äquivalenzen

$$\forall x A(x) \vee \forall x B(x) \Leftrightarrow \forall x (A(x) \vee B(x))$$

und

$$\exists x A(x) \wedge \exists x B(x) \Leftrightarrow \exists x (A(x) \wedge B(x))$$

gelten im Allgemeinen **nicht**. Wir betrachten dazu als Gegenbeispiel die Aussagen

$$A(x) := \text{“}x \text{ ist eine gerade natürliche Zahl“}$$

und

$$B(x) := \text{“}x \text{ ist eine ungerade natürliche Zahl“}.$$

Die Aussage

$$\exists x A(x) \wedge \exists x B(x)$$

besagt also in diesem Fall, dass es mindestens eine gerade natürliche Zahl gibt und dass es ebenfalls mindestens eine ungerade natürliche Zahl gibt. Diese Aussage ist offensichtlich wahr. Die Aussage

$$\exists x (A(x) \wedge B(x))$$

besagt nun aber, dass es eine natürliche Zahl gibt, welche “gleichzeitig” gerade und ungerade ist, was offensichtlich falsch ist. Die beiden Aussagen sind also nicht äquivalent.

**Übung 2.** Es seien  $P(x)$  ein einstelliges und  $Q(y, z)$  ein zweistelliges Prädikat. Formalisieren Sie:

- a) Es gibt genau ein  $x$  mit  $P(x)$ .
- b) Es gibt mindestens zwei Dinge mit der Eigenschaft  $P$ .
- c) Es gibt höchstens ein  $x$  mit  $P(x)$ .
- d) Wenn  $P(x)$  und  $P(y)$  gilt, dann gilt stets auch  $Q(x, y)$ .
- e) Für kein  $x$  gilt  $Q(x, x)$ .

**Lösung.**

**Übung 3.** Geben Sie Prädikate  $P(x)$  und  $Q(x)$  an, so dass  $\forall x P(x) \vee \forall x Q(x)$  falsch, aber  $\forall x (Q(x) \vee P(x))$  wahr ist.

**Lösung.**

**Übung 4.** Gruppieren Sie folgende Aussagen so, dass in jeder Gruppe alle Aussagen äquivalent sind und keine äquivalenten Aussagen in verschiedenen Gruppen sind.

1.  $\forall x (P(x) \Rightarrow Q(x))$
2.  $\exists x (P(x) \Leftrightarrow Q(x))$
3.  $\forall x (Q(x) \Rightarrow P(x))$
4.  $\forall x (\neg P(x) \Rightarrow \neg Q(x))$
5.  $\forall x (\neg Q(x) \Rightarrow \neg P(x))$
6.  $\neg \exists x (\neg \neg Q(x) \wedge \neg P(x))$
7.  $\neg \exists x (P(x) \wedge \neg Q(x))$
8.  $\exists x (P(x) \wedge Q(x)) \vee \exists x (\neg P(x) \wedge \neg Q(x))$
9.  $\forall x \exists y (P(x) \wedge P(y))$

**Lösung.**

## 1.2 Grundlegende Beweistechniken

Wir wollen im Folgenden einige der elementarsten Standardbeweistechniken besprechen. Natürlich sollen diese Techniken in etwas komplexeren Beweisen auch beliebig kombiniert werden dürfen. Wir könnten beispielsweise zum Beweis einer Äquivalenz die eine Richtung durch Kontraposition und die andere Richtung direkt oder durch Widerspruch beweisen.

### Direkter Beweis einer Implikation

**Problemstellung:** Es gilt eine Aussage  $A \Rightarrow B$  zu beweisen.

**Lösungsstrategie:** Wir geben, basierend auf der Annahme, dass  $A$  wahr ist, *zwingende* Argumente für die Richtigkeit von  $B$ .

**Beispiel:** Wir zeigen, wenn  $x$  und  $y$  gerade (natürliche) Zahlen sind, dann ist auch  $x \cdot y$  gerade.

*Beweis.* Wir nehmen an  $x, y$  seien (irgendwelche) gerade natürliche Zahlen (Voraussetzung). Da  $x, y$  gerade sind, gibt es natürliche Zahlen  $n_x$  und  $n_y$  so, dass

$$x = 2 \cdot n_x \qquad y = 2 \cdot n_y$$

gilt. Für das Produkt  $x \cdot y$  gilt folglich

$$x \cdot y = (2 \cdot n_x) \cdot (2 \cdot n_y) = 2 \cdot (n_x \cdot 2 \cdot n_y)$$

und ist somit dass  $x \cdot y$  ein vielfaches von 2 also gerade ist.  $\square$

### Beweis durch Widerspruch

**Problemstellung:** Es gilt eine Aussage  $A$  zu beweisen.

**Lösungsstrategie:** Nehmen Sie an, die Aussage  $A$  wäre falsch und benützen Sie diese Annahme um einen Widerspruch herzuleiten. Leiten Sie also unter der Annahme der Falschheit von  $A$  eine Aussage her von der bereits bekannt ist, dass sie falsch ist oder im Widerspruch zur Annahme steht.

**Beispiel:**  $A$  := “Es gibt keine grösste natürliche Zahl”

*Beweis.* Wir nehmen an, dass es eine grösste natürliche Zahl gibt, wir nennen sie  $m$ . Wir wissen, dass für jede natürliche Zahl  $n$  gilt, dass einerseits  $n + 1$  ebenfalls eine natürliche Zahl ist und dass andererseits  $n < n + 1$  erfüllt ist. Wir wenden dies auf die natürliche Zahl  $m$  an und erhalten damit eine grössere natürliche Zahl (nämlich  $m + 1$ ). Dies steht jedoch im Widerspruch zu unserer ursprünglichen Annahme, dass  $m$  die grösste natürliche Zahl sei.  $\square$

### Beweis durch (Gegen-) Beispiel

**Problemstellung:** Es gilt zu zeigen, dass eine bestimmte Eigenschaft nicht auf alle Objekte (aus einem Kontext) zutrifft.

**Lösungsstrategie:** Geben Sie konkret ein Objekt an, welches die erwähnte Eigenschaft nicht besitzt.

**Beispiel:** “Nicht jede natürliche Zahl ist eine Quadratzahl<sup>3</sup>.”

*Beweis.* Weil die Funktion  $f(x) = x^2$  monoton ist (später mehr dazu) und weil  $1 \cdot 1 < 2 < 2 \cdot 2$  gilt, kann die Zahl 2 nicht als Quadrat von einer natürlichen Zahl geschrieben werden. Somit ist 2 das (oder ein) gesuchte Gegenbeispiel.  $\square$

---

<sup>3</sup>Von der Form  $x^2$  für eine geeignete natürliche Zahl  $x$ .

**Beweis durch Kontraposition**

**Problemstellung:** Es gilt eine Aussage von der Form  $A \Rightarrow B$  zu beweisen.

**Lösungsstrategie:** Beweisen Sie die Kontraposition  $\neg B \Rightarrow \neg A$ .

**Beispiel:** “Für jede natürliche Zahl  $n$  gilt:  $(n^2 + 1 = 1) \Rightarrow (n = 0)$ ”

*Beweis.* Ist  $n \neq 0$  so folgt, dass auch  $n^2 \neq 0$  gilt. Dies impliziert, dass für jede weitere natürliche Zahl  $m$  die Ungleichung  $n^2 + m \neq m$  erfüllt ist. Insbesondere gilt daher, dass (der Fall  $m = 1$ )  $n^2 + 1 \neq 1$  gilt.  $\square$

**Beweis einer Äquivalenz**

**Problemstellung:** Es gilt eine Aussage von der Form  $A \Leftrightarrow B$  zu beweisen.

**Lösungsstrategie:** Beweisen Sie  $B \Rightarrow A$  sowie  $A \Rightarrow B$ .

**Beispiel 1:** “Für jede natürliche Zahl  $n$  gilt:  $(n^2 + 1 = 1) \Leftrightarrow (n = 0)$ ”

*Beweis.* Wir haben in den vorhergehenden Beispielen bereits  $A \Rightarrow B$  bewiesen, wir müssen also nur noch  $B \Rightarrow A$  beweisen. Wir nehmen also  $B$  an, es gelte also  $n = 0$ . Draus folgt  $n^2 = n \cdot n = 0 \cdot 0 = 0$  und somit  $n^2 + 1 = 0 + 1 = 1$ .  $\square$

**Beispiel 2:** “Für jede natürliche Zahl  $n$  gilt:  $(n \text{ ist gerade}) \Leftrightarrow (n^2 \text{ ist gerade}).$ ”

*Beweis.* Wir beweisen zuerst  $(n \text{ ist gerade}) \Rightarrow (n^2 \text{ ist gerade})$ . Wir nehmen also an, dass  $n$  eine gerade natürliche Zahl ist. Daraus folgt, dass es eine weitere natürliche Zahl  $k$  mit  $n = 2 \cdot k$  gibt. Es folgt, dass

$$n^2 = n \cdot n = 2 \cdot k \cdot 2 \cdot k = 2 \cdot (k \cdot 2 \cdot k)$$

offenbar gerade ist.

Nun wollen wir noch die “Rückrichtung”  $(n^2 \text{ ist gerade}) \Leftarrow (n \text{ ist gerade})$  beweisen. Wir wollen diese Richtung durch Kontraposition beweisen und nehmen also an, dass  $n$  ungerade sei. Es folgt, dass es eine natürliche Zahl  $k$  mit  $2k + 1 = n$  gibt. Folglich gilt:

$$n^2 = (2k + 1)(2k + 1) = 4k^2 + 4k + 1 = \underbrace{4(k^2 + k)}_{\text{gerade}} + 1.$$

Also ist  $n^2$  ungerade.  $\square$

**Übung 5.** Beweisen Sie: Jeder (ganzzahlige) Geldbetrag von mindestens 4 Cents lässt sich allein mit Zwei- und Fünfcentstücken bezahlen.

*Hinweis:* Machen Sie eine Fallunterscheidung ob der zu bezahlende Betrag gerade oder ungerade ist.

**Lösung.**

**Übung 6.** Beweisen Sie, dass man  $\sqrt{2}$  nicht als Bruch schreiben kann.  
*Hinweis:* Wenden Sie ein Widerspruchsargument an.

**Lösung.**





## 2 Syntax und Semantik am Beispiel der formalen Aussagenlogik

### Prolog

Wir betrachten Wörter, die aus den Zeichen  $z, P, G$  gebildet werden können, also zum Beispiel  $zzzPPGPGP$ ,  $zzz$  oder  $zzPzzzGzzzzzz$ . Da uns aber nicht alle diese Wörter interessieren, schränken wir uns auf “zulässige” Wörter ein, die wir folgendermassen definieren: Ein Wort ist zulässig, wenn

- genau ein  $G$  und ein  $P$  darin vorkommen und das  $P$  vor dem  $G$  vorkommt.

Zulässige Wörter (wir nennen diese jetzt auch  $zPG$ -Wörter) sind also von der Form

$$\dots P \dots G \dots$$

wobei “ $\dots$ ” für jeweils eine beliebige (nicht notwendigerweise von null verschiedener) Anzahl  $z$  steht. Beispiele von zulässigen Wörtern sind  $zzzPzzGzzzzzz$ ,  $PzG$  oder  $PzGz$ . Die Regeln, die wir eingeführt haben, um zulässige von unzulässigen Wörtern zu unterscheiden, sind Teil der *Syntax* unserer  $zPG$ -Sprache. Obwohl wir jetzt eine primitive “Grammatik” für unsere Sprache haben, bleibt völlig unklar was wir mit dieser Sprache aussagen wollen – was die Bedeutung oder *Semantik* von  $zPG$ -Wörtern ist. Wie können wir also zulässige Wörter interpretieren? Haben Sie eine Idee? Schauen wir was passiert, wenn wir  $zPG$ -Wörter wie Aussagen als Wahrheitswerte “wahr” oder “falsch” interpretieren. Wir betrachten die (partielle) Zuordnung

<b><math>zPG</math>-Wort</b>		<b>Wahrheitswert</b>
$zzzPzGzzzz$	$\longleftrightarrow$	falsch
$PG$	$\longleftrightarrow$	wahr
$zPzGzz$	$\longleftrightarrow$	wahr
$PzzGz$	$\longleftrightarrow$	falsch

Haben Sie eine Idee, wie wir diese Zuordnung von  $zPG$ -Wörtern zu Wahrheitswerten vervollständigen können? Nehmen Sie sich einen Moment Zeit darüber nachzudenken, bevor Sie weiter lesen. Wenn wir an elementare Arithmetik denken, so könnten<sup>1</sup> wir in einem  $zPG$ -Wort zum Beispiel die Symbole  $P, G$  als  $+$  und  $=$  und Blöcke von der Form  $z \dots z$  als unär-codierte natürliche Zahlen interpretieren. Unter dieser Interpretation ergibt sich das folgende Bild:

---

<sup>1</sup>Das heisst nicht, dass es keine anderen “sinnvollen” Interpretationen von  $zPG$ -Wörtern gibt, wir haben uns hier willkürlich festgelegt.

---

zPG-Wort		Wahrheitswert
zzzPzGzzz	$\longleftrightarrow$	$3 + 1 = 3$ (falsch)
PG	$\longleftrightarrow$	$0 + 0 = 0$ (wahr)
zPzGzz	$\longleftrightarrow$	$1 + 1 = 2$ (wahr)
PzzGz	$\longleftrightarrow$	$0 + 2 = 1$ (falsch)

Nun erweitern wir unsere zPG-Sprache (die Menge aller zPG-Wörter) zu einem “formalen System”, indem wir rein syntaktische Regeln angeben “die zPG-Reduktion”, um aus zPG-Wörtern neue zPG-Wörter zu generieren.

- Ist das zu reduzierende Wort von der Form  $z \dots Pz \dots Gzz \dots$ , dann reduzieren wir nach  $\dots P \dots G \dots$ .
- Ist das zu reduzierende Wort von der Form  $Pz \dots Gz \dots$ , dann reduzieren wir nach  $P \dots G \dots$ .
- Ist das zu reduzierende Wort von der Form  $z \dots PGz \dots$ , dann reduzieren wir nach  $\dots PG \dots$ .
- Trifft keiner der oben genannten Fälle zu, dann ist das Wort vollständig reduziert.

Was passiert, wenn wir ein “wahres” zPG-Wort reduzieren? Was passiert, wenn wir ein zPG-Wort reduzieren, das nicht “wahr” ist?

Die wahren zPG-Wörter sind genau diejenigen, deren vollständig reduzierte Form das Wort PG ist.

Wir können also sagen, dass eine Reduktion eines zPG-Wortes nach PG einem formalen “Beweis” im zPG-System vom ursprünglichen Wort entspricht. Eine vollständige Reduktion, die in einem Wort endet, welches von PG verschieden ist, ist in diesem Sinne eine “formale Verwerfung” vom Ursprungswort. Insbesondere haben wir einen syntaktischen Kalkül (Reduktion terminiert immer), der von einem zPG-Wort entscheidet, ob dieses wahr ist. Man sagt in diesem Fall, dass das System *entscheidbar* und vollständig (bzgl. der gegebenen Semantik) ist. Dies ist eine starke Eigenschaft, die für kompliziertere Systeme im Allgemeinen nicht gilt.

Noch ein paar Beispiele für die syntaktische und die semantische Ebene:

Syntax		Semantik
Partitur	$\longleftrightarrow$	Musik (Schallwellen)
Java Code	$\longleftrightarrow$	Verhalten eines Computers
Terme einer math. Theorie	$\longleftrightarrow$	Math. Objekte
Aussagenlogische Formeln	$\longleftrightarrow$	Boolesche Funktionen
Peano-Axiome	$\longleftrightarrow$	Die Struktur $(\mathbb{N}, +, \cdot)$
Feynman-Diagramm	$\longleftrightarrow$	Wechselwirkungen

### Beispiele für Anwendungen in der Informatik

- Künstliche Intelligenz, Wissensrepräsentation und Expertensysteme
- Theoretische Informatik ( $P = NP$ -Frage, SAT, ...)
- Regeltechnik und Simulation

### Lernziele

Sie kennen die

- Syntax der Aussagenlogik.
- Semantik der Aussagenlogik.

Sie verstehen

- Wie die Begriffe Syntax und Semantik zusammenhängen.
- Was der Wahrheitswert einer aussagenlogischen Formel ist.

Sie sind in der Lage

- von aussagenlogischen Formeln zu entscheiden, ob diese allgemeingültig, erfüllbar oder unerfüllbar sind.
- Wahrheitstabellen auch für kompliziertere Formeln aufzustellen und daraus Schlüsse über den Wahrheitswert der Formel zu ziehen.
- Aussagenlogische Formeln in verschiedene Normalformen zu überführen.

### Literatur und Links

Wie im ersten Kapitel.

## 2.1 Syntax der Aussagenlogik

**Definition 5.** Das *Alphabet der Aussagenlogik* (auch Zeichenvorrat genannt) besteht aus:

- Konstanten  $\top$  und  $\perp$ .
- Variablen  $p, q, r, s, \dots, p_0, p_1, p_2, \dots$
- Klammern  $(, )$

- Junktoren  $\neg, \wedge, \vee, \rightarrow$

Die Menge der Variablen bezeichnen wir mit  $\mathbb{V}$ .

Nachdem wir nun die Zeichen festgelegt haben, aus welchen die “Wörter der Aussagenlogik” zusammengesetzt sind, werden wir in der nächsten Definition, die für uns interessanten Wörter festlegen. Wir definieren, also im Sinn vom einführenden Beispiel, die “zulässigen Wörter” (genannt Formeln) der Aussagenlogik.

**Definition 6.** Jede Variable und jede Konstante ist eine *atomare Formel*. Wir bezeichnen die Menge aller atomaren Formeln mit  $\mathbb{A} := \{\perp, \top, p, q, r, s, \dots, p_0, p_1, p_2, \dots\}$ . Die *Formeln* der Aussagenlogik sind dann wie folgt gegeben:

- Alle atomaren Formeln sind Formeln.
- Sind  $P$  und  $Q$  schon Formeln, dann auch:  $(P \wedge Q)$ ,  $(P \vee Q)$ ,  $(P \rightarrow Q)$  und  $\neg P$ .

Wir schreiben  $\mathbb{F}$  für die Menge aller aussagenlogischen Formeln.

**Bemerkung 10.** Ist eine Formel von einem Klammernpaar umgeben, dann lassen wir die äussersten Klammern zugunsten einer besseren Lesbarkeit weg; wir schreiben beispielsweise  $(p_0 \vee p_1) \wedge p_3$  anstelle von  $((p_0 \vee p_1) \wedge p_3)$ . Des Weiteren setzen wir folgende Operatorrangfolge fest: Die Negation bindet stärker als die Konjunktion und die Disjunktion, die wiederum stärker binden als die Implikation.

**Beispiel 8.** Einige aussagenlogische Formeln:

$$p \vee (p \rightarrow \neg(q \wedge p)) \quad p \wedge \neg p \quad p \rightarrow (q \rightarrow p) \quad \neg(p \vee \neg q)$$

Einige Zeichenreihen, die *keine* aussagenlogische Formeln sind:

$$\neg \rightarrow p \quad \forall x p(x) \quad \text{“es regnet”}$$

## 2.2 Semantik der Aussagenlogik

Wir wollen jeder aussagenlogischen Formel nun eine Bedeutung zuordnen. Am bequemsten wäre es, wenn wir jeder Formel direkt einen der Wahrheitswert *wahr* oder *falsch* zuordnen könnten. Bei einigen Formeln gelingt dies tatsächlich ohne Probleme;  $\neg p \vee p$  beispielsweise ist immer wahr, egal ob  $p$  selbst wahr oder falsch ist. Für andere Formeln ist das aber weniger klar; der Wahrheitswert der Formel  $p_1 \vee p_4$  hängt von den Wahrheitswerten der Formeln  $p_1$  und  $p_4$  ab. Wir haben also folgendes Problem:

- Bevor wir die Wahrheitswerte von komplizierten Formeln bestimmen/definieren können, müssen wir die Wahrheitswerte der atomaren Formeln schon bestimmt haben.
- Die Zuordnung von Wahrheitswerten zu atomaren Formeln ist völlig willkürlich; es gibt keinen Grund, dass beispielsweise die Formel  $p_1$  "weniger wahr" als die Formel  $p_4$  sein soll.

Wir stellen also fest, dass wir einer aussagenlogischen Formel nur einen Wahrheitswert *bezüglich* einer Belegung der atomaren Formeln mit Wahrheitswerten geben können. Zum Beispiel, wenn wir die Variablen  $p_1$  und  $p_4$  beide mit dem Wahrheitswert *false* belegen, dann hat die Formel  $p_1 \vee p_4$  *unter dieser Belegung* ebenfalls den Wahrheitswert *false*.

**Definition 7.** Eine *Belegung* ist eine Zuordnung von Variablen zu Wahrheitswerten, d.h. eine Funktion  $B : \mathbb{V} \rightarrow \{\text{true}, \text{false}\}$ .

Nun werden wir sehen, wie man ausgehend von einer Belegung jeder aussagenlogischen Formel einen Wahrheitswert zuordnen kann. Bevor wir uns der formalen Definition widmen, skizzieren wir unser Vorgehen exemplarisch an der Formel  $(p \vee q) \wedge \neg p$ . Nehmen wir an, dass  $B$  eine Belegung mit  $B(p) = \text{true}$  und  $B(q) = \text{false}$  sei. Wir wollen nun den Wahrheitswert von  $(p \vee q) \wedge \neg p$  sinnvoll definieren. Wegen  $B(p) = \text{true}$  sollte die Formel  $\neg p$  den Wahrheitswert *false* haben, und die Formel  $p \vee q$  den Wert *true* erhalten. Zusammenfassend sehen wir, dass die Formel  $\underbrace{(p \vee q)}_X \wedge \underbrace{\neg p}_Y$  von der Form  $X \wedge Y$  ist wobei

$X$  den Wahrheitswert *true* und  $Y$  den Wahrheitswert *false* hat. Es ist daher sinnvoll den Wahrheitswert von  $(p \vee q) \wedge \neg p$  auf *false* zu setzen.

Nun zur formalen Definition

**Definition 8.** Es sei eine Belegung  $B$  gegeben. Die Funktion  $\hat{B}$  ist die Funktion, die jeder aussagenlogischen Formel ihren Wahrheitswert bezüglich der Belegung  $B$  zuordnet, d.h. die Funktion  $\hat{B} : \mathbb{F} \rightarrow \{\text{false}, \text{true}\}$  ist gegeben durch:

- $\hat{B}(\perp) = \text{false}$  und  $\hat{B}(\top) = \text{true}$ .
- Für beliebige Variablen  $v$  gilt  $\hat{B}(v) = B(v)$ .
- Für beliebige Formeln  $F$  und  $G$  gilt

$$\hat{B}(F \wedge G) = \begin{cases} \text{true} & \text{falls } \hat{B}(F) = \text{true} \text{ und } \hat{B}(G) = \text{true} \\ \text{false} & \text{sonst.} \end{cases}$$

- Für beliebige Formeln  $F$  und  $G$  gilt

$$\hat{B}(F \vee G) = \begin{cases} \text{true} & \text{falls } \hat{B}(F) = \text{true} \text{ oder } \hat{B}(G) = \text{true} \\ \text{false} & \text{sonst.} \end{cases}$$

- Für beliebige Formeln  $F$  gilt

$$\hat{B}(\neg F) = \begin{cases} \text{true} & \text{falls } \hat{B}(F) = \text{false} \\ \text{false} & \text{sonst.} \end{cases}$$

- Für beliebige Formeln  $F$  und  $G$  gilt  $\hat{B}(F \rightarrow G) = \hat{B}(\neg F \vee G)$ .

**Bemerkung 11.** Die Junktoren können wir auch als boolesche Funktionen (Funktionen, die Wahrheitswerte verarbeiten) anschauen:

$$\text{or}(x, y) = \begin{cases} \text{true} & \text{falls } x = \text{true} \text{ oder } y = \text{true} \\ \text{false} & \text{sonst} \end{cases}$$

$$\text{and}(x, y) = \begin{cases} \text{true} & \text{falls } x = \text{true} \text{ und } y = \text{true} \\ \text{false} & \text{sonst} \end{cases}$$

$$\text{not}(x) = \begin{cases} \text{true} & \text{falls } x = \text{false} \\ \text{false} & \text{sonst} \end{cases}$$

Durch diese Interpretation können wir die obige Definition etwas knapper formulieren:

- $\hat{B}(F \wedge G) = \text{and}(\hat{B}(F), \hat{B}(G))$
- $\hat{B}(F \vee G) = \text{or}(\hat{B}(F), \hat{B}(G))$
- $\hat{B}(\neg F) = \text{not}(\hat{B}(F))$

Mithilfe dieser Darstellung können wir, wenn eine Belegung  $B$  gegeben ist, den Wahrheitswert einer beliebigen aussagenlogischen Formel unter der Belegung  $B$  “berechnen”.

**Beispiel 9.** Es sei eine Belegung  $B$  gegeben, die  $B(p_n) = \text{true}$  genau dann erfüllt, wenn

$n$  eine gerade Zahl ist. Wir berechnen den Wahrheitswert von  $(p_4 \rightarrow (p_5 \rightarrow p_6)) \vee p_{13}$ .

$$\begin{aligned}
 \hat{B}((p_4 \rightarrow (p_5 \rightarrow p_6)) \vee p_{13}) &= \text{or}(\hat{B}(p_4 \rightarrow (p_5 \rightarrow p_6)), \underbrace{\hat{B}(p_{13})}_{\text{false}}) \\
 &= \hat{B}(p_4 \rightarrow (p_5 \rightarrow p_6)) \\
 &= \hat{B}(\neg p_4 \vee (p_5 \rightarrow p_6)) \\
 &= \text{or}(\hat{B}(\neg p_4), \hat{B}(p_5 \rightarrow p_6)) \\
 &= \text{or}(\underbrace{\text{not}(\hat{B}(p_4))}_{\text{true}}, \hat{B}(\neg p_5 \vee p_6)) \\
 &= \text{or}(\text{false}, \hat{B}(\neg p_5 \vee p_6)) \\
 &= \hat{B}(\neg p_5 \vee p_6) \\
 &= \text{or}(\hat{B}(\neg p_5), \underbrace{\hat{B}(p_6)}_{\text{true}}) \\
 &= \text{true}
 \end{aligned}$$

**Übung 7.** Von einer Belegung  $B : \mathbb{V} \rightarrow \{\text{false}, \text{true}\}$  seien folgende Werte bekannt:

$$\begin{aligned}
 B(p) &= B(q) = B(r) = B(s) = \text{true} \\
 B(u) &= B(v) = \text{false}
 \end{aligned}$$

Bestimmen Sie  $\hat{B}$  von folgenden Formeln:

- a)  $p \rightarrow s$
- b)  $(u \rightarrow r) \wedge s$
- c)  $v \vee ((r \rightarrow s) \wedge u)$

**Lösung.**



### Wahrheitstabellen

Um den Wahrheitswert einer Formel  $F$  bezüglich einer Belegung  $B$  zu bestimmen, genügt es die Werte  $B(x)$  für alle Variablen  $x$ , die in  $F$  vorkommen zu kennen. Da eine Formel immer nur eine endliche Anzahl an Variablen enthält, erlaubt uns dieser Umstand für jede Formel eine Tabelle aufstellen, die den Wahrheitsgehalt dieser Formel bezüglich jeder möglichen Belegung darstellt. Wir brauchen dazu den Begriff einer Teilformel.

**Definition 9.** Der Begriff einer *Teilformel* einer Formel  $F$  ist wie folgt gegeben:

- Wenn  $F$  eine atomare Formel ist, dann ist besitzt  $F$  nur die Teilformel  $F$  (also “sich selbst”).
- Wenn  $F$  von der Form  $A \vee B$ ,  $A \wedge B$  oder  $A \rightarrow B$  ist, dann besitzt  $F$  als Teilformeln, neben  $F$  selbst, alle Teilformeln von  $A$  und  $B$ .
- Wenn  $F$  von der Form  $\neg A$  ist, dann besitzt  $F$  als Teilformeln, neben  $F$  selbst, alle Teilformeln von  $A$ .

Eine *echte* Teilformel einer Formel  $F$  ist eine von  $F$  verschiedene Teilformel von  $F$ .

**Beispiel 10.** Die Teilformeln der Formel  $r \rightarrow (s \wedge p)$  sind  $r, s, p, s \wedge p$  sowie  $r \rightarrow (s \wedge p)$ .

**Definition 10.** In einer *Wahrheitstabelle einer Formel  $F$*  entspricht jede Spalte einer Teilformel von  $F$  und jede Zeile einer Belegung der in  $F$  vorkommenden Variablen. Es gelten folgende Bedingungen:

- In der Spalte einer Formel steht in jeder der folgenden Zeilen der Wahrheitswert dieser Formel unter der der Zeile entsprechenden Belegung.
- Steht in einer Spalte eine Formel, dann kommen alle echten Teilformeln dieser Formel in Spalten weiter links vor.
- Der letzte Eintrag der ersten Zeile ist die Formel  $F$ .

**Bemerkung 12.** Wahrheitstabellen sind bis auf die Reihenfolge der Zeilen sowie der Reihenfolge von Teilformeln eindeutig.

**Bemerkung 13.** Für eine bessere Übersicht werden in Wahrheitstabellen anstelle der Wahrheitswerte `true` und `false` oft Abkürzungen 1 und 0 verwendet.

**Beispiel 11.** Die Teilformeln von der Formel  $p_0 \rightarrow (q \vee p_1)$  sind:  $p_0, p_1, q, (q \vee p_1)$  und  $p_0 \rightarrow (q \vee p_1)$ . Eine vollständige Wahrheitstabelle von  $p_0 \rightarrow (q \vee p_1)$  ist:

$p_0$	$q$	$p_1$	$q \vee p_1$	$p_0 \rightarrow (q \vee p_1)$
0	0	0	0	1
0	0	1	1	1
0	1	0	1	1
0	1	1	1	1
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

**Bemerkung 14.** Man kann Wahrheitstabellen auch zur Darstellung von logischen Operatoren<sup>2</sup> benützen. Beispielhaft geben wir die Wahrheitstabellen für die Operatoren (Junktoren)  $\vee$ ,  $\wedge$ ,  $\rightarrow$ ,  $\neg$  an.

$F$	$G$	$F \wedge G$	$F$	$G$	$F \vee G$	$F$	$G$	$F \rightarrow G$	$F$	$\neg F$
0	0	0	0	0	0	0	0	1	0	1
0	1	0	0	1	1	0	1	1	1	0
1	0	0	1	0	1	1	0	0	1	0
1	1	1	1	1	1	1	1	1	1	0

## Semantische Eigenschaften

**Definition 11.** Eine aussagenlogische Formel  $A$  heisst

- *Gültig* oder *wahr* unter einer Belegung  $B$ , falls  $\hat{B}(A) = \text{true}$ .
- *Allgemeingültig*, wenn sie unter jeder Belegung gültig ist.
- *Widerlegbar*, wenn es mindestens eine Belegung gibt, unter der  $A$  nicht gültig ist.
- *Erfüllbar*, wenn es mindestens eine Belegung gibt, unter der  $A$  gültig ist.
- *Unerfüllbar*, wenn  $A$  nicht erfüllbar ist.

**Bemerkung 15.** Die eingeführten Begriffe können auch anhand von Wahrheitstabellen verstanden werden. Eine aussagenlogische Formel  $A$  ist

- Allgemeingültig, wenn in einer Wahrheitstabelle von  $A$  in der letzten Spalte alle Einträge **true** sind.
- Erfüllbar, wenn in einer Wahrheitstabelle von  $A$  in der letzten Spalte mindestens einer der Einträge **true** ist.

---

<sup>2</sup>Funktionen, die aus aussagenlogischen Formeln neue aussagenlogische Formeln generieren.

- Unerfüllbar, wenn in einer Wahrheitstabelle von  $A$  in der letzten Spalte alle Einträge **false** sind.
- Widerlegbar, wenn in einer Wahrheitstabelle von  $A$  in der letzten Spalte mindestens einer der Einträge **false** ist.

**Beispiel 12.** Einige allgemeingültige Formeln:

$$p \vee \neg p \qquad p \rightarrow (q \rightarrow p) \qquad F \rightarrow F \qquad .$$

Einige erfüllbare nicht allgemeingültige Formeln:

$$p_1 \vee (p_2 \vee p_3) \qquad p_3 \qquad p \rightarrow q$$

Einige unerfüllbare Formeln:

$$(p_1 \rightarrow \neg p_1) \wedge (\neg p_1 \rightarrow p_1) \qquad \neg p_3 \wedge p_3 \qquad \neg(F \rightarrow F)$$

Welche der Formeln

$$(p_1 \rightarrow (p_2 \vee p_1)) \vee (\neg p_1 \vee (p_2 \wedge p_1)) \qquad \neg p_3 \wedge p_3 \qquad \neg(F \rightarrow \neg F)$$

sind allgemeingültig, welche erfüllbar und welche unerfüllbar?

**Bemerkung 16.** Eines der grössten ungelösten Probleme der (theoretischen) Informatik ist die Frage, ob es einen “effizienten” Algorithmus gibt, der von jeder aussagenlogischen Formel entscheidet, ob sie erfüllbar ist oder nicht. Diese Problemstellung wird mit **SAT** (von engl. **satisfiability**) bezeichnet. Die Relevanz dieser Frage kommt daher, dass sich das  $P \stackrel{?}{=} NP$  Problem (die Frage, ob zwei der wichtigsten Komplexitätsklassen übereinstimmen) darauf reduzieren lässt.

**Übung 8.** Zeigen Sie: Eine aussagenlogische Formel  $F$  ist genau dann allgemeingültig, wenn  $\neg F$  unerfüllbar ist.

**Lösung.**

**Übung 9.** Ist die Behauptung korrekt, dass jede Formel genau dann erfüllbar ist, wenn ihre Negation nicht erfüllbar ist? Begründen Sie Ihre Antwort.

**Lösung.**

**Übung 10.** Geben Sie zwei erfüllbare Formeln  $F$  und  $G$  an, so dass die Formel  $F \wedge G$  nicht erfüllbar ist.

**Lösung.**

**Definition 12.** Es seien  $F$  und  $G$  beliebige aussagenlogische Formeln. Wir sagen

- $F$  ist eine *Konsequenz von  $G$* , falls  $F$  unter jeder Belegung wahr ist unter der  $G$  wahr ist.
- $F$  und  $G$  sind *logisch äquivalent*, wenn  $G$  und  $F$  unter jeder Belegung denselben Wahrheitswert annehmen.

Sind  $F$  und  $G$  äquivalente Formeln, dann schreiben wir  $F \equiv G$ .

**Bemerkung 17.** Zwei aussagenlogische Formeln sind genau dann äquivalent, wenn beide Formeln von der jeweils anderen eine Konsequenz sind.

Wir können nun, ähnlich wie wir dies im ersten Kapitel informell für die Prädikatenlogik getan haben (als Konsequenz davon!), einige grundlegende logische Äquivalenzen nachweisen.

**Bemerkung 18.** Mit einem *Satz* bezeichnet man in der Mathematik eine zur Theoriebildung wichtige oder in der Anwendung nützliche Erkenntnis, die durch einen Beweis belegt wird.

**Satz 1.** Sind  $F, G$  und  $H$  beliebige aussagenlogische Formeln, dann gelten folgende Äquivalenzen:

- *Gesetz der doppelten Negation:*  $\neg\neg F \equiv F$
- *Absorption:*  $F \wedge F \equiv F$  und  $F \vee F \equiv F$
- *Kommutativität:*  $F \wedge G \equiv G \wedge F$  und  $F \vee G \equiv G \vee F$
- *Assoziativität:*  $F \wedge (G \wedge H) \equiv (F \wedge G) \wedge H$
- *Assoziativität:*  $F \vee (G \vee H) \equiv (F \vee G) \vee H$
- *Distributivität:*  $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$
- *Distributivität:*  $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$
- *De Morgan:*  $\neg(F \wedge G) \equiv \neg F \vee \neg G$
- *De Morgan:*  $\neg(F \vee G) \equiv \neg F \wedge \neg G$

- *Kontraposition:*  $F \rightarrow G \equiv \neg G \rightarrow \neg F$

*Beweis.* Wir müssen für jede der behaupteten Äquivalenzen nachweisen, dass die genannten Formeln unter jeder Belegung denselben Wahrheitswert haben. Wenn wir also von einer beliebigen Belegung  $B$  ausgehen, dann müssen wir, um eine Äquivalenz von der Form  $X \equiv Y$  nachzuweisen, bloss zeigen, dass  $\hat{B}(X) = \hat{B}(Y)$  gilt.

- Doppelte Negation folgt aus  $\text{not}(\text{not}(x)) = x$ :

$$\hat{B}(\neg\neg F) = \text{not}(\hat{B}(\neg F)) = \text{not}(\text{not}(\hat{B}(F))) = \hat{B}(F).$$

- Absorption folgt sofort aus  $\text{and}(x, x) = \text{or}(x, x) = x$ .
- Kommutativität folgt sofort aus  $\text{or}(x, y) = \text{or}(y, x)$  und  $\text{and}(x, y) = \text{and}(y, x)$ .
- Für Assoziativität, Distributivität und DeMorgan siehe Fallunterscheidung an der Tafel.

□

**Bemerkung 19.** Mit *Theorem* bezeichnet man in der Mathematik besonders wichtige Sätze.

Das nächste Theorem schlägt eine wichtige Brücke zwischen Syntax und Semantik der Aussagenlogik, indem es die logische Konsequenz (Semantik) in Beziehung zur Implikation (Syntax) setzt. Man kann das Theorem dahingehend interpretieren, dass die Implikation  $\rightarrow$  eine adäquate Formalisierung des Folgerungsbegriffes  $\Rightarrow$  vom ersten Kapitel darstellt.

**Theorem 1** (Folgerungstheorem). *Sind  $F$  und  $G$  aussagenlogische Formeln, dann gelten:*

- $G$  ist genau dann eine Konsequenz von  $F$ , wenn die Formel  $F \rightarrow G$  allgemeingültig ist.*
- $F$  und  $G$  sind genau dann logisch äquivalent, wenn die Formel  $F \rightarrow G \wedge G \rightarrow F$  allgemeingültig ist.*

*Beweis.* Wir behandeln zuerst die Behauptung *i*).

$$\begin{aligned} F \rightarrow G \text{ allgemeingültig} &\Leftrightarrow \forall B(\hat{B}(F \rightarrow G) = \text{true}) \\ &\Leftrightarrow \forall B(\hat{B}(\neg F \vee G) = \text{true}) \\ &\Leftrightarrow \forall B(\neg \hat{B}(F) = \text{true} \quad \underbrace{\vee}_{\text{“oder” der Prädikatenlogik}} \quad \hat{B}(G) = \text{true}) \\ &\Leftrightarrow \forall B(\hat{B}(F) = \text{true} \Rightarrow \hat{B}(G) = \text{true}) \\ &\Leftrightarrow G \text{ ist Konsequenz von } F \end{aligned}$$

Die Behauptung *ii*) folgt direkt aus dem ersten Teil.

□

**Übung 11.** Zeigen Sie mit der Methode der Wahrheitstabellen, dass die Formeln  $p \rightarrow q$  und  $q \rightarrow p$  nicht äquivalent sind.

**Lösung.**

### Normalformen

**Bemerkung 20.** Ausdrücke von der Form  $F_1 \vee \dots \vee F_n$  oder  $F_1 \wedge \dots \wedge F_n$  stehen stellvertretend für alle möglichen Formeln die durch Klammersetzung aus ihnen gebildet werden können. Für den Wahrheitswert der Formeln ist die genaue Klammerung, wegen der Assoziativität unwichtig.

**Definition 13.** *Literale* sind atomare Formeln oder negierte atomare Formeln.

**Beispiel 13.** Beispiele für Literale:  $p$ ,  $\neg q$ ,  $\neg p_{34}$ .

**Definition 14.** Eine aussagenlogische Formel ist:

- In *Negationsnormalform*(NNF), wenn alle Negationen in Literalen vorkommen und wenn keine Implikationen ( $\rightarrow$ ) vorkommen.

- In *disjunktiver Normalform*(DNF), wenn sie von der Form

$$(L_{1,1} \wedge L_{1,2} \wedge \dots) \vee (L_{2,1} \wedge L_{2,2} \wedge \dots) \vee (L_{3,1} \wedge L_{3,2} \wedge \dots) \dots$$

mit Literalen  $L_{i,j}$  ist.

- In *konjunktiver Normalform*(KNF), wenn sie von der Form

$$(L_{1,1} \vee L_{1,2} \vee \dots) \wedge (L_{2,1} \vee L_{2,2} \vee \dots) \wedge (L_{3,1} \vee L_{3,2} \vee \dots) \dots$$

mit Literalen  $L_{i,j}$  ist.

**Beispiel 14.** Die Formel

$$\neg(p \vee q)$$

ist in keiner der oben eingeführten Normalformen. Die Formel

$$(\neg p \vee q) \wedge ((p \wedge p_1) \vee (p_2 \wedge p_3))$$

ist in *NNF* aber weder in *DNF* noch in *KNF*. Die Formel

$$p \vee q$$

ist in *NNF*, *KNF* und *DNF*.

**Satz 2.** Für jede aussagenlogische Formel gibt es äquivalente Formeln in *NNF*, *KNF* und *DNF*.

*Beweis.*

- *NNF*: Wir gehen folgendermassen vor, um aus einer Formel eine äquivalente Formel in *NNF* zu konstruieren.
  1. Implikationen eliminieren durch Anwenden der Regel  $F \rightarrow G \equiv \neg F \vee G$ .
  2. Negationen, die nicht zu einem Literal gehören, werden sukzessive durch Anwenden der De Morganschen Regeln und der Regel über doppelte Negation eliminiert.
- *KNF/DNF*: Jede Formel in *NNF* kann durch sukzessives Anwenden der Distributivgesetze wahlweise in *KNF* oder *DNF* gebracht werden. Da wir bereits wissen, dass jede Formel in *NNF* gebracht werden kann, ist die Behauptung somit bewiesen.  $\square$

**Beispiel 15.** Wir bringen die Formel

$$(\neg p \rightarrow q) \rightarrow ((p \wedge p_1) \vee (p_2 \wedge p_3))$$

in *DNF*. Wir eliminieren zuerst alle Implikationen und doppelten Negationen:

$$\begin{aligned} (\neg p \rightarrow q) \rightarrow ((p \wedge p_1) \vee (p_2 \wedge p_3)) &\equiv \neg(\neg p \rightarrow q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)) \\ &\equiv \neg(\neg \neg p \vee q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)) \\ &\equiv \neg(p \vee q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)). \end{aligned}$$

Als Nächstes eliminieren wir alle Negationen, die nicht in Literalen vorkommen:

$$\neg(p \vee q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)) \equiv (\neg p \wedge \neg q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)).$$

Die Formel, die wir erhalten haben, ist sowohl in *NNF* als auch in *DNF*. Wir konstruieren nun noch eine zur Formel

$$(p \wedge p_1) \vee (p_2 \wedge p_3)$$



äquivalente Formel in  $KNF$ . Wir wenden sukzessive die Distributivgesetze an:

$$\begin{aligned}(p \wedge p_1) \vee (p_2 \wedge p_3) &\equiv ((p \wedge p_1) \vee p_2) \wedge ((p \wedge p_1) \vee p_3) \\ &\equiv ((p \wedge p_1) \vee p_2) \wedge ((p \vee p_3) \wedge (p_1 \vee p_3)) \\ &\equiv ((p \vee p_2) \wedge (p_1 \vee p_2)) \wedge ((p \vee p_3) \wedge (p_1 \vee p_3)).\end{aligned}$$

**Übung 12.** Bringen Sie die Formel

$$(p_1 \rightarrow p_3) \vee (p_1 \wedge p_2)$$

in  $KNF$  und in  $DNF$ .

**Lösung.**

**Bemerkung 21.** Es ist auch möglich direkt aus einer Wahrheitstabelle einer gegebenen Formel  $F$  eine äquivalente Formel in  $KNF$  oder  $DNF$  abzulesen. Für die  $DNF$  geht man wie folgt vor: Für jede Zeile, die als Resultat `true` liefert, wird eine Konjunktion gebildet, die alle atomaren Teilformeln dieser Zeile verknüpft, dabei werden die Teilformeln, die in dieser Zeile (Belegung) falsch sind negiert. Schliesslich werden die so gewonnenen Konjunktionen als Disjunktion zusammengenommen. Eine zu  $F$  äquivalente Formel in  $KNF$  lässt sich dadurch konstruieren, dass man vorerst eine zu  $\neg F$  äquivalente Formel in  $DNF$  findet (wie oben beschrieben), diese Formel negiert und mit den Regeln von DeMorgan die Negationen in den Term schiebt.

**Beispiel 16.** Beispielhaft für dieses Vorgehens, bringen wir die Formel

$$p_0 \rightarrow (q \wedge p_1)$$

in  $DNF$  und  $KNF$ . Zuerst erstellen wir eine Wahrheitstabelle von  $p_0 \rightarrow (q \wedge p_1)$  und markieren zu jeder relevanten Zeile das gewonnene Disjunktionsglied.

$p_0$	$q$	$p_1$	$q \wedge p_1$	$p_0 \rightarrow (q \wedge p_1)$	
0	0	0	0	1	$\neg p_0 \wedge \neg q \wedge \neg p_1$
0	0	1	0	1	$\neg p_0 \wedge \neg q \wedge p_1$
0	1	0	0	1	$\neg p_0 \wedge q \wedge \neg p_1$
0	1	1	1	1	$\neg p_0 \wedge q \wedge p_1$
1	0	0	0	0	—
1	0	1	0	0	—
1	1	0	0	0	—
1	1	1	1	1	$p_0 \wedge q \wedge p_1$

Zusammengefasst ergibt sich die folgende Formel in *DNF*:

$$(\neg p_0 \wedge \neg q \wedge \neg p_1) \vee (\neg p_0 \wedge \neg q \wedge p_1) \vee (\neg p_0 \wedge q \wedge \neg p_1) \vee (\neg p_0 \wedge q \wedge p_1) \vee (p_0 \wedge q \wedge p_1).$$

Zum Erstellen einer Formel in *KNF*, betrachten wir die Wahrheitstabelle der negierten Formel:

$p_0$	$q$	$p_1$	$q \wedge p_1$	$p_0 \rightarrow (q \wedge p_1)$	$\neg(p_0 \rightarrow (q \wedge p_1))$	
0	0	0	0	1	0	—
0	0	1	0	1	0	—
0	1	0	0	1	0	—
0	1	1	1	1	0	—
1	0	0	0	0	1	$p_0 \wedge \neg q \wedge \neg p_1$
1	0	1	0	0	1	$p_0 \wedge \neg q \wedge p_1$
1	1	0	0	0	1	$p_0 \wedge q \wedge \neg p_1$
1	1	1	1	1	0	—

Durch Anwendung der DeMorgan Regeln erhalten wir daraus eine passende Formel in *KNF*:

$$\begin{aligned} & \neg((p_0 \wedge \neg q \wedge \neg p_1) \vee (p_0 \wedge \neg q \wedge p_1) \vee (p_0 \wedge q \wedge \neg p_1)) \\ & \equiv \neg(p_0 \wedge \neg q \wedge \neg p_1) \wedge \neg(p_0 \wedge \neg q \wedge p_1) \wedge \neg(p_0 \wedge q \wedge \neg p_1) \\ & \equiv (\neg p_0 \vee q \vee p_1) \wedge (\neg p_0 \vee q \vee \neg p_1) \wedge (\neg p_0 \vee \neg q \vee p_1) \end{aligned}$$

### 3 Mengen, Relationen und Funktionen

Die Mengenlehre stellt einen formalen Rahmen zur Verfügung, der es erlaubt, mehrere mathematische Objekte zusammenzufassen und diese Zusammenfassung als neues eigenständiges Objekt zu verstehen. Der Prozess der Mengenbildung und das Konzept einer Menge sind fundamental für den gesamten Aufbau der Mathematik aber nicht immer unproblematisch. Die Probleme, die ein allzu naiver Umgang mit Mengenexistenzannahmen verursachen können, zeigen sich zum Beispiel in der “Russelschen Antinomie”. Die Russelsche Antinomie verdeutlicht, dass man nicht beliebige Dinge anhand einer Eigenschaft zu einer Menge zusammenfassen kann. Das Paradox entsteht, wenn man naiverweise davon ausgeht, dass zu jeder Eigenschaft  $E$  die Menge aller Dinge mit der Eigenschaft  $E$

$$\{x \mid x \text{ hat die Eigenschaft } E(x)\}$$

gebildet werden kann. Ein solches Prinzip lässt die Bildung der paradoxen Menge

$$R = \{x \mid x \notin x\}$$

aller Mengen, die sich nicht selbst als Element enthalten, zu. Die Menge  $R$  ist widersprüchlich, weil sowohl  $R \in R$  als auch  $R \notin R$  im Widerspruch zur definierenden Eigenschaft von  $R$  steht.

In diesem Kapitel untersuchen wir, wie sich ein adäquater Umgang mit Mengen und Mengenbildung ausgestalten lässt. Weiter werden wir am Beispiel von Relationen und Funktionen sehen, dass Mengen ein mächtiges Werkzeug darstellen, das dazu geeignet ist, alle möglichen mathematischen Konstrukte präzise zu beschreiben.

#### Relevanz für die Informatik

Die Bedeutung der Mengenlehre für die Informatik kommt weniger von direkten Anwendungen, sondern von ihrer Stellung innerhalb der Mathematik - Mengen sind in gewisser Weise der *primitive Datentyp* der (modernen) Mathematik. Dies hat unter anderem folgende Konsequenzen:

- Die Mengenlehre bildet (zusammen mit der Prädikatenlogik) die Sprache der Mathematik.
- Alle mathematischen Objekte sind Mengen, insbesondere sind auch alle in der theoretischen Informatik behandelten Strukturen (berechenbare Funktionen, Turing Maschinen, ...) Mengen.

Weitere in diesem Kapitel behandelte Konzepte wie Funktionen und Relationen sind sowohl in der Mathematik als auch in der Informatik nahezu allgegenwärtig:

- 
- Funktionen in der (funktionalen) Programmierung
  - Input-Output Relation
  - Relationale Datenbanken
  - E-R-Diagramme
  - Zustandsklassen von endlichen Automaten
  - $\vdots$

Graphen und (binäre) Relationen sind im wesentlichen gleichwertig, in der Tat können Graphen auf natürliche Art und Weise dazu verwendet werden, Relationen grafisch darzustellen. In der Informatik sind Graphen (insbesondere Bäume) eine der fundamentalen Datenstrukturen (eine Art Daten zu organisieren).

## Lernziele

Sie kennen

- die grundlegenden mengentheoretischen Operationen (Vereinigung, Schnitt, Komplement, Potenzmenge).
- die Zahlenmengen  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$  und  $\mathbb{R}$ .
- die verschiedenen Darstellungsformen für Mengen.
- den Funktionsbegriff.
- Äquivalenzrelationen und Äquivalenzklassen sowie ihre grundlegenden Eigenschaften.
- Ordnungsrelationen (in den verschiedenen Variationen) und ihre grundlegenden Eigenschaften.
- grundlegende Typen von Graphen.

Sie verstehen

- den Zusammenhang von Funktionen, Relationen und Graphen.
- den Zusammenhang von Äquivalenzrelationen und Partitionen.
- die Problematik der “Wohldefiniertheit” von Funktionen auf Faktormengen.
- wie man Relationen mit Graphen darstellen kann.
- wie man Mengen in ihrer Mächtigkeit vergleicht.

- den Unterschied zwischen einer abzählbaren und einer überabzählbaren Menge.

Sie sind in der Lage

- (endliche) Ordnungsrelationen als Hasse Diagramme zu skizzieren.
- eine Ordnungsrelation aus einem Hasse Diagramm abzulesen.
- Argumente für die Abzählbarkeit von  $\mathbb{Z}$ ,  $\mathbb{Q}$  und ähnlichen Mengen anzugeben.
- zu beweisen, dass  $\mathbb{R}$  und ähnliche Mengen überabzählbar sind.

## Literatur und Links

Ergänzende Literatur:

- [3] Kapitel 2 ohne 2.4 und 2.5.
- [3] Kapitel 4.1 bis 4.3.
- [4] Kapitel 1 Teil 1 und Kapitel 1.4 sowie 1.5.

Nützliche Links:

- [http://de.wikipedia.org/wiki/Menge\\_\(Mathematik\)](http://de.wikipedia.org/wiki/Menge_(Mathematik))
- <http://builds.openlogicproject.org/courses/set-theory/settheory-screen.pdf> Kapitel 2. und 5.
- [http://de.wikipedia.org/wiki/Relation\\_%28Mathematik%29](http://de.wikipedia.org/wiki/Relation_%28Mathematik%29)
- [https://de.wikipedia.org/wiki/Graph\\_\(Graphentheorie\)](https://de.wikipedia.org/wiki/Graph_(Graphentheorie))

## 3.1 Der Mengenbegriff und grundlegende Definitionen

Wenn jedes mathematische Objekt eine Menge ist, was ist dann die mathematische Definition einer Menge? Dies ist in der Tat nicht ganz einfach und wird in der Literatur meist auf eine der folgenden Arten behandelt:

- Einführung einer formalen Axiomatisierung der (oder einer) Mengenlehre.
- Auf eine Definition wird verzichtet, stattdessen werden wichtige “definierende” Eigenschaften von Mengen festgehalten. Dieser Ansatz entspricht von der Idee her dem ersten Ansatz, ist aber weniger formal ausgelegt.
- Eine anschauliche “Definition” zu verwenden, die zwar den Standards einer mathematischen Definition nicht genügt, aus der sich aber trotzdem wichtige Eigenschaften von Mengen anschaulich ableiten lassen.

Wir wählen die zweite Variante und bauen unseren Mengenbegriff dadurch auf, dass wir einige *definierende Eigenschaften* und Schreibweisen für Mengen einführen.

Die wichtigste Schreibweise im Umgang mit Mengen ist die Notation, die ausdrückt, ob etwas zu einer Menge gehört oder nicht.

**Notation.** Ist  $X$  eine Menge und  $y$  ein *Element* von  $X$ , dann schreiben wir  $y \in X$ . Ist  $y$  kein Element von  $X$ , dann schreiben wir  $y \notin X$ .

Die erste *definierende Eigenschaft* von Mengen ist die Tatsache, dass jede Menge durch ihre Elemente vollständig beschrieben ist.

**Definition 15** (Definierende Eigenschaft). Zwei Mengen sind genau dann gleich, wenn sie dieselben Elemente enthalten: Es gilt für alle Mengen  $X$  und  $Y$  die Äquivalenz

$$X = Y \Leftrightarrow \forall z (z \in X \Leftrightarrow z \in Y).$$

Da Mengen bereits durch Angabe ihrer Elemente bestimmt werden, können wir jede (endliche) Menge durch Auflisten ihrer Elemente festlegen.

**Definition 16** (Explizite Schreibweise). Sind mathematische Objekte  $x_1, \dots, x_n$  gegeben, dann schreiben wir

$$\{x_1, \dots, x_n\}$$

für die Menge die als Elemente genau  $x_1, \dots, x_n$  hat.

**Beispiel 17.**

- Die Menge  $\{2, 34, 77\}$  enthält die drei Elemente 2, 34 und 77.
- Die Menge  $\{\}$  heisst *leere Menge*. Die leere Menge ist die einzige Menge, die gar keine Elemente besitzt, sie wird mit  $\emptyset$  bezeichnet.

**Bemerkung 22.** Wenn keine Missverständnisse zu befürchten sind, so beschreibt man Mengen auch durch “angedeutete” Aufzählung ihrer Elemente. Die Menge  $\mathbb{N}$  der *natürlichen Zahlen* wird beispielsweise durch

$$\mathbb{N} := \{0, 1, 2, \dots\}$$

beschrieben. Die Menge der *ganzen Zahlen* wird durch

$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$$

beschrieben.

**Bemerkung 23.** Die Tatsache, dass Mengen durch ihre Elemente eindeutig beschrieben werden hat zur Folge, dass Mengen sehr “unstrukturierte Datentypen” sind, d.h. Mengen haben keine “innere Ordnung”. Es gelten unter anderem:

- Für beliebige  $z, x_1, \dots, x_n$

$$z \in \{x_1, \dots, x_n\} \Leftrightarrow z = x_1 \vee \dots \vee z = x_n$$

- Für alle  $x$

$$\{x\} = \{x, x\} = \{x, x, x\} = \dots$$

- Für alle  $x, y$

$$\{x, y\} = \{y, x\}.$$

**Definition 17** (Teilmengen). Wir schreiben  $X \subseteq Y$  und sagen  $X$  ist eine *Teilmenge* von  $Y$ , wenn jedes Element von  $X$  auch ein Element von  $Y$  ist:

$$X \subseteq Y : \Leftrightarrow \forall x (x \in X \Rightarrow x \in Y).$$

Wir schreiben  $X \subsetneq Y$  und sagen  $X$  ist eine *echte Teilmenge* von  $Y$ , falls  $X$  eine von  $Y$  verschiedene Teilmenge von  $Y$  ist:

$$X \subsetneq Y : \Leftrightarrow X \subseteq Y \wedge X \neq Y.$$

**Beispiel 18.**

- Die Menge aller Hühner ist eine (echte) Teilmenge der Menge aller Vögel, weil alle Hühner Vögel sind (und weil es Vögel gibt die keine Hühner sind).
- Die Menge aller Primzahlen ist eine (echte) Teilmenge von  $\mathbb{N}$ .
- Die Menge aller Primzahlen ist *keine* Teilmenge aller ungeraden Zahlen, weil die Zahl 2 eine Primzahl aber keine ungerade Zahl ist.

**Bemerkung 24.** Zwei Mengen  $X$  und  $Y$  sind gleich, wenn  $X \subseteq Y$  und  $Y \subseteq X$  gilt.

Wir führen im Folgenden einige Operationen und Schreibweisen ein, mithilfe derer wir neue Mengen (aus bereits vorhandenen) generieren können. Wir erhalten beispielsweise die Menge aller Primzahlen aus der Menge der natürlichen Zahlen, indem wir

$$\{p \in \mathbb{N} \mid p \text{ hat genau 2 Teiler}\}$$

schreiben.

**Definition 18** (Prädikative Schreibweise). Ist  $X$  eine Menge und ist  $E$  eine Eigenschaft (Prädikat), dann bezeichnen wir mit

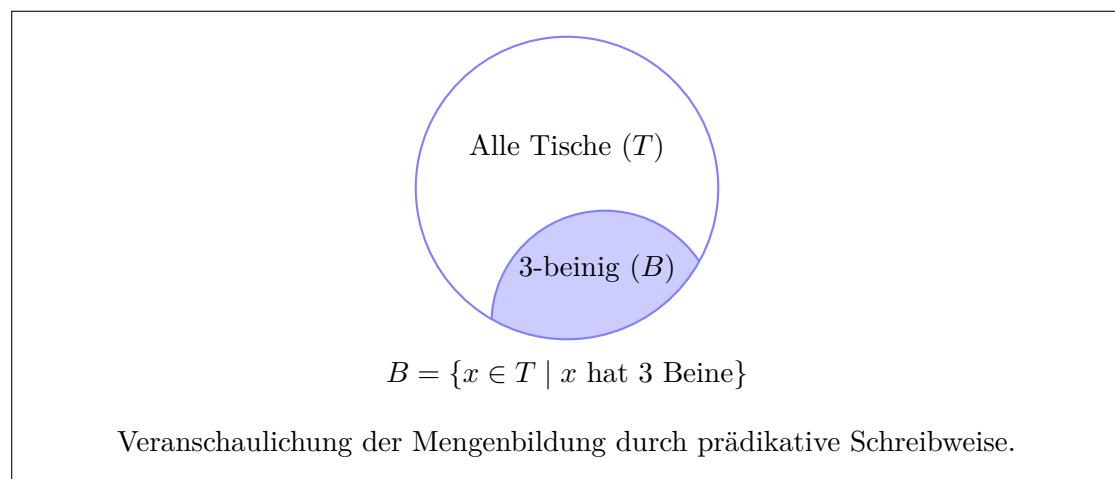
$$\{z \in X \mid E(z)\}$$

oder mit

$$\{z \mid z \in X \wedge E(z)\}$$

die Menge aller Elemente  $z$  von  $X$  mit der Eigenschaft  $E(z)$ .

**Beispiel 19.** Wenn man aus der Menge aller Tische die Dinge mit der Eigenschaft “drei Beine zu haben” aussondert (und zusammenfasst), dann erhält man die Menge aller dreibeinigen Tische.



**Beispiel 20.** Die Menge aller geraden natürlichen Zahlen erhält man auch durch die prädikative Schreibweise,

- $\{n \in \mathbb{N} \mid n \text{ ist gerade}\}$
- $\{n \in \mathbb{N} \mid \exists z \in \mathbb{N} (n = 2 \cdot z)\}$

**Definition 19** (Ersetzungsschreibweise). Ist  $F$  eine Funktion und ist  $X$  eine Menge, dann beinhaltet die Menge

$$\{F(x) \mid x \in X\}$$



alle Funktionswerte  $F(x)$ , die man dadurch erhalten kann, dass man ein Element  $x \in X$  in  $F$  einsetzt:

$$\{F(x) \mid x \in X\} := \{y \mid \exists x \in X (y = F(x))\}.$$

**Bemerkung 25.** Ist eine Funktion  $F$  und eine Menge von der Form

$$X = \{x_1, x_2, x_3, \dots\}$$

gegeben, dann entspricht die Menge  $\{F(x) \mid x \in X\}$  anschaulich der Menge

$$\{f(x_1), f(x_2), f(x_3), \dots\}.$$

**Bemerkung 26.** Das Prinzip der Ersetzungsschreibweise findet sich als Funktion zum Manipulieren von Datensätzen in vielen Programmiersprachen wieder:

- Haskell: `map`, `fmap`
- Java: `map()`
- Python: `map`
- C#: `.select`

**Beispiel 21.** Die Menge der geraden natürlichen Zahlen lässt sich nun mithilfe der Funktion  $F(x) = 2 \cdot x$  als

$$\{F(x) \mid x \in \mathbb{N}\} = \{2x \mid x \in \mathbb{N}\}$$

schreiben.

**Definition 20.** Sind  $X$  und  $Y$  Mengen, dann ist

$$X \cup Y := \{x \mid x \in X \vee x \in Y\}$$

die *Vereinigung* von  $X$  mit  $Y$ . Die *Schnittmenge* von  $X$  und  $Y$  ist durch

$$X \cap Y := \{x \in X \mid x \in Y\} = \{x \in Y \mid x \in X\} = \{x \mid x \in X \wedge x \in Y\}$$

gegeben. Ist  $I$  eine Menge so, dass für alle Elemente  $i \in I$  auch  $A_i$  eine Menge ist, dann wird

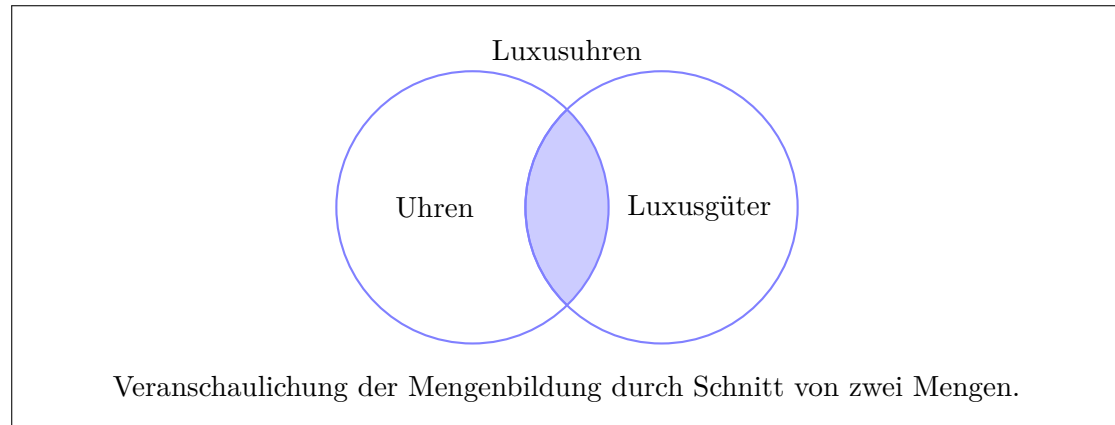
$$\bigcup_{i \in I} A_i := \{x \mid \exists i \in I (x \in A_i)\}.$$

die Vereinigung von  $\{A_i \mid i \in I\}$  genannt. Analog dazu, ist die *Schnittmenge* durch

$$\bigcap_{i \in I} A_i := \{x \mid \forall i \in I (x \in A_i)\}$$

gegeben, falls  $I \neq \emptyset$  ist.

**Beispiel 22.** Die Schnittmenge der Menge der Luxusgüter mit der Menge aller Uhren beinhaltet genau die Luxusuhren.



**Beispiel 23.**

a)  $\mathbb{N} = \{n \in \mathbb{N} \mid n \text{ ist gerade}\} \cup \{n \in \mathbb{N} \mid n \text{ ist ungerade}\}$

b)  $\emptyset = \{n \in \mathbb{N} \mid n \text{ ist gerade}\} \cap \{n \in \mathbb{N} \mid n \text{ ist ungerade}\}$

c) Sind  $X_a$  und  $X_b$  beliebige Mengen, dann gilt:

$$X_a \cup X_b = \bigcup_{i \in \{a, b\}} X_i.$$

d) Ist für jede natürliche Zahl  $n$  die Menge  $X_n$  als  $\{0, \dots, n\}$  gegeben, dann gilt

$$\bigcup_{n \in \mathbb{N}} X_n = \mathbb{N}$$

und

$$\bigcap_{n \in \mathbb{N}} X_n = \{0\}.$$

**Übung 13.** Beschreiben Sie folgende Mengen:

a)  $\{0, 2, 4, \dots\} \cap \{p \in \mathbb{N} \mid p \text{ ist eine Primzahl}\}$

b)  $\mathbb{N} \cap \{\mathbb{N}\}$

c)  $\mathbb{N} \cup \{\mathbb{N}\}$

d)  $\{3x \mid x \in \mathbb{N}\} \cap \{5x \mid x \in \mathbb{N}\}$

**Lösung.**

**Definition 21.** Zwei Mengen  $X$  und  $Y$  heissen *disjunkt*, falls sie keine gemeinsamen Elemente haben, d.h. falls  $X \cap Y = \emptyset$  gilt. Wir sagen eine Menge  $\{X_i \mid i \in I\}$  von Mengen bestehe aus *paarweise disjunkten* Mengen, wenn folgendes gilt:

$$\forall i, j \in I (i \neq j \Rightarrow X_i \cap X_j = \emptyset).$$

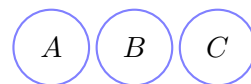
**Bemerkung 27.** Für Mengen  $\{X_i \mid i \in I\}$ , hat die Annahme

$$\bigcap_{i \in I} X_i = \emptyset$$

nicht notwendigerweise zur Folge, dass die  $X_i$ 's paarweise disjunkt sind.



Disjunkt ( $A \cap B \cap C = \emptyset$ ),  
nicht paarweise disjunkt



Paarweise disjunkt

**Definition 22.** Sind  $X$  und  $Y$  beliebige Mengen, so definieren wir als

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

die Menge aller Elemente von  $X$ , die nicht zu  $Y$  gehören. Die Menge  $X \setminus Y$  nennt man “ $X$  ohne  $Y$ ”. Ist eine “Grundmenge”  $A$  (implizit oder explizit) vorgegeben, so bezeichnet man die Menge  $A \setminus Y$  auch als “Komplement” oder “Komplementärmenge” von  $X$  (relativ zu  $A$ ).

**Beispiel 24.** Die Menge der ungeraden Zahlen können wir als

$$\mathbb{N} \setminus \{2x \mid x \in \mathbb{N}\}$$

schreiben.

**Übung 14.** Beschreiben Sie folgende Mengen.

- a)  $\mathbb{N} \setminus \{x \in \mathbb{N} \mid x \text{ ist gerade}\}$
- b)  $\{x \in \mathbb{N} \mid x \text{ ist gerade}\} \setminus \{3x \mid x \in \mathbb{N}\}$
- c)  $\mathbb{N} \setminus (\mathbb{N} \setminus \mathbb{Z})$

**Lösung.**

**Satz 3** (Rechenregeln). *Es gelten für beliebige Mengen  $A, B$  und  $C$  folgende Identitäten:*

- a) *Kommutativität der Vereinigung und des Schnittes:*

$$A \cup B = B \cup A \text{ und } A \cap B = B \cap A.$$

- b) *Assoziativgesetze von Schnitt und Vereinigung:*

$$A \cap (B \cap C) = (A \cap B) \cap C \text{ und } A \cup (B \cup C) = (A \cup B) \cup C$$

- c) *Distributivgesetze von  $\cap$  mit  $\cup$ :*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \text{ und } A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

- d) *Idempotenzgesetz:*

$$A \cap A = A \text{ und } A \cup A = A$$

- e) *Regeln von DeMorgan:*

$$(C \setminus A) \cap (C \setminus B) = C \setminus (A \cup B) \text{ und } (C \setminus A) \cup (C \setminus B) = C \setminus (A \cap B)$$

f) *Charakterisierung der Teilmengenbeziehung:*

$$A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$$

*Beweis.* Übung □

**Übung 15.** Zeigen Sie für beliebige Mengen  $A$  und  $B$ :

a)  $A \setminus (A \setminus B) = A \cap B$

b)  $(A \setminus B) \setminus B = A \setminus B$

**Lösung.**

**Definition 23.** Ist  $A$  eine beliebige Menge, dann bezeichnen wir mit

$$\mathcal{P}(A) := \{x \mid x \subseteq A\}$$

die *Potenzmenge* von  $A$ , die genau die Teilmengen von  $A$  als Elemente enthält.

**Beispiel 25.** a)  $\mathcal{P}(\emptyset) = \{\emptyset\} \neq \emptyset$

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

**Übung 16.** Beschreiben Sie in aufzählender Form:

- a)  $\mathcal{P}(\{3, 4\})$
- b)  $\mathcal{P}(\{a, \{c\}\})$
- c)  $\mathcal{P}(\{\{\{x\}\}\})$

**Lösung.**

**Übung 17.** Geben Sie Mengen  $A$  und  $B$  an, mit

$$\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B).$$

**Lösung.**

**Definition 24** (Partitionen). Eine *Partition*  $P = \{P_i \mid i \in I\}$  einer Menge  $A$ , ist eine Menge von Teilmengen von  $A$ , die folgende beiden Voraussetzungen erfüllt:

- Die Elemente von  $P$  sind nichtleer und paarweise disjunkt.
- $\bigcup_{i \in I} P_i = A$

Die Elemente einer Partition werden *Blöcke* der Partition genannt.

**Beispiel 26.**

- Die Menge aller geraden natürlichen Zahlen und die Menge aller ungeraden natürlichen Zahlen bilden zusammen eine Partition der natürlichen Zahlen. Genauer, falls  $G$  die Menge der geraden natürlichen Zahlen und  $U$  die Menge der ungeraden natürlichen Zahlen ist, dann ist die Menge  $\{G, U\}$  eine Partition von  $\mathbb{N}$  mit zwei Blöcken.
- Für

$$A_i = \{i, -i\}$$

ist die Menge  $P = \{A_i \mid i \in \mathbb{N}\}$  eine Partition der Menge  $\mathbb{Z}$  (in unendlich viele Blöcke).

**Übung 18.**

- Geben Sie eine Partition von  $\mathbb{N}$  in unendlich viele Blöcke an.
- Geben Sie eine Partition von  $\mathbb{N}$  an, deren Blöcke alle unendlich gross sind.
- Geben Sie eine Partition der rationalen Zahlen in unendlich viele, unendlich grosse Blöcke an.

**Lösung.**

## 3.2 Relationen, Funktionen und Graphen

Relationen beschreiben unterschiedlichste Beziehungen zwischen (mathematischen) Objekten. Vier völlig unterschiedliche Relationen könnten etwa wie folgt gegeben sein.

**Beispiel 27.** Die Relationen  $R_1, R_2, R_3$  und  $T$  sind durch folgende Zuordnungen gegeben:

- Zwei Geraden stehen in Relation  $R_1$  zueinander, wenn sie parallel sind. Dies ist eine (binäre) Relation auf der Menge aller Geraden.
- Zwei Punkte auf der Erdoberfläche stehen zueinander in Relation  $R_2$ , wenn der erste Punkt zu Fuss (und ohne weitere Hilfsmittel) vom zweiten Punkt aus erreichbar ist.
- Eine Person  $P$  steht in Relation  $R_3$  zu Person  $Q$ , wenn  $P$  in  $Q$  verliebt ist.
- Eine natürliche Zahl  $x$  steht in Relation  $T$  zu einer natürlichen Zahl  $y$ , falls  $x$  ein Teiler von  $y$  ist.

Zum präziseren Formulieren von Relationen verwenden wir *Tupel*, diese erlauben es uns beliebig Elemente zu kombinieren und in Beziehung zueinander zu setzen. *Tupel* haben im Gegensatz zu Mengen mehr innere Struktur - die Reihenfolge und Wiederholung von Elementen sind wesentlich, sie sind gewissermassen die mathematische Entsprechung zu Listen und Arrays in der Informatik.

**Definition 25** (Tupel). Es sei  $n > 0$  eine natürliche Zahl. Ein  $n$ -Tupel ist ein Term von der Form

$$(x_1, \dots, x_n).$$

Für beliebige Tupel gilt:

$$(x_1, \dots, x_n) = (y_1, \dots, y_k) :\Leftrightarrow n = k \wedge x_1 = y_1 \wedge \dots \wedge y_n = x_n.$$

2-Tupel nennen wir *Paare* und 3-Tupel *Tripel*.

Die Gesamtheit aller Tupel mit Elementen aus einer oder mehreren gegebenen Mengen nennt man kartesisches Produkt.

**Definition 26.** Es seien  $A_1, \dots, A_n$  Mengen und  $n \in \mathbb{N}$  mit  $n > 0$ . Das *kartesische Produkt* von  $A_1, \dots, A_n$ , ist die Menge aller  $n$ -Tupel mit Einträgen aus den Mengen  $A_1, \dots, A_n$ :

$$\prod_{i=1}^n A_i = \{(a_1, \dots, a_n) \mid a_1 \in A_1 \wedge \dots \wedge a_n \in A_n\}.$$

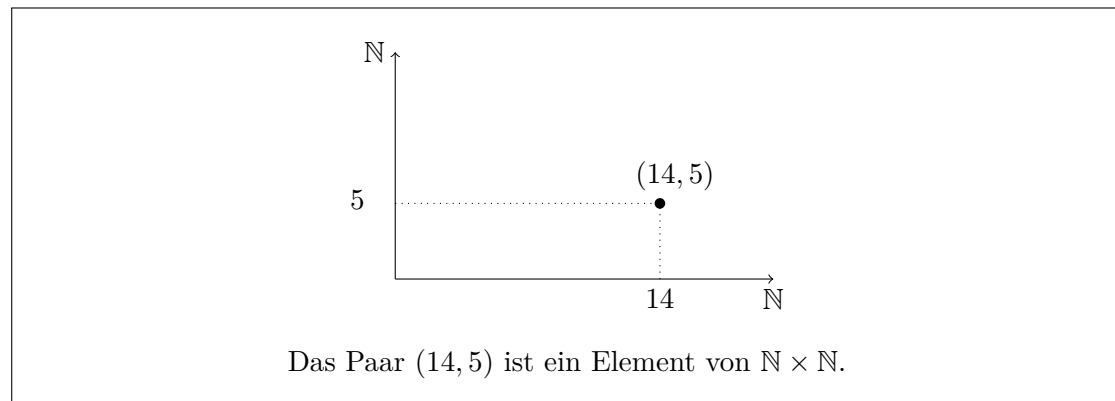


**Bemerkung 28.** Oft schreiben wir auch  $A_1 \times A_2 \times \cdots \times A_n$  für das kartesische Produkt  $\prod_{i=1}^n A_i$ . Insbesondere schreiben wir  $X \times Y$  für das kartesische Produkt von zwei Mengen  $X$  und  $Y$ , konkret heisst das:

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

Für das  $n$ -fache kartesische Produkt  $A \times A \times \cdots \times A$  einer Menge  $A$  mit sich selbst schreiben wir auch  $A^n$ .

**Beispiel 28.** Das kartesische Produkt der Menge  $\mathbb{N}$  mit sich selbst enthält alle möglichen Paare von natürlichen Zahlen.



**Beispiel 29.** Die Menge der rationalen Zahlen

$$\mathbb{Q} := \left\{ \frac{x}{y} \mid x \in \mathbb{Z} \wedge y \in \mathbb{N} \setminus \{0\} \right\}$$

kann man als das kartesische Produkt

$$\mathbb{Z} \times (\mathbb{N} \setminus \{0\})$$

auffassen.

Nun können wir Relationen mit Mengen von Tupeln, also Teilmengen von kartesischen Produkten, identifizieren. Wir erhalten dadurch einen sehr einfachen und allgemeinen Relationsbegriff, der beliebige (auch beliebig exotische) Beziehungen als Relationen zulässt.

**Definition 27.** Eine  $n$ -stellige *Relation*  $R$  auf den Mengen  $A_1, \dots, A_n$  ist eine Menge von  $n$ -Tupeln aus  $A_1 \times \cdots \times A_n$ . Mit anderen Worten, die Relationen auf  $A_1, \dots, A_n$  sind genau die Teilmengen

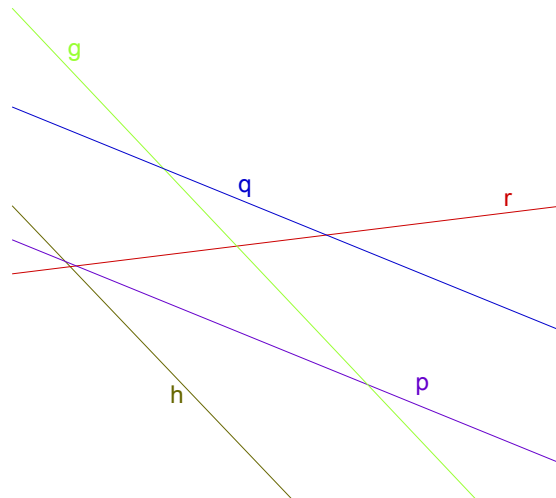
$$R \subseteq A_1 \times \cdots \times A_n.$$

Ist  $R$  eine  $n$ -stellige Relation und gilt  $(x_1, \dots, x_n) \in R$ , dann sagen wir, dass die Elemente  $x_1, \dots, x_n$  zueinander in Relation  $R$  stehen.

**Bemerkung 29.** Eine 2-stellige Relation  $R \subseteq X \times Y$  heisst auch eine *binäre Relation* auf den Mengen  $X$  und  $Y$ . Ist  $R$  eine binäre Relation, so schreiben wir auch  $xRy$  für  $(x, y) \in R$ .

Wir werden uns im Folgenden auf binäre Relationen beschränken.

**Beispiel 30.** Wir betrachten die Relation  $R_1$  von Beispiel 27 auf  $\{g, h, p, q, r\}$ . Die Geraden  $g, h, p, q, r$  sind wie im folgenden Bild gegeben:



Offenbar gelten folgende Beziehungen:

- Die Gerade  $g$  steht in Relation  $R_1$  zu folgenden Geraden:  $g, h$ .
- Die Gerade  $h$  steht in Relation  $R_1$  zu folgenden Geraden:  $g, h$ .
- Die Gerade  $p$  steht in Relation  $R_1$  zu folgenden Geraden:  $p, q$ .
- Die Gerade  $q$  steht in Relation  $R_1$  zu folgenden Geraden:  $p, q$ .
- Die Gerade  $r$  steht mit keiner anderen Geraden in Relation  $R_1$ .

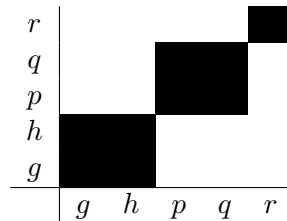
Als Menge geschrieben, nimmt die Relation  $R_1$  also folgende Gestalt an:

$$R_1 = \{(g, g), (g, h), (h, h), (h, g), (p, p), (p, q), (q, q), (q, p), (r, r)\}.$$

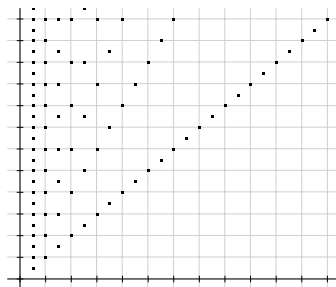
Bildlich lässt sich die Relation als Tabelle darstellen:

$r$	$\times$	$\times$	$\times$	$\times$	$\checkmark$
$q$	$\times$	$\times$	$\checkmark$	$\checkmark$	$\times$
$p$	$\times$	$\times$	$\checkmark$	$\checkmark$	$\times$
$h$	$\checkmark$	$\checkmark$	$\times$	$\times$	$\times$
$g$	$\checkmark$	$\checkmark$	$\times$	$\times$	$\times$
	$g$	$h$	$p$	$q$	$r$

Aus der Tabelle erhält man, ähnlich (gleich) wie im Fall von Funktionen und Funktionsgraphen, den Relationsgraph von  $R_1$ :

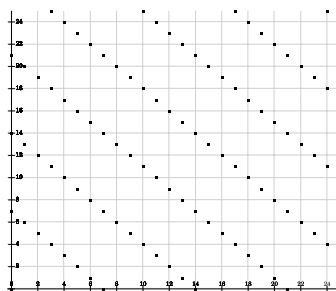


**Beispiel 31.** Der Relationsgraph der Teilbarkeitsrelation (die Relation  $T$  von Beispiel 27) auf der Menge  $\{n \in \mathbb{N} \mid 1 < n < 100\}$ .



Der Relationsgraph von

$$R = \{(x, y) \mid x, y \in \mathbb{N} \wedge x, y < 100 \wedge x + y \text{ ist ein Vielfaches von } 7\}$$



Ein alternativer Zugang zum Veranschaulichen von binären Relationen bietet die “Graphentheorie”. Ein Graph<sup>1</sup> ist in diesem Kontext eine abstrakte Struktur bestehend aus Knoten und Verbindungen zwischen diesen Knoten (Kanten).

---

<sup>1</sup>Nicht zu verwechseln mit einem Funktionsgraphen oder einem Relationsgraphen

**Definition 28.** Ein (*gerichteter*) *Graph* ist ein Paar  $G = (V, E)$  bestehend aus einer Menge  $V$  (Knotenmenge) und einer binären Relation  $E \subseteq V \times V$  (Kantenmenge).

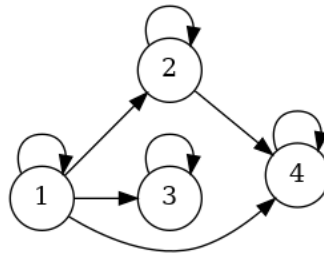
Endliche Graphen können grafisch dargestellt werden, dazu werden die Knoten durch Punkte oder Kreise und die Kanten durch Linien oder Pfeile zeichnerisch repräsentiert. Dies erlaubt es beliebige binäre Relationen zeichnerisch darzustellen.

**Beispiel 32.** Die Teilbarkeitsrelation auf der Menge  $\{1, 2, 3, 4\}$  lässt sich als Graph  $G = (V, E)$  mit

$$V = \{1, 2, 3, 4\}$$

$$E = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}$$

auffassen. Wir veranschaulichen den Graphen, indem wir die Knoten als Punkte oder Kreise und die Kanten als Pfeile zwischen den Knoten darstellen:



**Übung 19.** Stellen Sie die Relation  $<$  auf der Menge  $\{1, 2, 3, 4\}$  als Graph dar.

**Lösung.**

### 3.2.1 Funktionen

Wichtige Vertreter von binären Relationen sind die *Funktionen* wobei die grundlegende Idee einer Funktion im Verbinden von gewissen “Inputelementen” mit eindeutig bestimmten, dazu passenden, “Outputelementen” besteht. Konkret heisst dies:

- Für jede Funktion gibt es eine klar definierte Menge von zulässigen “Inputelementen”, dies nennt man die Definitionsmenge oder den Definitionsbereich der Funktion.
- Jedem “Inputelement” wird genau ein “Outputelement” zugeordnet. Jede Funktion “produziert” also für jeden zulässigen Input einen und nur einen (und stets den gleichen) Output.

Dies lässt sich wie folgt als mathematische Definition fassen.

**Definition 29.** Es seien  $A$  und  $B$  beliebige Mengen. Eine Relation  $f \subseteq A \times B$  ist eine *Funktion* von  $A$  nach  $B$ , falls:

$$\forall x \in A \exists! y \in B ((x, y) \in f)$$

gilt. In diesem Fall schreiben wir

$$f : A \rightarrow B.$$

**Bemerkung 30.** Im Kontext einer Funktion  $f : A \rightarrow B$  verwenden wir folgende Schreibweisen und Konventionen:

- Da zu jedem  $x \in A$  ein eindeutig bestimmtes Element  $y \in B$  mit  $(x, y) \in f$  existiert, kann dieses  $y$  mit  $f(x)$  bezeichnet und *Funktionswert von  $f$  bei  $x$*  genannt werden.
- Die Menge aller Funktionswerte  $Im(f) := \{f(x) \mid x \in A\}$  wird als *Bild(menge)* von  $f$  bezeichnet.
- Die Menge  $A$  nennen wir den Definitionsbereich von  $f$  und schreiben dafür auch  $Dom(f)$ .
- Der Definitionsbereich ist eindeutig durch die Funktion gegeben:

$$A = Dom(f) = \{x \mid \exists y((x, y) \in f)\} = \{x \mid \exists y(f(x) = y)\}$$

- Die Menge  $B$  ist durch die Voraussetzung  $f : A \rightarrow B$  nicht eindeutig bestimmt, tatsächlich gilt  $f : A \rightarrow B$  für jede Menge  $B$  mit  $Im(f) \subseteq B$ .

**Bemerkung 31.** Oft werden Funktionen durch Spezifikation einer Definitions- und Zielmenge sowie einem Term für die “Zuordnungsvorschrift” oder “Abbildungsvorschrift” definiert. Die Funktion

$$f = \{(x, y) \in \mathbb{N}^2 \mid y = x^2\}$$

könnte etwa wie folgt angegeben werden:

$$\begin{aligned} f &: \mathbb{N} \rightarrow \mathbb{N} \\ f(x) &= x^2 \end{aligned}$$

Grundsätzlich gibt es keine Einschränkungen darüber wie eine Abbildungsvorschrift angegeben werden kann. Insbesondere lässt sich eine Funktion auf viele verschiedene Arten beschreiben<sup>2</sup>. Zur Veranschaulichung folgen zwei unterschiedliche Beschreibungen der Betragsfunktion:

$$\begin{aligned} |\cdot| &: \mathbb{Z} \rightarrow \mathbb{Z} \\ |x| &= \sqrt{x^2} \end{aligned}$$

oder

$$\begin{aligned} |\cdot| &: \mathbb{Z} \rightarrow \mathbb{Z} \\ |x| &= \begin{cases} -x & \text{wenn } x < 0 \\ x & \text{sonst} \end{cases} \end{aligned}$$

**Übung 20.** Geben Sie die Betragsfunktion wie oben definiert als Relation (Menge von geordneten Paaren) an.

**Lösung.**

---

<sup>2</sup>Man beachte die Unterscheidung zwischen einer Funktion (der Menge von geordneten Paaren) und ihrer Beschreibungen.

Funktionen lassen sich (bei geeigneten Definitions- und Bildmengen) kombinieren, man spricht dabei von der Komposition von Funktionen.

**Definition 30.** Sind  $f : A \rightarrow B$  und  $g : B \rightarrow C$  Funktionen, dann ist die Komposition  $g$  nach  $f$  durch

$$\begin{aligned} g \circ f &: A \rightarrow C \\ (g \circ f)(x) &= g(f(x)) \end{aligned}$$

gegeben.

Einige Funktionen ordnen nicht nur jedem Inputelement genau einen Output zu, sondern besitzen auch die “umgekehrte Eigenschaft”, dass jeder Output nur mittels einem einzigen Inputelement erreicht werden kann. Derartige Funktionen nennt man *injektiv*.

**Definition 31.** Eine Funktion  $f$  ist genau dann *injektiv*, wenn die Relation

$$f^{-1} = \{(y, x) \mid (x, y) \in f\}$$

eine Funktion ist. Ist  $f : A \rightarrow B$  eine injektive Funktion, dann nennt man  $f^{-1} : \text{Im}(f) \rightarrow A$  die *Umkehrfunktion* oder *inverse Funktion* von  $f$ .

**Bemerkung 32.** Für  $f : A \rightarrow B$  sind folgende Aussagen äquivalent.

- a) Die Funktion  $f$  ist injektiv
- b) Für alle  $x, y \in A$  gilt: Aus  $x \neq y$  folgt  $f(x) \neq f(y)$
- c) Für alle  $x, y \in A$  gilt: Aus  $f(x) = f(y)$  folgt  $x = y$

*Beweis.* Die Aussagen in b) und c) sind offensichtlich äquivalent (Kontraposition). Für die Äquivalenz von a) und c) sei  $f$  injektiv. Die Relation  $f^{-1} = \{(y, x) \mid (x, y) \in f\}$  sei also eine Funktion. Daraus folgt, dass zu jedem  $y$  höchstens ein  $x$  mit  $(y, x) \in f^{-1}$  existiert. Formal heisst das:

$$(y, x) \in f^{-1} \wedge (y, x') \in f^{-1} \Rightarrow x = x'$$

Dies ist gleichbedeutend mit

$$(x, y) \in f \wedge (x', y) \in f \Rightarrow x = x'$$

und somit

$$f(x) = y \wedge f(x') = y \Rightarrow x = x'$$

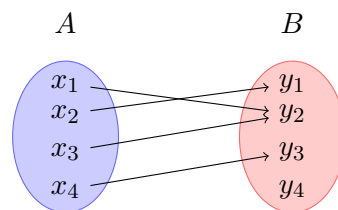
was genau der Aussage in c) entspricht. □

Eine Funktion, die jedes Element einer gegebenen Zielmenge als Funktionswert realisiert, nennt man *surjektiv auf der entsprechenden Zielmenge*.

**Definition 32.** Eine Funktion  $f : A \rightarrow B$  heisst *surjektiv* auf  $B$ , wenn  $B = \text{Im}(f)$ . Ist die Funktion  $f$  zusätzlich injektiv, so sagen wir  $f : A \rightarrow B$  sei *bijektiv*.

**Warnung.** So wie wir Funktionen eingeführt haben (als Mengen von geordneten Paaren) ist Surjektivität keine Eigenschaft, die eine Funktion für sich selbst genommen erfüllen kann. Nach dem hier gewählten Ansatz ist der Begriff der Surjektivität nur im Zusammenhang mit einer gegebenen Zielmenge sinnvoll. Andere Ansätze setzen voraus, dass jede Funktion bereits per Definition eine feste Zielmenge beinhaltet. In solchen Kontexten kann sinnvollerweise von surjektiven Funktionen gesprochen werden.

**Bemerkung 33.** Surjektivität und Injektivität lassen sich gut anhand von “Gegenbeispielen” veranschaulichen. Ist die Funktion  $f : A \rightarrow B$  durch



gegeben, dann gilt:

- Die Funktion ist wegen  $f(x_1) = f(x_3)$  nicht injektiv.
- Die Funktion ist wegen  $y_4 \in B$  nicht surjektiv auf  $B$ .
- Die Funktion ist surjektiv auf  $\{y_1, y_2, y_3\}$ .

**Lemma 1.** Für beliebige Funktionen  $f : X \rightarrow Y$  und  $g : Y \rightarrow Z$  gelten folgende Aussagen:

- a) Falls  $f : X \rightarrow Y$  und  $g : Y \rightarrow Z$  injektiv sind, dann ist auch  $g \circ f : X \rightarrow Z$  injektiv.
- b) Falls  $f : X \rightarrow Y$  und  $g : Y \rightarrow Z$  surjektiv sind, dann ist auch  $g \circ f : X \rightarrow Z$  surjektiv.

**Beweis.** a) Wir nehmen an, dass  $f : X \rightarrow Y$  und  $g : Y \rightarrow Z$  injektiv sind und zeigen, dass  $g \circ f : X \rightarrow Z$  injektiv ist. Es seien  $a, b \in X$  verschiedene Elemente. Weil  $f$  injektiv ist, folgt  $f(a) \neq f(b)$  und folglich aus der Injektivität von  $g$ , wie gewünscht

$$g \circ f(a) = g(f(a)) \neq g(f(b)) = g \circ f(b).$$



- b) Für die zweite Behauptung müssen wir zeigen, dass zu jedem  $z \in Z$  ein  $x \in X$  existiert mit  $g(f(x)) = z$ . Es sei also  $z \in Z$  beliebig. Weil  $g : Y \rightarrow Z$  surjektiv ist, gibt es ein  $y \in Y$  mit  $g(y) = z$ . Weil  $f : X \rightarrow Y$  ebenfalls surjektiv ist, gibt es weiter ein  $x \in X$  mit  $f(x) = y$ . Insgesamt haben wir wie gewünscht

$$g(f(x)) = g(y) = z.$$

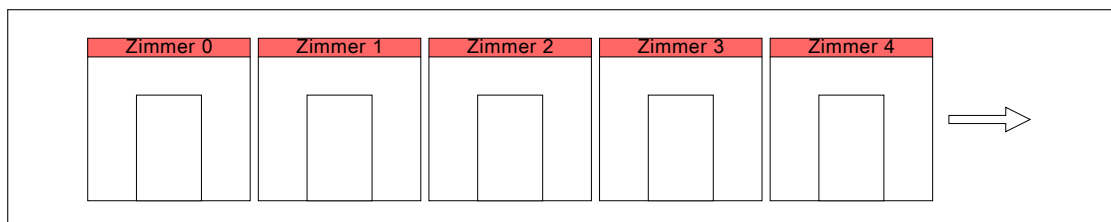
□

Eine wichtige Anwendung vom Funktionsbegriff innerhalb der Mengenlehre besteht darin mithilfe von Funktionen unendlich grosse Mengen (z.B.  $\mathbb{N}$ ,  $\mathbb{Z}$ , etc.) miteinander bezüglich ihrer Grösse zu vergleichen.

### 3.2.2 Grössenvergleiche von unendlichen Mengen

Bevor wir uns mit unendlichen Mengen befassen, sollten wir uns darüber im Klaren sein, dass unser “gesunder Menschenverstand” ein gefährlicher Begleiter auf diesem Weg sein kann. Um zu sehen, wie heikel die Vermischung von alltäglichen Konzepten mit der Vorstellung des Unendlichen sind, betrachten wir ein Hotel mit unendlich vielen Zimmern – das sogenannte Hilbert Hotel.

**Beispiel 33** (Hilbert’s Hotel). Hilbert’s Hotel hat unendlich viele Zimmer, für jede natürliche Zahl eines.



Im Rahmen eines Ferienjobs haben Sie eine Stelle als Concierge in Hilbert’s Hotel angenommen<sup>3</sup>. An Ihrem ersten Arbeitstag haben Sie die Nachtschicht. Herr Hilbert, der Hotelbesitzer, hat sich bereits zu seinem wohlverdienten Feierabend verabschiedet, als unvermittelt ein älterer Herr (ä.H.) die Lobby betritt.

ä.H.: Ich bräuchte ein Zimmer in Ihrem Hotel.

Sie: Es tut mir leid, wir sind voll belegt. Ich könnte Ihnen aber das Hotel “Cantors Paradise” empfehlen. Es ist hier ganz in der Nähe, hier steht die Adresse.

*Sie überreichen dem ä.H. eine Visitenkarte vom “Cantors Paradise”.*

ä.H.: Mein lieber Concierge, laut Werbebroschüre hat Ihr Hotel unendlich viele Zimmer. Wie soll denn das bitte ausgebucht sein?

---

<sup>3</sup>Sie verdienen schliesslich für jedes Zimmer einen Franken pro Arbeitstag.

Sie: Na ja, wir haben im Moment unendlich viele Gäste – in jedem Zimmer einen.

ä.H.: Das lass ich mal Ihr Problem sein! Mir genügt es, dass hier schwarz auf weiss steht, dass man angeblich keine Reservation zu tätigen braucht, um in diesem Hotel unterzukommen. Zudem werben Sie, mit Bezugnahme auf die Unendlichkeit Ihres Hotels, damit, dass jedem Gast und zu jeder Zeit ein Zimmer garantiert werden kann!

*Der ä.H. kramt generot seine Werbebroschüre hervor und zeigt sichtlich irritiert auf die entsprechende Seite.*

Sie: Hmm, ich werde sehen, ob sich da vielleicht doch was machen lässt. Bitte gedulden Sie sich einen Moment.

*Der ä.H. lässt sich auf die grosse Couch fallen, die in der Eingangshalle steht. Sie, nicht ohne ein ziemlich ungutes Gefühl dabei zu haben, wählen Hilberts private Telefonnummer.*

Hi.: Hilbert am Apparat.

Sie: Entschuldigen Sie die späte Störung Herr Hilbert. Es ist mir unendlich unangenehm, aber ich habe hier im Hotel ein Problem.

Hi. Worum geht es denn?

Sie: Ich habe einen Gast, der trotz Vollbelegung auf ein Zimmer besteht. Und er kann sich erst noch auf unsere eigene Broschüre stützen, in der ja steht, dass wir nie ausgebucht seien, selbst dann nicht, wenn wir mal voll sein sollten!

Hi.: Ach ja, ich hatte vergessen Sie darauf aufmerksam zu machen. Alle unsere Gäste haben sich beim Bezug ihres Zimmers, im Kleingedruckten, damit einverstanden erklärt, dass wir sie im Notfall ein einziges Mal umplatzen können. Nutzen Sie diese Klausel um unserem Gast ein Zimmer freizumachen. Noch etwas, machen Sie das Zimmer so frei, dass sie weitere Gäste, die vielleicht später noch kommen, ebenfalls noch unterbringen könnten und bedenken Sie stets, dass jeder Gast höchstens einmal umplatziert werden darf.

*Sie beenden das Gespräch und wenden sich dem ungeduldig wartenden ä.H. zu.*

Sie: Sehr geehrter Herr, wir haben ein Zimmer für Sie gefunden, sie müssen sich bloss zwei Minuten gedulden, dann können Sie einziehen.

ä.H.: Sehen Sie, geht doch!

Wie bringen Sie den ä.H. unter? Bringen Sie weitere Gäste unter? Was machen Sie, wenn ein voller Limesbus (ein Bus mit unendlich vielen Sitzplätzen) ankommt? Wie lange dauert es bis der ganze Limesbus untergebracht wird?

**Definition 33.**

- Eine Menge  $X$  heisst *endlich*, falls  $X = \emptyset$  oder eine natürliche Zahl  $n \geq 1$  und eine bijektive Funktion  $f : X \rightarrow \{1, \dots, n\}$  existieren. Ist  $X \neq \emptyset$  eine endliche Menge, dann existiert eine Darstellung der Form  $X = \{x_1, x_2, \dots, x_n\}$  wobei die Elemente  $x_i$  paarweise verschieden sind (d.h. es gilt  $i \neq j \Rightarrow x_i \neq x_j$ ). In diesem Fall hat die Menge  $X$  genau  $n$  viele Elemente und wir schreiben  $|X| = n$ . Weiter schreiben wir  $|\emptyset| = 0$ .
- Nicht endliche Mengen nennen wir *unendlich*.
- Eine Menge  $X$  heisst *abzählbar*, wenn eine surjektive Funktion  $F : \mathbb{N} \rightarrow X$  existiert oder wenn  $X = \emptyset$  gilt.
- Die Menge  $X$  heisst *abzählbar unendlich*, wenn  $X$  abzählbar und unendlich ist.
- Eine *überabzählbare* Menge ist eine Menge, die nicht abzählbar ist.

**Bemerkung 34.** Ähnlich wie im Fall von endlichen Mengen ist jede nichtleere abzählbare Menge  $X$  von der Form

$$X = \{a_0, a_1, a_2, \dots\} = \{a_i \mid i \in \mathbb{N}\}.$$

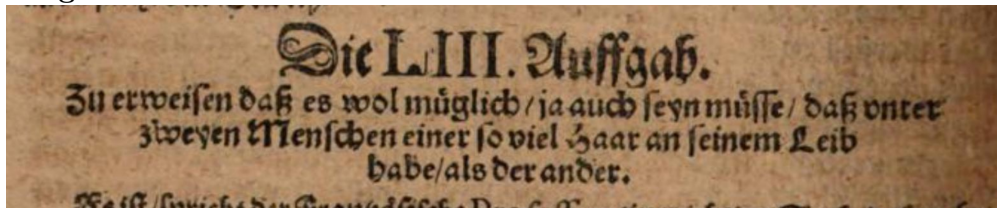
Den Zusammenhang zu Definition 33 liefert hier die Funktion  $F : \mathbb{N} \rightarrow X$ , die durch  $F(i) = a_i$  gegeben ist.

**Bemerkung 35.** Abzählbare Mengen kann man sich auch als die Mengen vorstellen, deren Elemente von den natürlichen Zahlen durchnummeriert (Wiederholungen erlaubt) werden können. Die Elemente einer abzählbaren Menge lassen sich also in eine Liste schreiben, die für jede natürliche Zahl eine Zeile hat.

$\mathbb{N}$	$X$
0	$x$
1	$y$
2	$z$
$\vdots$	$\vdots$

**Lemma 2** (Schubfachprinzip). *Wenn  $n$  Objekte auf  $m$  Behälter verteilt werden und  $n > m$  gilt, dann gibt es mindestens einen Behälter, der mehr als ein Objekt enthält. Formal, sind  $n > m$  natürliche Zahlen und gelte  $|X| = n$  sowie  $|Y| = m$ , dann gibt es keine injektive Funktion*

$$F : X \rightarrow Y.$$

**Übung 21.**


**Lösung.**

**Lemma 3.** *Gibt es eine injektive Funktion  $F : \mathbb{N} \rightarrow A$ , dann ist die Menge  $A$  unendlich.*

*Beweis.* Es sei eine Menge  $A$  und eine injektive Funktion  $F : \mathbb{N} \rightarrow A$  gegeben. Wäre die Menge  $A$  endlich, dann gäbe es eine natürliche Zahl  $n$  mit  $|A| = n$ . Die Funktion

$$\begin{aligned} G : \{0, \dots, n\} &\rightarrow A \\ G(x) &= F(x) \end{aligned}$$

wäre injektiv und würde, wegen  $|\{0, \dots, n\}| = n + 1$ , dem Schubfachprinzip widersprechen.  $\square$

**Satz 4.** *Folgende Aussagen sind für unendliche Mengen  $A$  äquivalent:*

- a) *Die Menge  $A$  ist abzählbar.*
- b) *Es gibt eine surjektive Funktion  $F_{\mathbb{N},A} : \mathbb{N} \rightarrow A$ .*
- c) *Es gibt eine injektive Funktion  $F_{A,\mathbb{N}} : A \rightarrow \mathbb{N}$ .*
- d) *Es gibt eine bijektive Funktion  $B_{\mathbb{N},A} : \mathbb{N} \rightarrow A$ .*
- e) *Es gibt eine bijektive Funktion  $B_{A,\mathbb{N}} : A \rightarrow \mathbb{N}$ .*

*Beweis.*

- Die Aussagen in *a)* und *b)* sind per Definition äquivalent.
- Die Aussagen in *d)* und *e)* sind offensichtlich äquivalent (Umkehrfunktion).
- Für die Implikation *c) ⇒ b)*, gehen wir von einer injektiven Funktion  $F_{A,\mathbb{N}} : A \rightarrow \mathbb{N}$  aus. Weil diese Funktion injektiv ist, und weil  $\text{Dom}(F_{A,\mathbb{N}}) = A$  gilt, ist

$$F_{A,\mathbb{N}}^{-1} : \text{Im}(F_{A,\mathbb{N}}) \rightarrow A$$

eine surjektive Funktion. Um eine surjektive Funktion von  $\mathbb{N}$  nach  $A$  zu erhalten, brauchen wir bloss noch die “restlichen” Elemente aus  $\mathbb{N}$  zuzuordnen, dazu wählen wir ein beliebiges Element aus  $a \in A$  und setzen:

$$F_{\mathbb{N},A}(n) = \begin{cases} F_{A,\mathbb{N}}^{-1}(n) & \text{falls } n \in \text{Im}(F_{A,\mathbb{N}}) \\ a & \text{sonst} \end{cases}$$

- Für die Implikation *b) ⇒ d)* müssen wir, ausgehend von einer unendlichen Menge  $A$  und einer surjektiven Abbildung  $F_{\mathbb{N},A} : \mathbb{N} \rightarrow A$ , eine bijektive Abbildung  $B_{\mathbb{N},A} : \mathbb{N} \rightarrow A$  konstruieren. Da uns für einen vollständigen Beweis die Werkzeuge noch fehlen (Rekursion), wollen wir hier bloss eine Beweisskizze präsentieren. Wir definieren die Funktion  $B_{\mathbb{N},A}$  rekursiv wie folgt:

$$\begin{aligned} B_{\mathbb{N},A}(0) &= F_{\mathbb{N},A}(0) \\ B_{\mathbb{N},A}(n+1) &= F_{\mathbb{N},A}(\min\{k \in \mathbb{N} \mid F(k) \neq B_{\mathbb{N},A}(0), \dots, B_{\mathbb{N},A}(n)\}) \end{aligned}$$

Die resultierende Funktion ist auf ganz  $\mathbb{N}$  definiert, weil die Menge  $A$  unendlich ist (würde die Rekursion abbrechen, dann wäre  $A$  von der Form  $\{F_{\mathbb{N},A}(0), \dots, F_{\mathbb{N},A}(m)\}$  für ein  $m \in \mathbb{N}$ ). Die Funktion  $B_{\mathbb{N},A}$  ist surjektiv, weil  $F_{\mathbb{N},A}$  surjektiv ist. Die Injektivität folgt, weil per Konstruktion für alle  $x, y$

$$x < y \Rightarrow B_{\mathbb{N},A}(x) \neq B_{\mathbb{N},A}(y)$$

gilt.

Weil aus *d)* und *e)* alle anderen Aussagen direkt folgen, genügen die gezeigten Implikationen für den Beweis des Satzes. □

**Übung 22.** Die Funktion

$$\begin{aligned} f : \mathbb{N} &\rightarrow \mathbb{N} \\ f(x) &= \begin{cases} \frac{x}{2} & \text{falls } x \text{ gerade} \\ 3x+1 & \text{sonst} \end{cases} \end{aligned}$$

Ist surjektiv aber nicht injektiv. Wenn Sie die Funktion so wie im vorhergehenden Beweis im Schritt von  $F_1$  zu  $B_{\mathbb{N},A}$  anpassen, welchen Funktionswert erhalten Sie dann für die Eingabe 8?

**Lösung.**

**Beispiel 34.** Die Menge aller geraden natürlichen Zahlen ist abzählbar.

*Beweis.* Ist  $G$  die Menge der geraden Zahlen, dann folgt die Behauptung aus der Tatsache, dass die Funktion

$$F : \mathbb{N} \rightarrow G \quad \text{mit} \quad F(n) = 2n$$

jede gerade natürliche Zahl trifft (und somit surjektiv ist).  $\square$

Dass die Menge der geraden natürlichen Zahlen auch anschaulich abzählbar ist, kann man sich etwa mit folgender Auflistung vergegenwärtigen:

$\mathbb{N}$	$G$
0	0
1	2
2	4
$\vdots$	$\vdots$

**Beispiel 35.** Die Menge  $\mathbb{Z}$  der ganzen Zahlen ist abzählbar.

*Beweis.* Wir müssen eine Funktion  $F : \mathbb{N} \rightarrow \mathbb{Z}$  angeben, die jedes Element von  $\mathbb{Z}$  trifft. Dies gelingt uns wie folgt:

$$F(n) = \begin{cases} -\frac{n}{2} & \text{falls } n \text{ gerade} \\ \frac{n+1}{2} & \text{falls } n \text{ ungerade.} \end{cases}$$

$\square$

Anschaulich ergibt sich durch die Funktion  $F$  folgende Auflistung der ganzen Zahlen:

$\mathbb{N}$	$\mathbb{Z}$
0	0
1	1
2	-1
3	2
4	-2
5	3
$\vdots$	$\vdots$

**Beispiel 36.** Die Menge aller *endlichen* Sequenzen der Buchstaben  $a, b$  ist abzählbar unendlich. Eine mögliche Auflistung der endlichen Sequenzen ist etwa durch

$\mathbb{N}$	$X$
0	$a$
1	$b$
2	$aa$
3	$ab$
4	$ba$
5	$bb$
6	$aaa$
7	$aab$
8	$aba$
9	$abb$
$\vdots$	$\vdots$

gegeben.

**Beispiel 37.** Die Menge aller Java, C, C#, C++, Fortran... Programme ist abzählbar.

*Beweis.* Wenn jedes Programm mit seinem Bytecode identifiziert wird, dann entspricht jedes Programm einer endlichen 0, 1-Folge. Diese können, gleich wie endliche  $a, b$ -Sequenzen, abgezählt werden.  $\square$

**Satz 5.** Jede endliche Menge ist abzählbar.

*Beweis.* Ist  $X$  eine endliche Menge, dann können wir  $X$  als  $\{x_1, \dots, x_n\}$  mit einer natürlichen Zahl  $n$  schreiben. Da die leere Menge per Definition abzählbar ist, können wir annehmen, dass  $X$  mindestens ein Element  $x_1$  besitzt. Wir definieren nun die Funktion  $F : \mathbb{N} \rightarrow X$  mit

$$F(i) = \begin{cases} x_i & \text{falls } 0 < i \leq n \\ x_1 & \text{sonst.} \end{cases}$$

Da  $F$  offensichtlich jedes Element von  $X = \{x_1 \dots x_n\}$  trifft, ist  $F$  surjektiv. Somit ist  $X$  abzählbar.  $\square$

**Satz 6.** Jede Teilmenge einer abzählbaren Menge ist abzählbar.

*Beweis.* Es sei  $X \subseteq Y$  und  $Y$  sei eine abzählbare Menge. Da  $Y$  abzählbar ist, gibt es eine surjektive Funktion  $F : \mathbb{N} \rightarrow Y$ . Wenn  $X = \emptyset$  gilt, dann ist  $X$  per Definition abzählbar und wir sind fertig. Ist  $X \neq \emptyset$ , dann gibt es ein Element  $a \in X$ . Wir können nun wie folgt eine Abbildung  $G : \mathbb{N} \rightarrow X$  angeben.

$$G(x) = \begin{cases} F(x) & \text{falls } F(x) \in X \\ a & \text{sonst.} \end{cases}$$

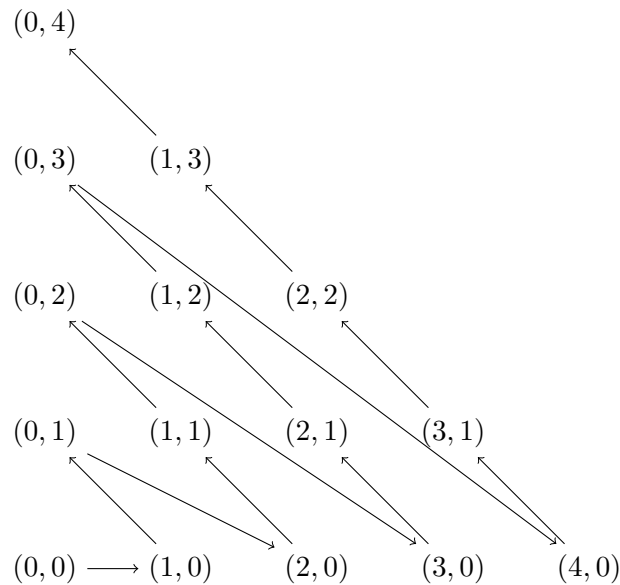
Da  $X \subseteq Y$  gilt und weil jedes Element von  $Y$  von der Funktion  $F$  getroffen wird, wird auch jedes Element von  $X$  von  $G$  getroffen. Somit ist  $G : \mathbb{N} \rightarrow X$  surjektiv und  $X$  ist also abzählbar.  $\square$

**Satz 7.** Ist  $X$  eine abzählbare Menge und gibt es eine surjektive Funktion  $F : X \rightarrow Y$ , dann ist auch  $Y$  abzählbar.

*Beweis.* Diese Behauptung folgt sofort aus Lemma 1 (die Komposition von surjektiven Funktionen ist wieder surjektiv).  $\square$

**Satz 8** (Erstes Diagonalargument). Die Menge  $\mathbb{N} \times \mathbb{N}$ , bestehend aus allen Paaren von natürlichen Zahlen, ist abzählbar.

*Beweisidee.* Anstelle eines formalen Beweises, skizzieren wir eine Abzählung aller Paare von natürlichen Zahlen wie folgt:



$\square$

**Satz 9.** Jede Vereinigung von abzählbar vielen abzählbaren Mengen ist abzählbar. Konkret, jede Vereinigung von der Form

$$\bigcup_{i \in \mathbb{N}} A_i$$

ist abzählbar, wenn alle  $A_i$ 's abzählbar sind.

*Beweis.* Wir nehmen an, dass die Menge  $\{A_i \mid i \in \mathbb{N}\}$  aus lauter abzählbaren Mengen besteht. Um zu zeigen, dass  $\bigcup_{i \in \mathbb{N}} A_i$  abzählbar ist, genügt es, aufgrund von Satz 7 und Satz 8, zu zeigen, dass es eine surjektive Funktion

$$H : \mathbb{N} \times \mathbb{N} \rightarrow \bigcup_{i \in \mathbb{N}} A_i$$



gibt. Da für jede natürliche Zahl  $i$  die Menge  $A_i$  abzählbar ist, gibt es für jede natürliche Zahl  $i$  auch eine surjektive Funktion  $F_i : \mathbb{N} \rightarrow A_i$ . Wir können die Vereinigungsmenge der  $A_i$ 's also wie folgt schreiben:

$$\begin{aligned} \bigcup_{i \in \mathbb{N}} A_i &= \{F_i(j) \mid i, j \in \mathbb{N}\} \\ &= \{F_i(j) \mid (i, j) \in \mathbb{N} \times \mathbb{N}\}. \end{aligned}$$

Daraus folgt, dass die Funktion

$$H : \mathbb{N} \times \mathbb{N} \rightarrow \bigcup_{i \in \mathbb{N}} A_i \quad \text{mit} \quad H(i, j) = F_i(j),$$

die gesuchte surjektive Funktion ist. □

**Folgerung.** Die Menge  $\mathbb{Z} \times \mathbb{Z}$  ist abzählbar.

*Beweis.* Wir wissen bereits, dass die Menge  $\mathbb{N} \times \mathbb{N}$  abzählbar ist. Daraus folgt, dass auch die Mengen

$$\begin{aligned} X &= \mathbb{N} \times \{-n \mid n \in \mathbb{N}\} \\ Y &= \{-n \mid n \in \mathbb{N}\} \times \mathbb{N} \\ Z &= \{-n \mid n \in \mathbb{N}\} \times \{-n \mid n \in \mathbb{N}\} \end{aligned}$$

abzählbar sind. Aus Satz 9 folgt also, dass die Menge

$$\mathbb{Z} \times \mathbb{Z} = (\mathbb{N} \times \mathbb{N}) \cup X \cup Y \cup Z$$

abzählbar ist. □

**Folgerung.** Die Menge  $\mathbb{Q} = \{\frac{x}{y} \mid x, y \in \mathbb{Z}\}$  der rationalen Zahlen (Brüche) ist abzählbar.

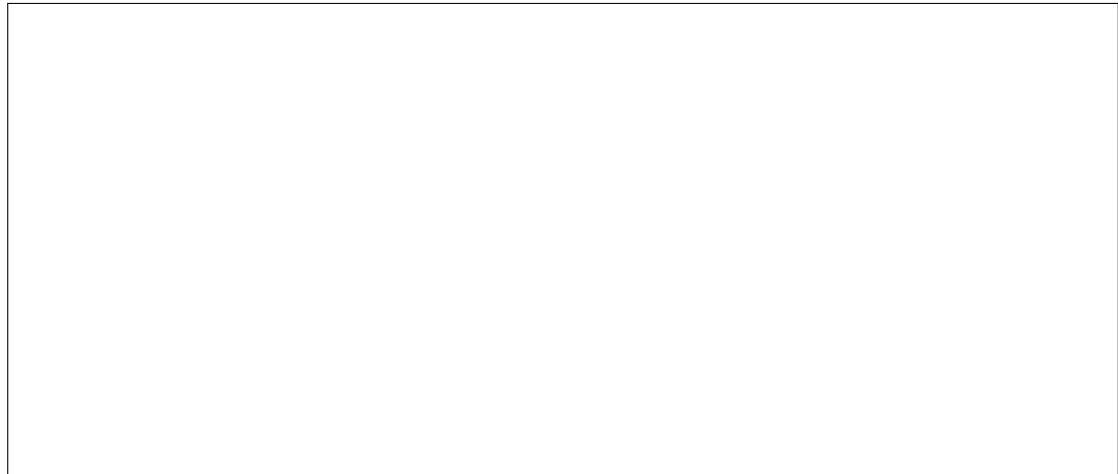
*Beweis.* Da die Funktion

$$F : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \rightarrow \mathbb{Q} \quad \text{mit} \quad F(x, y) = \frac{x}{y}$$

surjektiv ist, folgt die Behauptung aus Satz 7. □

**Übung 23.** Ist die Menge aller endlichen Teilmengen von  $\mathbb{N}$  abzählbar? Begründen Sie Ihre Antwort.

**Lösung.**



**Theorem 2** (Zweites Diagonalargument). *Die Menge aller unendlichen Binärsequenzen (Sequenzen aus Nullen und Einsen) ist überabzählbar.*

*Beweis.* Beweis durch Widerspruch. Wäre die Menge aller unendlichen Binärsequenzen abzählbar, dann gäbe es eine Liste von der Form<sup>4</sup>

$\mathbb{N}$	Binärsequenzen
0	$s_0 = 01101011 \dots$
1	$s_1 = 10010110 \dots$
2	$s_2 = 00101001 \dots$
$\vdots$	$\vdots$

in der alle unendlichen Binärsequenzen vorkommen. Wir konstruieren nun, ausgehend von dieser Liste, eine Binärsequenz  $b$ , die nicht in der Liste enthalten sein kann. Wir definieren  $b$  wie folgt:

$$0\text{-tes Glied} = b(0) = 1 - s_0(0)$$

$$1\text{-tes Glied} = b(1) = 1 - s_1(1)$$

$$2\text{-tes Glied} = b(2) = 1 - s_2(2)$$

$$\vdots$$

$$n\text{-tes Glied} = b(n) = 1 - s_n(n)$$

$$\vdots$$

Die Folge  $b = 110 \dots$  kann nicht in der Liste vorkommen, weil sie sich von jedem Element in der Liste in mindestens einem Glied unterscheidet (von der  $n$ -ten Sequenz unterscheidet sich  $b$  im  $n$ -ten Glied). Dies steht im Widerspruch zu unserer Annahme, dass in der Liste alle unendlichen Binärsequenzen vorkommen.  $\square$

---

<sup>4</sup>Natürlich ist die angedeutete Liste Beispielhaft und dient nur der Veranschaulichung unserer Konstruktion der Sequenz  $b$ . Die Sequenz  $s_0$ , beispielsweise, könnte auch mit dem Präfix 00000100 oder irgend einer anderen Folge von Nullen und Einsen beginnen.

**Folgerung.** Das Intervall  $(0, 1) = \{r \in \mathbb{R} \mid 0 < r < 1\}$  ist überabzählbar. Insbesondere ist die Menge  $\mathbb{R}$  der reellen Zahlen überabzählbar.

*Beweis.* Die reellen Zahlen (in Binärdarstellung) im Intervall  $(0, 1)$ , sind von der Form  $0, \dots$  wobei  $\dots$  für eine unendliche Binärsequenz steht. Daher steht das Intervall  $(0, 1)$  mit der Menge aller unendlichen Binärsequenzen in eins-zu-eins Korrespondenz. Die Behauptung folgt daher aus Theorem 2.  $\square$

**Folgerung.** Die Potenzmenge von  $\mathbb{N}$  ist überabzählbar.

*Beweis.* Jede Teilmenge  $A$  von  $\mathbb{N}$  kann wie folgt durch eine Binärsequenz  $\chi_A$  beschrieben werden:

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

Daher folgt die Behauptung aus Theorem 2.  $\square$

**Folgerung.** Die Menge aller Funktionen  $F : \mathbb{N} \rightarrow \mathbb{N}$  ist überabzählbar.

*Beweis.* Die Menge der Binärsequenzen entspricht der Menge der Funktionen  $F : \mathbb{N} \rightarrow \{0, 1\}$ . Daher folgt die Behauptung aus Theorem 2.  $\square$

**Folgerung.** Es gibt Funktionen  $F : \mathbb{N} \rightarrow \mathbb{N}$ , die von keinem Java, C, C++, Fortran... Programm berechenbar sind. Solche Funktionen heissen unberechenbar.

**Übung 24.** Zeigen Sie, dass die Menge

$$U = \{1, 11, 111, 1111, \dots\}$$

aller endlichen Sequenzen von Einsen abzählbar ist. Ist die Menge aller unendlichen<sup>5</sup> Sequenzen von Einsen auch abzählbar?

**Lösung.**

---

<sup>5</sup>Streng genommen müsste man hier nach der Menge der “abzählbar langen” Sequenzen von Einsen fragen.

### 3.2.3 Ordnungs- und Äquivalenzrelationen

Neben den Funktionen und ihren Anwendungen gibt es in der Mathematik noch zahlreiche weitere wichtige Klassen von Relationen. Im Folgenden wollen wir auch aufgrund ihrer Wichtigkeit in der Informatik die Ordnungsrelationen (inklusive Halbordnungen) und Äquivalenzrelationen etwas genauer betrachten. Wie viele Typen von Relationen werden auch Ordnungen und Äquivalenzen aufgrund von bestimmten Kombinationen von Grundeigenschaften definiert. Folgend einige wichtige solche Grundeigenschaften.

**Definition 34.** Eine binäre Relation  $R$  auf einer Menge  $X$  heisst:

- *Reflexiv*, wenn für alle  $x \in X$

$$xRx$$

gilt.

- *Symmetrisch*, wenn für alle  $x, y \in X$

$$xRy \Rightarrow yRx$$

gilt.

- *Antisymmetrisch*, wenn für alle  $x, y \in X$

$$xRy \wedge yRx \Rightarrow x = y$$

gilt.

- *Transitiv*, wenn für alle  $x, y, z \in X$

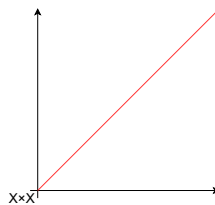
$$xRy \wedge yRz \Rightarrow xRz$$

gilt.

**Bemerkung 36.** Die Relation  $R \subseteq X \times X$  ist genau dann reflexiv, wenn die Diagonale

$$\Delta_X := \{(x, x) \mid x \in X\}$$

eine Teilmenge von  $R$  ist. Grafisch heisst das, dass die Diagonale (rot markiert) in  $R$  enthalten ist.



Die Relation  $R$  ist symmetrisch, wenn ihr Graph symmetrisch bezüglich der Geraden  $\Delta_X$  ist.

**Beispiel 38.** Wir betrachten nochmals die Verliebtheitsrelation aus Beispiel 27:

$$pLq :\Leftrightarrow \text{Person } p \text{ liebt Person } q.$$

Die Verliebtheitsrelation hat unter anderem folgende Eigenschaften:

- $L$  ist nicht reflexiv, da nicht alle Menschen “selbstverliebt” sind.
- $L$  ist (leider<sup>6</sup>) nicht symmetrisch, da Liebe nicht immer auf Gegenseitigkeit beruht.
- $L$  ist nicht Antisymmetrisch, da es durchaus “echte” Liebespaare (aus zwei Partnern bestehend) gibt.
- $L$  ist nicht transitiv, da die meisten Leute den angebeteten der eigenen angebeteten nicht lieben (ganz im Gegenteil!).

**Übung 25.** Geben Sie binäre Relationen (auf der Menge aller Menschen) mit folgenden Eigenschaften an:

- a) Transitiv und nicht antisymmetrisch.
- b) Transitiv, reflexiv und antisymmetrisch.
- c) Nicht reflexiv, nicht transitiv.

**Lösung.**

---

<sup>6</sup> Andererseits gäbe es wohl keine Literatur oder gar Kunst, wenn diese Relation tatsächlich symmetrisch wäre.

### Äquivalenzrelationen

Äquivalenzrelationen sind in einem gewissen Sinn (konkret im Sinn von Satz 13) verallgemeinerte Gleichheitsrelationen. Sie werden dazu verwendet, (im Sinn der Relation) ähnliche Objekte miteinander zu identifizieren und als “gleich” zu behandeln.

**Definition 35.** *Äquivalenzrelationen* sind reflexive, symmetrische und transitive Relationen.

**Beispiel 39.** Auf jeder Menge  $X$  ist die Gleichheitsrelation  $\Delta_X = \{(x, x) \mid x \in X\}$  eine Äquivalenzrelation. Weil jede Äquivalenzrelation reflexiv ist, ist die Gleichheitsrelation auf jeder Menge die “kleinste” Äquivalenzrelation. Am anderen Ende des Spektrums steht die Relation  $X \times X$ , sie ist die grösste Äquivalenzrelation auf der Menge  $X$ .

**Beispiel 40.** Von den Relationen  $R_1, R_2, R_3$  und  $T$  aus Beispiel 27, sind  $R_1, R_2$  Äquivalenzrelationen.

- Die Relation  $R_3$  ist keine Äquivalenzrelation, weil sie nicht reflexiv (nicht jeder liebt sich selbst), nicht symmetrisch (es gibt unglücklich Verliebte) und nicht transitiv ist. Man beachte, dass jeder einzelne der genannten Gründe genügt, damit  $R_3$  keine Äquivalenzrelation ist.
- Die Relation  $T$  ist zwar reflexiv und transitiv, aber nicht symmetrisch und daher auch keine Äquivalenzrelation.

**Definition 36.** Es sei  $R$  eine Äquivalenzrelation auf einer Menge  $X$  und  $x \in X$ . Die *Äquivalenzklasse*  $[x]_R$  von  $x$  bezüglich  $R$  ist die Menge aller Elemente von  $X$ , die zu  $x$  in Relation  $R$  stehen:

$$[x]_R := \{y \in X \mid xRy\}$$

Jedes Element einer Äquivalenzklasse nennen wir einen *Repräsentanten* der entsprechenden Äquivalenzklasse. Die *Faktormenge*  $X/R$  von  $X$  modulo  $R$  ist die Menge aller Äquivalenzklassen:

$$X/R := \{[x]_R \mid x \in X\}$$

**Beispiel 41.** Wir betrachten die Relation  $\equiv_5$  auf der Menge  $\mathbb{Z}$ , die wie folgt gegeben ist:

$$x \equiv_5 y :\Leftrightarrow (x - y) \text{ ist ein Vielfaches von } 5.$$

Als Java Code könnte man die Relation auch wie folgt darstellen:

```
static boolean Rel(int x, int y){
    if (y<0) return Rel(x,y+5);
    if (x<0) return Rel(x+5,y);
    if (y>=5) return Rel(x,y-5);
    if (x>=5) return Rel(x-5,y);
    return x == y;
}
```

Wir überzeugen uns nun davon, dass diese Relation eine Äquivalenzrelation ist.

- **Reflexivität:** Es gilt für jede ganze Zahl  $z$

$$0 \cdot 5 = 0 = (z - z).$$

Also ist  $(z - z)$  ein Vielfaches von 5, somit gilt  $z \equiv_5 z$ .

- **Symmetrie:** Gilt  $x \equiv_5 y$ , dann gibt es eine ganze Zahl  $z$  mit  $5z = (x - y)$ . Also ist auch

$$(y - x) = -(x - y) = -5z = 5 \cdot (-z)$$

ein Vielfaches von 5, d.h. es gilt  $y \equiv_5 x$ .

- **Transitivität:** Gilt  $x \equiv_5 y$  und  $y \equiv_5 z$ , dann gibt es ganze Zahlen  $r, s$  mit  $5r = x - y$  und  $5s = y - z$ . Insgesamt erhalten wir, dass

$$x - z = (x - y) + (y - z) = 5r + 5s = 5(r + s)$$

ein Vielfaches von 5 ist und somit, dass  $x \equiv_5 z$  gilt.

Wir betrachten nun die Äquivalenzklassen modulo der Relation  $\equiv_5$  (diese heissen Rest-

klassen modulo 5).

$$\begin{aligned}[0]_{\equiv_5} &= \{x \in \mathbb{Z} \mid 0 \equiv_5 y\} \\ &= \{z \in \mathbb{Z} \mid z \text{ ist ein Vielfaches von } 5\} \\ &= \{5z \mid z \in \mathbb{Z}\}\end{aligned}$$

$$\begin{aligned}[1]_{\equiv_5} &= \{x \in \mathbb{Z} \mid 1 \equiv_5 y\} \\ &= \{z \in \mathbb{Z} \mid \text{Bei Division durch } 5 \text{ lässt } z \text{ den Rest } 1\} \\ &= \{5z + 1 \mid z \in \mathbb{Z}\}\end{aligned}$$

$$\begin{aligned}[2]_{\equiv_5} &= \{x \in \mathbb{Z} \mid 2 \equiv_5 y\} \\ &= \{z \in \mathbb{Z} \mid \text{Bei Division durch } 5 \text{ lässt } z \text{ den Rest } 2\} \\ &= \{5z + 2 \mid z \in \mathbb{Z}\}\end{aligned}$$

$$\begin{aligned}[3]_{\equiv_5} &= \{x \in \mathbb{Z} \mid 3 \equiv_5 y\} \\ &= \{z \in \mathbb{Z} \mid \text{Bei Division durch } 5 \text{ lässt } z \text{ den Rest } 3\} \\ &= \{5z + 3 \mid z \in \mathbb{Z}\}\end{aligned}$$

$$\begin{aligned}[4]_{\equiv_5} &= \{x \in \mathbb{Z} \mid 4 \equiv_5 y\} \\ &= \{z \in \mathbb{Z} \mid \text{Bei Division durch } 5 \text{ lässt } z \text{ den Rest } 4\} \\ &= \{5z + 4 \mid z \in \mathbb{Z}\}\end{aligned}$$

Die Faktormenge der Relation  $\equiv_5$  ist also durch

$$\mathbb{Z}/\equiv_5 = \{[0]_{\equiv_5}, [1]_{\equiv_5}, [2]_{\equiv_5}, [3]_{\equiv_5}, [4]_{\equiv_5}\}$$

gegeben.

**Lemma 4.** *Ist  $\sim$  eine Äquivalenzrelation auf einer Menge  $X$  und gilt  $x, y \in X$  mit  $x \sim y$ , dann gilt  $[x]_{\sim} = [y]_{\sim}$ . Mit anderen Worten, äquivalente Elemente repräsentieren stets dieselbe Äquivalenzklasse.*

*Beweis.* Seien  $X, \sim, x, y$  wie in der Behauptung. Um zu zeigen, dass  $[x]_{\sim} = [y]_{\sim}$  gilt, genügt es nachzuweisen, dass  $x \sim z \Leftrightarrow y \sim z$  für beliebige  $z \in X$  gilt. Wir nehmen  $x \sim y$  an, dann gilt

$$y \sim z \Rightarrow x \sim y \wedge y \sim z \xrightarrow{\text{Transitivität}} x \sim z$$

und

$$x \sim z \Rightarrow x \sim y \wedge x \sim z \xrightarrow{\text{Symmetrie}} y \sim x \wedge x \sim z \xrightarrow{\text{Transitivität}} y \sim z,$$

wie gewünscht. □



**Folgerung.** Ist  $\sim$  eine Äquivalenzrelation auf  $X$  und sind  $x, y \in X$  mit  $x \in [y]_\sim$ , dann gilt  $[x]_\sim = [y]_\sim$ . Mit anderen Worten, jedes Element einer Äquivalenzklasse ist auch ein Repräsentant dieser Äquivalenzklasse.

*Beweis.* Es seien  $X, \sim, x$  und  $y$  wie in der Behauptung. Aus  $x \in [y]_\sim$  folgt  $y \sim x$ . Die Behauptung folgt nun aus Lemma 4.  $\square$

**Satz 10.** Ist  $\sim$  eine Äquivalenzrelation auf  $X$  und sind  $x, y \in X$  mit  $[x]_\sim \neq [y]_\sim$ , dann gilt  $[x]_\sim \cap [y]_\sim = \emptyset$ . Mit anderen Worten, verschiedene Äquivalenzklassen sind immer disjunkt.

*Beweis.* Es seien  $X, \sim, x$  und  $y$  wie in der Behauptung. Wir zeigen die Kontraposition, d.h.

$$[x]_\sim \cap [y]_\sim \neq \emptyset \Rightarrow [x]_\sim = [y]_\sim.$$

Es gelte also  $[x]_\sim \cap [y]_\sim \neq \emptyset$ , es gibt daher ein  $z \in [x]_\sim \cap [y]_\sim$ . Daraus folgt, dass  $x \sim z \wedge y \sim z$  gilt und wegen der Transitivität und der Symmetrie von  $\sim$  folgt sofort  $x \sim y$ . Die Behauptung folgt nun aus Lemma 4.  $\square$

**Satz 11.** Ist  $\sim$  eine Äquivalenzrelation auf einer Menge  $X$ , dann ist die Faktormenge  $X/\sim$  eine Partition von  $X$ .

*Beweis.* Es sei  $\sim$  eine beliebige Äquivalenzrelation auf einer Menge  $X$ . Wir müssen folgende Punkte verifizieren:

- a) Die Äquivalenzklassen sind alle nichtleer.
- b) Die Äquivalenzklassen sind paarweise disjunkt.
- c) Es gilt

$$\bigcup_{x \in X} [x]_\sim = X.$$

Der erste Punkt folgt aus der Definition von der Faktormenge (die Äquivalenzklassen sind via ihrer Repräsentanten definiert). Die Tatsache, dass die Äquivalenzklassen paarweise disjunkt sind, ist genau die Aussage von Satz 10. Wir brauchen also bloss noch den letzten Punkt zu verifizieren. Dies folgt, da für jedes  $z \in X$ , wegen der Reflexivität,  $z \sim z$  und somit

$$z \in [z]_\sim \subseteq \bigcup_{x \in X} [x]_\sim$$

gilt.  $\square$

**Bemerkung 37.** Das Konzept von Äquivalenzklassen (und deren Zusammenhang mit Partitionen) werden Sie in der theoretischen Informatik in Form von sogenannten “Zustandsklassen” wiederfinden, diese werden dort gebraucht, um zu zeigen, dass es Sprachen gibt, die nicht mit “endlichen Zustandsautomaten” erkannt werden können.

**Übung 26.** Gegeben Sei die Äquivalenzrelation

$$pRq :\Leftrightarrow p \text{ hat am gleichen Tag Geburtstag wie } q.$$

Kommentieren Sie folgende Aussagen mit “wahr”, “falsch” oder “unklar” unter der Annahme *Ray R Greg*:

- a) Ray ist älter als Greg oder Greg ist älter als Ray.
- b) Ray und Greg sind gleich alt.
- c) Ray ist verwandt mit Greg.
- d) Der Altersunterschied von Ray und Greg in Jahren ist ganzzahlig.

**Lösung.**

**Übung 27.** Wie viele Äquivalenzklassen hat die Relation  $R$  von Übung 26?

**Lösung.**

Wir haben in Satz 11 gesehen, dass jede Äquivalenzrelation auf einer Menge eine Partition auf eben dieser Menge induziert. Als Nächstes sehen wir, dass auch die Umkehrung gilt; jede Partition induziert eine Äquivalenzrelation, deren Faktormenge genau der ursprünglichen Partition entspricht. Insgesamt sehen wir, dass eine eins-zu-eins Korrespondenz zwischen allen möglichen Partitionen und allen möglichen Äquivalenzrelationen auf einer gegebenen Menge existiert.

**Satz 12.** Ist  $P = \{A_i \mid i \in I\}$  eine Partition von der Menge  $X$ , dann ist die Relation  $\sim$ , gegeben durch

$$x \sim y :\Leftrightarrow \exists i \in I (x \in A_i \wedge y \in A_i),$$

eine Äquivalenzrelation auf  $X$ . Zusätzlich gilt

$$X/\sim = P.$$

*Beweis.* Zuerst zeigen wir, dass die Relation  $\sim$  unter den gegebenen Umständen eine Äquivalenzrelation ist.

- **Reflexivität:** Sei  $x \in X$  beliebig. Wir müssen zeigen, dass  $x \sim x$  gilt. Da  $P = \{A_i \mid i \in I\}$  eine Partition von  $X$  ist, gibt es ein  $i \in I$  mit  $x \in A_i$ , daraus folgt sofort  $x \sim x$ .
- **Symmetrie:** Es gelte  $x \sim y$ . Wir müssen  $y \sim x$  zeigen. Aus  $x \sim y$  folgt, dass es ein  $i \in I$  mit  $x \in A_i \wedge y \in A_i$  gibt, dies ist offensichtlich äquivalent zu  $y \sim x$ .
- **Transitivität:** Es gelte  $x \sim y \wedge y \sim z$ . Wir müssen  $x \sim z$  zeigen. Aus  $x \sim y \wedge y \sim z$  folgt, dass es  $i, j \in I$  gibt so, dass  $x, y \in A_i$  und  $y, z \in A_j$  gilt. Da  $P = \{A_i \mid i \in I\}$  eine Partition ist, kann  $y$  nicht in zwei verschiedenen Blöcken enthalten sein, es gilt daher  $i = j$  und somit  $x \sim z$ .

Dass die Äquivalenzklassen von  $\sim$  genau den Blöcken von  $P$  entsprechen ist sofort klar, wenn man beachtet, dass zwei Elemente genau dann äquivalent sind, wenn sie im selben Block von  $P$  liegen.  $\square$

Am Anfang dieses Abschnittes haben wir Äquivalenzrelationen als verallgemeinerte Gleichheitsrelationen beschrieben, dies können wir im folgenden Satz präzisieren.

**Satz 13.** *Für jede Relation  $\sim$  auf einer Menge  $X$  sind folgende beiden Aussagen äquivalent.*

1. *Die Relation  $\sim$  ist eine Äquivalenzrelation.*
2. *Es gibt eine Menge  $Y$  und eine Funktion  $F : X \rightarrow Y$  so, dass für alle  $x, y \in X$*

$$x \sim y \Leftrightarrow F(x) = F(y)$$

*gilt.*

*Beweis.* Wenn  $\sim$  eine Äquivalenzrelation auf der Menge  $X$  ist, dann erfüllt die Abbildung

$$F : X \rightarrow \mathcal{P}(X) \quad \text{mit} \quad F(x) = [x]_{\sim}$$

alle geforderten Eigenschaften. Ist umgekehrt eine Funktion  $F : X \rightarrow Y$  wie in der Behauptung gegeben, dann gilt für die Relation  $\sim$  Folgendes:

- **Reflexivität** gilt, da für jedes Element  $x \in X$  trivialerweise  $F(x) = F(x)$  gilt.
- **Symmetrie** folgt, da für beliebige Elemente  $x, y \in X$

$$x \sim y \Rightarrow F(x) = F(y) \Rightarrow F(y) = F(x) \Rightarrow y \sim x$$

*gilt.*

- **Transitivität** folgt, da für beliebige Elemente  $x, y, z \in X$

$$x \sim y \wedge y \sim z \Rightarrow F(x) = F(y) \wedge F(y) = F(z) \Rightarrow F(x) = F(z) \Rightarrow x \sim z$$

gilt.

□

**Beispiel 42.** Es sei  $\sim_{14}$  die folgendermassen auf der Menge  $Fun(\mathbb{R}) = \{F \mid F : \mathbb{R} \rightarrow \mathbb{R}\}$  gegebene Relation:

$$F \sim G :\Leftrightarrow F(14) = G(14).$$

Wir betrachten die Funktion

$$Eval_{14} : Fun(\mathbb{R}) \rightarrow \mathbb{R} \quad \text{mit} \quad Eval_{14}(F) = F(14).$$

Offenbar gilt

$$F \sim_{14} G \Leftrightarrow Eval_{14}(F) = Eval_{14}(G).$$

Anhand von Satz 13 sehen wir also sofort, dass es sich bei  $\sim_{14}$  um eine Äquivalenzrelation handelt.

**Bemerkung 38** (Wohldefiniertheitsproblem). Wir betrachten die Relation  $\simeq$ , die auf der Menge  $\mathbb{N}$  folgendermassen gegeben ist.

$$n \simeq m \Leftrightarrow n, m \text{ haben die gleichen Primteiler.}$$

Nun definieren wir eine Funktion

$$F : \mathbb{N}/\simeq \rightarrow \mathbb{N} \quad F([x]_{\simeq}) := x + 102.$$

Es soll zum Beispiel  $F([7]_{\simeq}) = 109$  gelten. Sehen Sie ein Problem bei unserem Vorgehen? Ist  $F([49]_{\simeq}) = 151$ ? Es gilt doch  $7 \simeq 49$  und somit auch  $[7]_{\simeq} = [49]_{\simeq}$ . Sollte dann nicht auch  $F([7]_{\simeq}) = F([49]_{\simeq})$  gelten? Natürlich schon! Das Problem, das wir hier haben, nennt man ein *Wohldefiniertheitsproblem*. Es entsteht, wenn man Funktionswerte von Äquivalenzklassen mit Bezugnahme auf deren Repräsentanten definiert, ohne sicherzustellen, dass der Funktionswert nicht von der Wahl der Repräsentanten abhängt.

Sind eine Äquivalenzrelation  $\sim$  auf einer Menge  $X$  und eine Funktion  $F : X \rightarrow Y$  gegeben, so erhält man nur dann durch die Zuordnung

$$\tilde{F}([x]_{\sim}) := F(x)$$

eine wohldefinierte Funktion

$$\tilde{F} : X/\sim \rightarrow Y,$$

wenn die Funktion  $F$  mit der Relation  $\sim$  verträglich ist. Das heisst, wenn

$$x \sim y \Rightarrow F(x) = F(y)$$

gilt.

**Beispiel 43.** Ein Beispiel (vgl. 41) für eine wohldefinierte Abbildung

$$F : \mathbb{Z}/\equiv_5 \rightarrow \mathbb{Z}/\equiv_5$$

erhalten wir z.B. durch die Zuordnung

$$F([x]_{\equiv_5}) := [2x + 3]_{\equiv_5}.$$

Um zu sehen, dass diese Funktion tatsächlich wohldefiniert ist, betrachten wir:

$$\begin{aligned} x \equiv_5 y &\Rightarrow (x - y) \text{ ist Vielfaches von } 5 \\ &\Rightarrow \exists z \in \mathbb{Z} (5z = x - y) \\ &\Rightarrow \exists z \in \mathbb{Z} ((2x + 3) - (2y + 3) = 2x - 2y = 2(x - y) = 5(2z)) \\ &\Rightarrow (2x + 3) - (2y + 3) \text{ ist ein Vielfaches von } 5 \\ &\Rightarrow [2x + 3]_{\equiv_5} = [2y + 3]_{\equiv_5} \end{aligned}$$

### Ordnungsrelationen

Unter Ordnungsrelationen fasst man alle Arten von Relationen zusammen, mithilfe derer man Objekte in gewisser Weise vergleichen und mehr oder weniger eindeutig sortieren kann. Das Standardbeispiel ist die Ordnungsrelationen  $\leq$  auf den verschiedenen Zahlenmengen.

**Definition 37.** Es sei  $R$  eine binäre Relation auf der Menge  $M$ .

- Zwei Elemente  $x, y \in M$  heißen *R-unvergleichbar*, falls weder  $xRy$  noch  $yRx$  gilt.
- Ein Element  $x \in X$  einer Teilmenge  $X \subseteq M$  von  $M$  heisst *R-minimal in X*, falls es kein anderes Element  $y \in X$  mit  $yRx$  gibt.
- Ein Element  $x \in X$  einer Teilmenge  $X \subseteq M$  von  $M$  heisst *R-maximal in X*, falls es kein anderes Element  $y \in X$  mit  $xRy$  gibt.

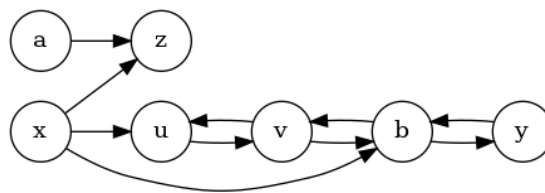
Wenn keine Missverständnisse zu befürchten sind, dann schreiben wir anstelle von *R-minimal*, *R-maximal* und *R-unvergleichbar* auch einfach *minimal*, *maximal* und *unvergleichbar*.

**Übung 28.** Es sei  $R$  die Gleichheitsrelation auf der Menge der natürlichen Zahlen. Welches sind die *R-minimalen* und *R-maximalen* Elemente?

**Lösung.**

**Bemerkung 39.** Es sei  $X$  eine Teilmenge von  $M$  und  $R$  eine binäre Relation auf  $M$ . Die  $R$ -minimalen Elemente von  $X$  entsprechen im Graph  $G = (M, R)$  genau den Knoten, bei denen keine Pfeile enden, die ihren Ursprung in  $X$  haben. Die maximalen Elemente entsprechen den Knoten, von denen alle ausgehenden Pfeile aus der Menge  $X$  “hinauszeigen”. Zwei Elemente  $x, y \in M$  sind  $R$ -unvergleichlich, wenn es keine Pfeile (egal in welcher Richtung) gibt, die  $x$  und  $y$  verbinden.

**Übung 29.** Die Relation  $R$  auf der Menge  $M = \{a, b, u, v, x, y, z\}$  sei durch den Graph  $(M, R)$  wie folgt gegeben.



Geben Sie alle minimalen und maximalen Elemente von  $M$  an. Geben Sie weiter zwei Elemente an, die unvergleichbar sind.

**Lösung.**

**Definition 38.** Es sei  $R$  eine binäre Relation auf der Menge  $M$ .

- $R$  ist eine *Präordnung* auf  $M$ , wenn  $R$  reflexiv und transitiv ist.
- $R$  ist eine *Halbordnung* auf  $M$ , wenn  $R$  reflexiv, antisymmetrisch und transitiv ist.

- $R$  ist eine *totale oder lineare Ordnung* auf  $M$ , wenn  $R$  eine Halbordnung ist und keine  $R$ -unvergleichbaren Elemente existieren.
- $R$  ist eine *Wohlordnung* auf  $M$ , wenn  $R$  eine totale Ordnung auf  $M$  ist so, dass jede Teilmenge  $X \neq \emptyset$  von  $M$  (mindestens) ein  $R$ -minimales Element enthält.

#### Beispiel 44.

- Die Relation  $\leq$  auf der Menge  $\mathbb{R}$  ist eine totale Ordnung, die aber keine Wohlordnung ist (die Menge  $\{x \in \mathbb{R} \mid 0 < x < 1\}$  hat kein kleinstes Element). Auf der Menge  $\mathbb{N}$  ist  $\leq$  eine Wohlordnung<sup>7</sup>. Auf der Menge  $\mathbb{Z}$  ist die Relation  $\leq$  keine Wohlordnung. Wieso?
- Ist  $A$  eine Menge von Mengen, dann ist die Teilmengenrelation  $\subseteq$  eine Halbordnung.
- Die Teilerrelation  $T$  auf der Menge  $\mathbb{Z}$  ist eine Halbordnung aber keine totale Ordnung. Die Elemente 7 und 5 sind  $T$ -unvergleichlich.

**Definition 39.** Es sei  $R$  eine (binäre) Relation.

- Als *transitiven Abschluss* von  $R$  bezeichnet man die kleinste (bezüglich  $\subseteq$ ) transitive Relation, die  $R$  als Teilmenge enthält, sie wird mit  $R^+$  notiert.
- Die kleinste Relation, die  $R^+$  enthält und reflexiv ist, nennt man den *reflexiv-transitiven Abschluss* von  $R$ , sie wird mit  $R^*$  bezeichnet.

**Bemerkung 40.** Für eine beliebige (binäre) Relation  $R$  gilt genau dann  $xR^*y$ , wenn es eine endliche Folge  $x = k_1, \dots, k_n = y$  gibt, so dass  $k_i R k_{i+1}$  für alle Indices  $i = 1, \dots, n-1$  gilt. Es gilt also genau dann  $xR^*y$ , wenn es eine Folge von Elementen gibt, die mit  $x$  beginnt, mit  $y$  endet und deren Elemente alle der Reihe nach in Relation  $R$  zueinander stehen. Ist  $G = (V, E)$  ein Graph, dann bedeutet  $xR^*y$ , dass in  $G$  ein Pfad von  $x$  nach  $y$  existiert.

**Definition 40.** Ein *Weg* oder *Pfad* in einem Graph  $G = (V, E)$  ist eine endliche Folge  $k_1, \dots, k_n \in V$  von Knoten, so dass  $k_i E k_{i+1}$  für alle Indices  $i = 1, \dots, n-1$  gilt. Die Knoten  $k_1$  und  $k_n$  bezeichnet man als *Anfangs-* und *Endpunkt* des Pfades. Gilt zusätzlich  $k_1 = k_n$ , dann spricht man von einem *Zyklus*.

<sup>7</sup>Ein Beweis dazu kommt im nächsten Kapitel.

**Bemerkung 41.** In der Informatik wichtige Datenstrukturen sind sogenannte *DAGs* (von “directed acyclic graph”), gerichtete zyklensfreie Graphen. Eine der charakteristischen Eigenschaften von DAG’s ist die Tatsache, dass sich ihre Elemente auf eine mit der Struktur des Graphen verträgliche Art sortieren lassen. Oft werden Abhängigkeiten von einzelnen Arbeitsschritten eines Prozesses als DAG modelliert, eine mit der Struktur des Graphen verträgliche lineare Ordnung der Knoten entspricht dann einer möglichen Reihenfolge in der die einzelnen Arbeitsschritte abgearbeitet werden können (ohne Abhängigkeiten zu verletzen).

**Definition 41.** Es sei  $M$  eine endliche Menge und  $G = (M, E)$  ein DAG. Eine lineare Ordnung  $\preceq \subseteq M \times M$  ist eine *topologische Sortierung* von  $G$ , wenn für alle  $a, b \in M$

$$aE^*b \Rightarrow a \preceq b$$

gilt.

**Satz 14.** *Jeder endliche DAG besitzt (mindestens) eine topologische Sortierung.*

*Beweis.* Wir bemerken zuerst, dass jeder endliche DAG  $G = (V, E)$  minimale Elemente bezüglich der Relation  $E$  besitzt (wieso?). Weiter bemerken wir, dass jeder DAG, von dem ein minimaler Knoten (zusammen mit den von diesem Knoten ausgehenden Pfeilen) entfernt wird, wieder ein DAG ist (entfernen von Knoten und Verbindungen kann keine neuen Zyklen erzeugen). Aus diesen Beobachtungen folgt, dass folgender Algorithmus eine topologische Sortierung für jeden endlichen DAG generiert:

- a) Wenn  $G = (V, E)$  nicht leer ist, dann wähle ein bezüglich  $E$  minimales Element  $x \in V$  (Wenn  $V$  leer ist, terminiere).
- b) Wiederhole die erste Instruktion mit  $G' = (V \setminus \{x\}, \{(a, b) \in E \mid a \neq x\})$  (d.h. erstelle den DAG  $G'$  durch Entfernen von  $x$  aus  $V$  und entfernen von allen von  $x$  ausgehenden Kanten in  $E$ ).

Die Reihenfolge, mit der die Elemente entfernt werden, entspricht einer topologischen Sortierung.  $\square$

**Satz 15.** *Folgende Aussagen sind äquivalent:*

- a)  $(V, E \setminus \Delta_V)$  ist ein DAG.
- b)  $E^*$  ist eine Halbordnung auf  $V$ .

*Beweis.*  $a) \Rightarrow b)$ : Es sei  $(V, E)$  ein DAG. Weil  $E^*$  nach Definition bereits reflexiv und transitiv ist, müssen wir bloss noch zeigen, dass  $E^*$  antisymmetrisch ist. Gilt  $xE^*y$ ,  $yE^*x$  und  $x \neq y$ , dann gibt es Pfade  $x, a_1, \dots, a_n, y$  und  $y, b_1, \dots, b_m, x$  in  $(V, E \setminus \Delta_V)$



(eventuell ist das Entfernen von Wiederholungen nötig, vgl. Wandtafel) und daher auch einen Zyklus  $x, a_1, \dots, a_n, y, b_1, \dots, b_m$ . Die Behauptung folgt per Kontraposition.

$b) \Rightarrow a)$ : Wenn  $E^*$  eine Halbordnung ist, dann existieren aufgrund der Antisymmetrie keine Zyklen mit mehr als einem Knoten in  $(V, E)$ , daher existieren in  $(V, E \setminus \Delta_V)$  gar keine Zyklen (vgl. Bild Wandtafel).  $\square$

**Folgerung.** Jede endliche Halbordnung kann zu einer linearen Ordnung erweitert werden. Formal, zu jeder Halbordnung  $\preceq$  auf einer Menge  $M$  gibt es eine lineare Ordnung  $\ll$  auf  $M$ , so dass

$$a \preceq b \Rightarrow a \ll b$$

gilt.

**Beweis.** Wir haben bereits gesehen, dass der Graph  $G = (M, \preceq \setminus \Delta_M)$  ein DAG ist. Jede topologische Sortierung von  $G$  erfüllt die Behauptung.  $\square$

**Bemerkung 42.** Sind zwei Mengen  $A$  und  $B$  sowie zwei Halbordnungen  $<_A$  auf  $A$  und  $<_B$  auf  $B$  gegeben, dann nennt man die Relation

$$(x, y) \prec (u, v) :\Leftrightarrow x <_A u \vee (x = u \wedge y <_B v)$$

die *lexikographische Ordnung* auf  $A \times B$ . Sind  $<_A$  und  $<_B$  totale Ordnungen, dann ist auch die lexikographische Ordnung  $\prec$  eine totale Ordnung auf  $A \times B$ .

**Bemerkung 43.** Wohlordnungen spielen eine wichtige Rolle im Zusammenhang mit rekursiven Strukturen. Die Tatsache, dass eine Wohlordnung keine unendlichen absteigenden Ketten zulässt, stellt sicher, dass Rekursionen entlang dieser Ordnung immer “terminieren”. Wir werden uns im nächsten Kapitel genauer mit dieser Beziehung auseinandersetzen. Der nächste Satz gibt aber einen ersten Hinweis auf diesen Zusammenhang.

**Satz 16.** Ist  $\preceq$  eine Wohlordnung auf einer Menge  $M$ , dann gibt es keine unendlich absteigende Folge

$$a_0 \succeq a_1 \succeq \dots \succeq a_n \succeq a_{n+1} \succeq \dots$$

von verschiedenen Elementen aus  $M$ .

**Beweis.** Gibt es eine absteigende Folge  $a_0, a_1, \dots$  wie in der Behauptung, dann ist die Menge

$$\{a_i \mid i \in \mathbb{N}\}$$

eine Teilmenge von  $M$ , die kein  $\preceq$ -minimales Element besitzt. Die Relation  $\preceq$  kann also in diesem Fall keine Wohlordnung sein. Die Behauptung folgt durch Kontraposition.  $\square$

**Beispiel 45.** Die im Folgenden definierte Präordnung spielt eine wichtige Rolle in der sogenannten  $\mathcal{O}$ -Notation zur Beschreibung des Laufzeitverhaltens von Programmen. Die Relation  $\leq^*$  ist auf der Menge  $\{f \mid f : \mathbb{N} \rightarrow \mathbb{N}\}$  wie folgt gegeben:

$$f \leq^* g :\Leftrightarrow K(g, f) \text{ ist endlich}$$

wobei

$$K(g, f) = \{x \in \mathbb{N} \mid g(x) < f(x)\}.$$

Die Relation  $f \leq^* g$  besagt informell, dass die Funktion  $f$  nicht schneller als die Funktion  $g$  wächst. Die Relation  $\leq^*$  ist eine Präordnung aber keine Halbordnung und auch nicht total. Es gibt darüber hinaus unendlich absteigende Folgen von Funktionen bezüglich der Relation  $\leq^*$ .

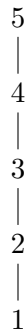
**Übung 30.** Geben Sie zwei  $\leq^*$  unvergleichbare Funktionen  $f$  und  $g$  an.

**Lösung.**

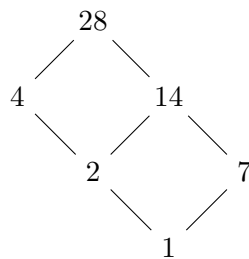
**Definition 42.** Es sei  $\preceq$  eine Halbordnung auf einer Menge  $M$ . Das *Hasse-Diagramm* von  $R$  ist eine vereinfachte Darstellung des Graphen  $(M, \preceq)$ .

- Die Richtung eines Pfeiles  $a \rightarrow b$  für Elemente  $a, b \in M$  wird dadurch zum Ausdruck gebracht, dass sich der Knoten  $b$  oberhalb von  $a$  befindet.
- Pfeile zwischen zwei Punkten  $a, b$  werden gelöscht, wenn es einen weiteren Punkt  $c$  mit  $a \preceq c \preceq b$  gibt.
- Pfeile, die von einem Punkt auf denselben Punkt zeigen (Schleifen), werden weggelassen.

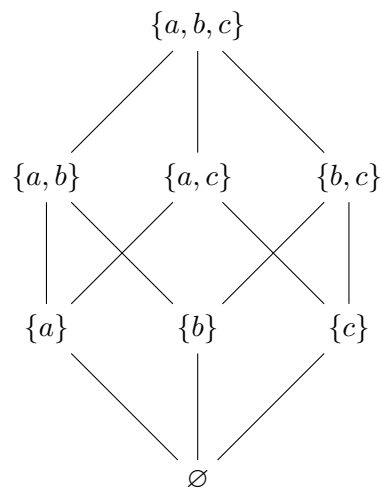
**Beispiel 46.** Eine Darstellung als Hasse-Diagramm von der Relation  $\leq$  auf der Menge  $\{1, \dots, 5\}$ .



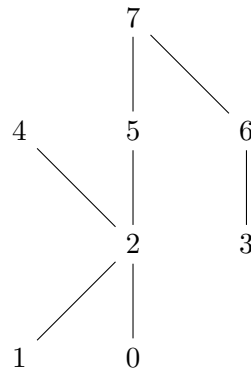
**Beispiel 47.** Eine Darstellung der Teilbarkeitsrelation auf der Menge Teilmengen von 28 ( $\{1, 2, 4, 7, 14, 28\}$ ).



**Beispiel 48.** Die Teilmengenrelation  $\subseteq$  auf der Menge  $\mathcal{P}(\{a, b, c\})$ , als Hasse-Diagramm dargestellt.



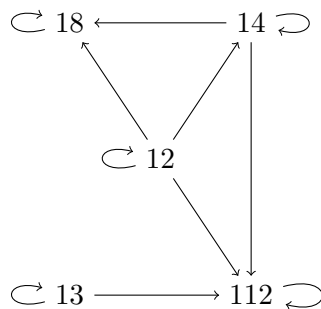
**Übung 31.** Das Hasse-Diagramm einer Halbordnung auf der Menge  $\{0, \dots, 7\}$  ist wie folgt gegeben.



- a) Geben Sie alle maximalen und alle minimalen Elemente von der Menge  $\{0, \dots, 7\}$  an.
- b) Geben Sie drei paarweise unvergleichbare Elemente an.

**Lösung.**

**Übung 32.** Der Graph  $G = (\{12, 13, 14, 18, 112\}, \preceq)$  ist wie folgt gegeben.



- a) Zeichnen Sie ein Hasse-Diagramm für die Halbordnung  $\preceq$ .
- b) Geben Sie die Relation als Menge an.

**Lösung.**

# 4 Rekursive Strukturen und die natürlichen Zahlen

## Relevanz für die Informatik

- Rekursion ist ein wichtiges Sprachelement von höheren Programmiersprachen (absolut zentral für funktionale Sprachen).
- Induktion kann verwendet werden, um die Korrektheit von rekursiven Programmen zu beweisen.
- Rekursion und Induktion sind von fundamentaler Bedeutung für die theoretische Informatik (rekursive Funktionen, verallgemeinerter Rekursionsbegriff)
- Informatik ist voll von “induktiven Definitionen” (Syntax und Semantik von Programmiersprachen, primitiv rekursive Funktionen uvm.).

## Lernziele

Sie kennen die

- Peano-Axiome und verstehen deren Bedeutung.
- Die Begriffe von Induktion und Rekursion

Sie verstehen

- wie Induktion und Rekursion zusammenhängen.
- wie man rekursiv eine Funktion definieren kann und wie diese Definitionsweise zu rechtfertigen ist.
- wie sich die arithmetischen Operationen rekursiv aus der Nachfolgerabbildung definieren lassen.
- wie die üblichen Rechenregeln für natürliche Zahlen aus den Peano-Axiomen folgen.

Sie sind in der Lage

- Induktionsbeweise zu führen.
- Algorithmen und Problemlösungsstrategien durch Rekursion zu beschreiben.
- Probleme zu erkennen, die sich effektiv durch Rekursion lösen lassen.

## Literatur und Links

- Aufgaben mit Lösungen zu Induktion:  
<http://www.emath.de/Referate/induktion-aufgaben-loesungen.pdf>
- Erklärungen zu Induktion:  
Appendix B von <https://slc.openlogicproject.org/slc-screen.pdf>
- Wikipedia Einträge zu Induktion und Rekursion:  
[http://de.wikipedia.org/wiki/Vollst%C3%A4ndige\\_Induktion](http://de.wikipedia.org/wiki/Vollst%C3%A4ndige_Induktion)  
<http://de.wikipedia.org/wiki/Rekursion>

## 4.1 Die grundlegende Struktur der natürlichen Zahlen

Wir haben die Menge  $\mathbb{N}$  bereits kennen und als Grundlage für viele Beispiele auch schätzen gelernt. In diesem Kapitel möchten wir diese Menge etwas genauer verstehen, wir wollen ihre innere Struktur (Ordnung und Operationen) untersuchen. Ausgangspunkt für unsere Betrachtungen ist die Anschauung der natürlichen Zahlen als eine auf dem “Zahlenstrahl” angeordnete, diskrete Menge:

$$0 \xrightarrow{+1} 1 \xrightarrow{+1} 2 \xrightarrow{+1} 3 \xrightarrow{+1} \dots$$

Von dieser Anschauung geleitet, listen wir nun einige Grundtatsachen über die Struktur  $\mathbb{N}$  auf. Diese Grundannahmen entsprechen den sogenannten *Peano-Axiomen*.

- Die Zahl 0 ist eine natürliche Zahl. Jede natürliche Zahl  $k$  hat genau einen Nachfolger  $k + 1$ . Der Nachfolger jeder natürlichen Zahl ist wiederum eine natürliche Zahl.
- Die Zahl 0 ist die einzige natürliche Zahl, die kein Nachfolger ist:

$$\forall n \in \mathbb{N} \underbrace{(\forall k \in \mathbb{N} (n \neq k + 1))}_{n \text{ ist kein Nachfolger}} \Leftrightarrow n = 0.$$

- Jede natürliche Zahl ist Nachfolger von höchstens einer natürlichen Zahl:

$$\forall n, m \in \mathbb{N} (n + 1 = m + 1 \Rightarrow n = m).$$

- *Das Prinzip der (vollständigen) Induktion:* Es sei  $A(n)$  eine Eigenschaft (ein Prädikat) von natürlichen Zahlen. Aus den beiden Voraussetzungen

**Induktionsverankerung (I.V.):**  $A(0)$

**Induktionsschritt (I.S.):**  $\forall n \in \mathbb{N} (A(n) \Rightarrow A(n + 1))$ ,

folgt die Gültigkeit von  $\forall n \in \mathbb{N} (A(n))$ .

**Bemerkung 44.** Der Induktionsschritt ist stets von der Form

$$\forall n \in \mathbb{N} \left( \underbrace{A(n)}_{\text{Induktionsannahme}} \Rightarrow A(n+1) \right)$$

für ein Prädikat  $A$ . Der Teil  $A(n)$  wird dabei *Induktionsannahme* genannt, weil er beim Nachweis von  $A(n+1)$  als Annahme verwendet werden darf.

**Bemerkung 45.** Das Prinzip der vollständigen Induktion ist ein mächtiges Mittel um viele verschiedene Behauptungen über natürliche Zahlen beweisen zu können. Will man eine Aussage von der Form

$$\text{Jede natürliche Zahl } n \text{ erfüllt } E(n)$$

für ein Prädikat  $E$  beweisen, dann muss man, wenn man die Eigenschaft  $E$  nicht für alle natürlichen Zahlen *simultan* beweisen kann, im Prinzip unendlich viele Schritte bewältigen:

1. Schritt: Zeige  $E(0)$ .
2. Schritt: Zeige  $E(1)$ .
3. Schritt: Zeige  $E(2)$ .
- ⋮

Die Stärke des Induktionsargumentes liegt nun darin, all diese unendlich vielen Schritte auf zwei Schritte zu reduzieren:

1. Schritt (I.V.): Zeige  $E(0)$ .
2. Schritt (I.S.): Zeige, dass die Eigenschaft  $E$  unter Nachfolgern erhalten bleibt. Intuitiv könnte man sagen, dass die Eigenschaft  $E$  von jeder natürlichen Zahl auf die nächste “vererbt” wird.

**Beispiel 49.** Wir betrachten die Eigenschaft  $A(n)$ , die besagt, dass die Summe aller natürlichen Zahlen bis  $n$  halb so gross wie die Zahl  $n(n+1)$  ist:

$$0 + 1 + \dots + n = \frac{n(n+1)}{2}.$$

Wir beweisen nun per Induktion nach  $n$ , dass die Eigenschaft  $A(n)$  für jede natürliche Zahl  $n$  zutrifft.

*Beweis.* Wir zeigen zuerst die Induktionsverankerung:

- **Verankerung** ( $n = 0$ ):  $A(0)$  gilt, weil

$$0 = \frac{0 \cdot 1}{2}$$

offensichtlich korrekt ist.



- **Schritt** ( $n \rightarrow n + 1$ ): Für den Induktionsschritt müssen wir zeigen, dass für jede natürliche Zahl  $n$  mit der Eigenschaft  $A(n)$  auch  $A(n + 1)$  gilt. Wir nehmen dazu an, dass  $n$  eine beliebige solche natürliche Zahl sei und betrachten

$$\begin{aligned} 0 + 1 + \cdots + n + (n + 1) &= (0 + 1 + \cdots + n) + (n + 1) \\ &\stackrel{A(n)}{=} \frac{n(n + 1)}{2} + (n + 1) \\ &= \frac{n(n + 1) + 2(n + 1)}{2} \\ &= \frac{(n + 1)(n + 2)}{2}. \end{aligned}$$

Daraus folgt der Induktionsschritt.

□

**Beispiel 50.** Wir benützen ein Induktionsargument um zu beweisen, dass alle natürlichen Zahlen  $n > 1$  für beliebige reelle Zahlen  $r > -1, r \neq 0$  die folgende Eigenschaft haben:

$$(1 + r)^n > 1 + nr.$$

*Beweis.*

- **Verankerung** ( $n = 2$ ): Die Verankerung gilt, wegen

$$(1 + r)^2 = 1 + 2r + r^2 > 1 + 2r.$$

- **Schritt** ( $n \rightarrow n + 1$ ): Wir nehmen nun an, dass die Aussage für  $n$  gilt (I.A.) und zeigen sie für  $n + 1$ :

$$\begin{aligned} (1 + r)^{n+1} &= (1 + r)^n(1 + r) \\ &\stackrel{I.A.}{>} (1 + nr)(1 + r) \\ &= 1 + nr + r + \underbrace{nr^2}_{\text{positiv}} \\ &> 1 + (n + 1)r. \end{aligned}$$

□

**Beispiel 51.** Für jede endliche Menge  $X$  gilt

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

*Beweis.* Wir führen den Beweis durch Induktion nach der Anzahl Elemente der Menge  $X$ .

- **Verankerung** ( $|X| = 0$ ): Die einzige Menge mit 0 Elementen ist die leere Menge, es gilt also wie gewünscht

$$|\mathcal{P}(X)| = |\mathcal{P}(\emptyset)| = |\{\emptyset\}| = 1 = 2^0 = 2^{|X|}.$$

- **Schritt:** Es sei nun  $X$  eine  $n + 1$  elementige Menge. Aufgrund der Induktionsannahme können wir davon ausgehen, dass für alle Mengen  $Y$  mit  $n$  Elementen die Gleichung

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

erfüllt ist. Da  $X \neq \emptyset$  gilt, können wir ein  $x \in X$  auswählen. Wir unterteilen die Potenzmenge von  $X$  in zwei disjunkte, gleich grosse Teile  $A$  und  $B$ :

$$\begin{aligned} A &= \{Y \subseteq X \mid x \notin Y\} \\ B &= \{Y \subseteq X \mid x \in Y\}. \end{aligned}$$

Es gilt:

$$\begin{aligned} |\mathcal{P}(X)| &= |A \cup B| = |A| + |B| \\ &= |A| + |A| = 2|A| = 2|\mathcal{P}(X \setminus \{x\})| \\ &\stackrel{I.A.}{=} 2 \cdot 2^n = 2^{n+1}. \end{aligned} \quad \square$$

**Satz 17** (Vollständige Induktion mit Mengen). *Für jede Menge  $X$  von natürlichen Zahlen gilt: Wenn  $X$  die Bedingungen*

- *Induktionsverankerung:*  $0 \in X$
- *Induktionsschritt:*  $\forall n (n \in X \Rightarrow n + 1 \in X)$

*erfüllt, dann ist bereits  $X = \mathbb{N}$ .*

**Beweis.** Ist  $E(n)$  das Prädikat  $n \in X$ , dann folgt mit vollständiger Induktion sofort  $\forall n (E(n))$  und somit  $\mathbb{N} = X$ .  $\square$

**Definition 43.** Die Ordnung  $\leq$  auf den natürlichen Zahlen ist durch

$$x \leq y :\Leftrightarrow \exists k \in \mathbb{N} (x + k = y)$$

gegeben. Wir schreiben weiter

$$x < y :\Leftrightarrow x \leq y \wedge x \neq y.$$

**Bemerkung 46.** Wird die Zahlengerade der natürlichen Zahlen vertikal aufgezeichnet, dann ist sie ein Hasse-Diagramm für die Ordnung  $\leq$  auf  $\mathbb{N}$ .

$$\begin{array}{c} \vdots \\ | \\ 2 \\ | \\ 1 \\ | \\ 0 \end{array}$$

**Satz 18.** *Jede nichtleere Menge von natürlichen Zahlen hat ein minimales Element.*

*Beweis.* Wir zeigen, dass jede Menge von natürlichen Zahlen, die kein minimales Element enthält, leer ist. Dazu wählen wir eine beliebige Menge  $X \subseteq \mathbb{N}$  ohne minimales Element. Um zu zeigen, dass die Menge  $X$  leer ist, genügt es zu zeigen, dass die Menge

$$Y = \{n \in \mathbb{N} \mid \forall x \in X (n < x)\}$$

aller natürlichen Zahlen, die “unterhalb” von  $X$  liegen, bereits alle natürlichen Zahlen enthält. Wir zeigen  $Y = \mathbb{N}$  mithilfe von Satz 17.

- **Verankerung:** Es gilt  $0 \in Y$ , weil sonst 0 das minimale Element von  $X$  wäre, was unserer Wahl von  $X$  widerspricht.
- **Induktionsschritt:** Ist  $n \in Y$ , dann gilt für alle Elemente  $x$  von  $X$  die Ungleichung  $n < x$ . Es gilt daher  $n + 1 \leq x$  für alle Elemente  $x$  von  $X$ . Da  $n + 1$  kein minimales Element von  $X$  sein kann, gilt daher  $n + 1 \in Y$ .

Aus Satz 17 folgt nun, dass  $Y = \mathbb{N}$  und somit wie gewünscht  $X = \emptyset$  ist. □

**Satz 19.** *Es gibt keine unendlich absteigende Folge*

$$a_0 > a_1 > \cdots > a_n > a_{n+1} > \cdots$$

*von natürlichen Zahlen.*

*Beweis.* Gäbe es eine absteigende Folge

$$a_0 > a_1 > \cdots > a_n > a_{n+1} > \cdots,$$

dann hätte die Menge

$$\{a_0, a_1, \dots, a_n, a_{n+1}, \dots\}$$

kein minimales Element. Dies widerspricht Satz 18. □

Aus den eben bewiesenen Sätzen können wir neue Beweismethoden herleiten:

**Bemerkung 47** (Der kleinste Verbrecher). Die Beweismethode des “kleinsten Verbrechers” geht wie folgt: Will man zeigen, dass alle natürlichen Zahlen eine Eigenschaft  $E$  haben, dann geht man davon aus, dass wenn dies nicht der Fall wäre, es eine kleinste natürliche Zahl  $n_0$  (den kleinsten Verbrecher) gäbe, die *nicht* die Eigenschaft  $E$  hat. Führt man diese Annahme zu einem Widerspruch, so hat man die ursprüngliche Behauptung bewiesen. Obwohl die Methode des “kleinsten Verbrechers” also nichts anderes als die Kombination eines Widerspruchsargumentes mit Satz 18 ist, handelt es sich doch um eine sehr “anwenderfreundliche” und einprägsame Beschreibung dieser Argumentationsfolge.

**Beispiel 52.** Wir benützen die Methode des “kleinsten Verbrechers” um zu beweisen, dass jede natürliche Zahl, die mindestens zwei Teiler hat, mindestens einen Primfaktor besitzt (von einer Primzahl geteilt wird).

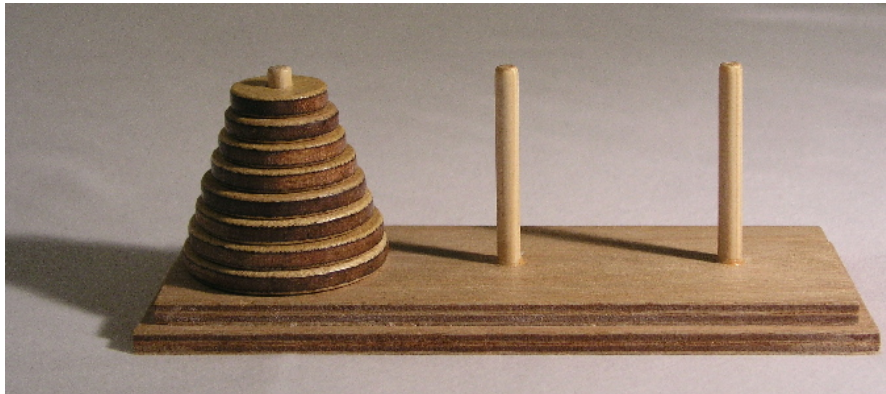
*Beweis.* Es sei  $n_0$  die kleinste natürliche Zahl mit mindestens zwei Teilern, die keine Primfaktoren besitzt (der “kleinste Verbrecher”). Da  $n_0$  keine Primfaktoren hat, ist  $n_0$  selbst auch keine Primzahl und es gilt  $n_0 \neq 0$ . Es folgt somit, dass ein Teiler  $1 < x < n_0$  von  $n_0$  existieren muss. Da  $1 < x$  gilt, hat  $x$  mindestens zwei Teiler (1 und  $x$ ) und somit, wegen  $x < n_0$ , einen Primfaktor  $p$ . Da die Teilbarkeitsrelation transitiv ist, muss  $p$  aber auch ein Primfaktor von  $n_0$  sein. Dies ist der gesuchte Widerspruch.  $\square$

**Übung 33.** Beweisen Sie mit der Methode des “kleinsten Verbrechers”. Jede natürliche Zahl von der Form  $(n^2 + n)$  ist gerade.

**Lösung.**

## 4.2 Vom Induktionsbeweis zum rekursiven Algorithmus

**Beispiel 53** (Türme von Hanoi).



“Die Türme von Hanoi”<sup>1</sup> ist ein Geduldspiel. Das Spiel besteht aus drei gleich grossen Stäben A, B und C, auf die mehrere gelochte Scheiben gelegt werden, alle verschieden gross. Zu Beginn liegen alle Scheiben auf Stab A, der Grösse nach geordnet, mit der grössten Scheibe unten und der kleinsten oben. Ziel des Spiels ist es, den kompletten Scheiben-Stapel von A nach C zu versetzen. Bei jedem Zug darf die oberste Scheibe eines beliebigen Stabes auf einen der beiden anderen Stäbe gelegt werden, vorausgesetzt, dort liegt nicht schon eine kleinere Scheibe. Folglich sind zu jedem Zeitpunkt des Spieles die Scheiben auf jedem Feld der Grösse nach geordnet.

Wir wollen beweisen, dass “die Türme von Hanoi” mit beliebig vielen Scheiben erfolgreich gespielt werden können.

*Beweis.* Wir benutzen ein Induktionsargument ( $n$  sei die Anzahl Scheiben):

- **Verankerung**  $n = 0$ : Dieser Fall ist trivial, da es keine Scheiben zu bewegen gibt.
- **Induktionsschritt**  $n \rightarrow n + 1$ : Wir betrachten das Spiel mit  $n + 1$  Scheiben. Nach Induktionsvoraussetzung gibt es eine Lösungsstrategie für das Spiel mit nur  $n$  Scheiben. Diese Strategie können wir offensichtlich dazu verwenden, um alle bis auf die grösste Scheibe auf den Stab B zu verschieben. Nun können wir die grösste Scheibe auf den Stab C verschieben, um anschliessend nochmal die Strategie für das Spiel mit  $n$  Scheiben anzuwenden und alle kleineren Scheiben auf den Stab C zu bewegen. Das Spiel ist somit auch für  $n + 1$  Scheiben lösbar.  $\square$

**Bemerkung 48.** Der Beweis, dass die Türme von Hanoi für beliebige  $n$  gelöst werden können, ist mehr als nur eine Argumentationskette, die dazu geeignet ist jemanden davon zu überzeugen, dass es tatsächlich *irgendwie möglich sein muss* das Spiel zu gewinnen.

---

<sup>1</sup>Beschreibung und Bild von Wikipedia.

Es steckt viel mehr in diesem Beweis; der Beweis gibt einen konkreten Algorithmus (rekursiv) vor, wie das Spiel erfolgreich gespielt werden kann. Wir betrachten eine Implementierung dieser Lösungsstrategie in Java.

```
// x-viele Scheiben von A nach B verschieben:
// Falls x=0, dann ist nichts zu tun.
// Sonst, zuerst die oberen (x-1) Scheiben von A nach C
// verschieben,
// dann die groesste Scheibe von A nach B verschieben
// und schliesslich alle anderen Scheiben von C nach B
// verschieben
public class HanoiSolver{

    public String solve(int size){
        return AC(size);
    }

    private String AB(int x){
        if (x==0) return "";
        return AC(x-1)+"_AB_"+CB(x-1);
    }

    private String AC(int x){
        if (x==0) return "";
        return AB(x-1)+"_AC_"+BC(x-1);
    }

    private String BC(int x){
        if (x==0) return "";
        return BA(x-1)+"_BC_"+AC(x-1);
    }

    private String BA(int x){
        if (x==0) return "";
        return BC(x-1)+"_BA_"+CA(x-1);
    }

    private String CB(int x){
        if (x==0) return "";
        return CA(x-1)+"_CB_"+AB(x-1);
    }
}
```

```
private String CA(int x){
    if (x==0) return "";
    return CB(x-1)+"_CA_"+BA(x-1);
}
```

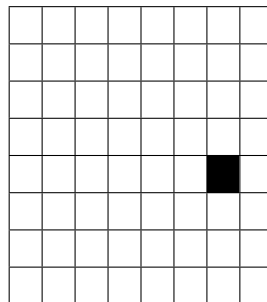
und die kurze Fassung:


```
public class HanoiSolverCompact{

    public String solve(int size){
        return hanoi("A","C","B",size);
    }

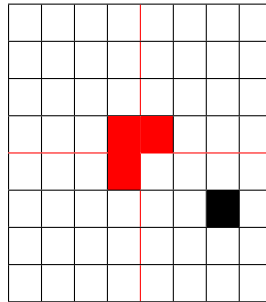
    private String hanoi(String x,String y,String z,int n){
        if(n==0) return "";
        return hanoi(x,z,y,n-1)+"_"+x+y+hanoi(z,y,x,n-1);
    }
}
```

**Beispiel 54.** Ist es immer möglich ein “gelochtes  $n \times n$ -Quadrat”



mit Flächen von der Form  “passgenau” zu überdecken? Ja, wenn  $n$  eine Zweierpotenz ist. Wir können diese Behauptung durch Induktion wie folgt beweisen: Wir nehmen an, dass das “gelochte Quadrat” eine Seitenlänge von  $2^n$  hat.

- Verankerung ( $n = 0$ ): Wenn  $n = 0$ , dann besteht das gelochte Quadrat nur aus einem Loch. Wir können das Quadrat (ohne etwas zu tun) überdecken.
- Hat das Quadrat die Seitenlänge  $2^{n+1}$ , dann zerlegen wir es in vier gleich grosse Quadranten, die alle die Seitenlänge  $2^n$  haben. Wir platzieren eine der Flächen wie unten angedeutet (rot).



Nun sind alle Quadranten ein “gelochtes Quadrat” der Seitenlänge  $2^n$ . Wir können also nach Induktionsvoraussetzung alle Quadranten passgenau belegen.

**Übung 34.** Implementieren Sie (ausgehend vom Beispiel 54) in einer Programmiersprache Ihrer Wahl, einen Algorithmus zur Überdeckung von “gelochten Quadraten”, die eine Zweierpotenz als Seitenlänge haben.

## 4.3 Rekursive Definitionen

Rekursive Definitionen bezeichnen die mathematisch einwandfreie Art, ein Objekt durch Bezugnahme (Selbstreferenz) auf das zu definierende Objekt selbst zu definieren.

**Beispiel 55.** Ein Palindrom ist ein Wort, das rückwärts und vorwärts gelesen gleich lautet. Beispiele von Palindromen sind *xyx*, *acaca*, *arbbra*, *b*, *a*,  $\dots$ . Obwohl es uns anschaulich klar ist, welche Wörter Palindrome sind und welche nicht, ist unsere Beschreibung keine mathematisch präzise Definition. Dies wird insbesondere dann offensichtlich, wenn wir ein Programm schreiben müssen (ohne “String-umkehrende” Operatoren benützen zu dürfen), das von einem gegebenen Wort (String) entscheidet ob dieses ein Palindrom ist oder nicht. Wie können wir also Palindrome definieren (eindeutig beschreiben), ohne auf unsere Vorstellung von rückwärts und vorwärts lesen angewiesen zu sein? Durch Rekursion:

Ein Wort  $w$  ist ein Palindrom, wenn mindestens eine der beiden folgenden Bedingungen erfüllt ist:

- Das Wort  $w$  besteht aus einem oder gar keinem Buchstaben (Länge von  $w < 2$ ).
- Es gibt einen Buchstaben (Zeichen, Char)  $x$  und ein Palindrom  $u$  so, dass  $w = xux$  gilt.

*Selbstreferenz*

Obwohl diese Definition, durch die in ihr vorhandenen Selbstreferenz, ein wenig “obskur” erscheinen mag, können wir sie direkt in ein Computerprogramm übersetzen.

In Java:



```
boolean palindrome(String w){
    if (w.length() < 2) return true;
    int last = w.length() - 1;
    char a = w.charAt(0);
    char b = w.charAt(last);
    if (a == b) return palindrome(w.substring(1, last - 1));
    return false;
}
```

**Theorem 3** (Rekursive Definitionen). *Ist  $M$  eine Menge und  $G : M \times \mathbb{N} \rightarrow M$  sowie  $c \in M$ , dann gibt es eine eindeutig bestimmte Funktion  $F : \mathbb{N} \rightarrow M$ , welche die Gleichungen (Rekursionsgleichungen)*

$$\begin{aligned} F(0) &= c \\ F(k+1) &= G(\underbrace{F(k)}_{\text{Selbstbezug}}, k) \end{aligned}$$

erfüllt.

*Beweisidee.* Die Behauptung besteht aus einer Eindeutigkeitsaussage und einer Existenzaussage:

- Die Funktion  $F : \mathbb{N} \rightarrow M$  ist durch die Rekursionsgleichungen eindeutig bestimmt. Das heisst, dass es keine andere Funktion gibt, die den Rekursionsgleichungen von  $F$  genügt.
- Es gibt überhaupt eine Funktion, die den Rekursionsgleichungen genügt.

Wir beweisen zuerst die Eindeutigkeitsbedingung. Wir nehmen an, dass  $F$  und  $H$  zwei Funktionen sind, die beide die oben genannten Rekursionsgleichungen erfüllen und zeigen, dass daraus  $F = H$  folgt. Es genügt mit Induktion zu zeigen, dass für jede natürliche Zahl  $n \in \mathbb{N}$  die Gleichung  $F(n) = H(n)$  gilt (weil dann  $H = F$  gilt).

- Verankerung ( $n = 0$ ): Aufgrund von

$$F(0) = c = H(0)$$

ist die Induktionsverankerung erfüllt.

- Schritt ( $n \rightarrow n+1$ ): Wir nehmen an, dass  $F(n) = H(n)$  gilt und müssen  $F(n+1) = H(n+1)$  beweisen. Dies folgt sofort aus

$$F(n+1) = G(F(n), n) \stackrel{IA}{=} G(H(n), n) = H(n+1).$$

### 4.3. REKURSIVE DEFINITIONEN

---

Nun kommen wir zur Existenzaussage. Anstelle eines formalen Beweises, wollen wir uns an dieser Stelle bloss anschaulich davon überzeugen, dass eine Funktion  $F$  immer existiert. Wir geben einen iterativen Algorithmus (in Pseudocode) an, der die gesuchte Funktion realisiert.

```
input(n)
lst=[c] // Eine Liste mit einzigem Eintrag c
for i = 0..(n-1) do
    x = G(lst[i], i)
    lst.add(x) // Den aktuellen Funktionswert zur Liste
                // (aller Funktionswerte) hinzufuegen.
return lst[n]
```

□

**Beispiel 56.** Die üblichen arithmetischen Grundoperationen können alle relativ kompakt als rekursive Definitionen geschrieben werden:

- Die Addition von natürlichen Zahlen:

$$\begin{aligned}x + 0 &= x \\ x + (n + 1) &= (x + n) + 1\end{aligned}$$

- Die Multiplikation von natürlichen Zahlen:

$$\begin{aligned}x \cdot 0 &= 0 \\ x \cdot (n + 1) &= (x \cdot n) + x\end{aligned}$$

- Die Exponentiation von natürlichen Zahlen:

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

- Die Fakultätsfunktion:

$$\begin{aligned}0! &= 1 \\ (n + 1)! &= n! \cdot (n + 1)\end{aligned}$$

- Endliche Summen:

$$\begin{aligned}\sum_{i=1}^0 a_i &= 0 \\ \sum_{i=1}^{n+1} a_i &= \left(\sum_{i=0}^n a_i\right) + a_{n+1}\end{aligned}$$

- Endliche Produkte:

$$\prod_{i=1}^0 a_i = 1$$
$$\prod_{i=1}^{n+1} a_i = \left( \prod_{i=1}^n a_i \right) \cdot a_{n+1}$$

Die üblichen Rechenregeln für natürliche Zahlen lassen sich aufgrund dieser rekursiven Definitionen mit Induktion (und genügend Geduld) beweisen. Wir beschränken uns beispielhaft auf den Beweis von Satz 22.

**Übung 35.** Implementieren Sie alle Funktionen von Beispiel 56 in der Programmiersprache Ihrer Wahl (natürlich ohne Verwendung der vorimplementierten Grundoperationen). Halten Sie sich so präzise wie möglich an die mathematische Definition.

**Lösung.** Elektronisch zu lösen.

**Satz 20.** Für alle natürlichen Zahlen  $n, m, k$  gelten folgende Rechenregeln für deren Addition:

- a) *Neutrales Element:*  $0 + n = n$
- b) *Kommutativität:*  $n + m = m + n$
- c) *Assoziativität:*  $(n + m) + k = n + (m + k)$
- d) *Kürzbarkeit:*  $n + k = m + k \Rightarrow n = m$

**Bemerkung 49.** Wegen der Assoziativität der Addition, können wir Klammern in endlichen Summen von natürlichen Zahlen weglassen.

**Satz 21** (Rechenregeln für die Multiplikation). Für alle  $n, m, k \in \mathbb{N}$  gelten folgende Identitäten<sup>2</sup>:

- a) *Absorption:*  $0 \cdot n = 0$
- b) *Neutrales Element:*  $1 \cdot n = n$
- c) *Kommutativität:*  $n \cdot m = m \cdot n$
- d) *Assoziativität:*  $n \cdot (m \cdot k) = (n \cdot m) \cdot k$
- e) *Distributivität:*  $n \cdot (m + k) = nm + nk$

---

<sup>2</sup>Wir vereinbaren hier, dass die Multiplikation “stärker bindet” als die Addition. Ein Ausdruck von der Form  $nm + k$  wird also als  $(nm) + k$  interpretiert.

**Übung 36.** Nachdem wir die Addition und die Multiplikation rekursiv definiert haben, lassen sich dies in den Sätzen 20 und 21 geäußerten Tatsachen durch Induktion beweisen. Die einzelnen Beweise sind nicht sonderlich spannend aber eine gute Übung.

**Satz 22** (Rechenregeln für Partialsummen). *Sind  $(a_i)_{i \in \mathbb{N}}$  und  $(b_i)_{i \in \mathbb{N}}$  beliebige Folgen und ist  $c \in \mathbb{N}$ , dann gilt für jedes  $n \in \mathbb{N}$ :*

$$\sum_{i=1}^n (ca_i + cb_i) = c \left( \sum_{i=1}^n a_i + \sum_{i=1}^n b_i \right)$$

*Beweis.* Induktion nach  $n$ .

- Verankerung ( $n = 0$ ): Die Verankerung gilt aufgrund von

$$\sum_{i=1}^0 (ca_i + cb_i) = 0 = c(0 + 0) = c \left( \sum_{i=1}^0 a_i + \sum_{i=1}^0 b_i \right).$$

- Schritt ( $n \rightarrow n + 1$ ):

$$\begin{aligned} \sum_{i=1}^{n+1} (ca_i + cb_i) &= \left( \sum_{i=1}^n (ca_i + cb_i) \right) + (ca_{n+1} + cb_{n+1}) \\ &= \left( \sum_{i=1}^n (ca_i + cb_i) \right) + c(a_{n+1} + b_{n+1}) \\ &\stackrel{IA}{=} c \left( \sum_{i=1}^n a_i + \sum_{i=1}^n b_i \right) + c(a_{n+1} + b_{n+1}) \\ &= c \left( \sum_{i=1}^n a_i + \sum_{i=1}^n b_i + a_{n+1} + b_{n+1} \right) \\ &= c \left( \sum_{i=1}^n a_i + a_{n+1} + \sum_{i=1}^n b_i + b_{n+1} \right) \\ &= c \left( \sum_{i=1}^{n+1} a_i + \sum_{i=1}^{n+1} b_i \right) \end{aligned}$$

□

# 5 Elementare Zahlentheorie

## Lernziele

Sie kennen die

- Grundlagen der Teilbarkeitslehre.
- den Begriff der Primzahl.
- das kgV und den ggT und wie diese mithilfe des euklidischen Algorithmus berechnet werden.
- das Lemma von Bézout.
- den chinesischen Restsatz.
- den kleinen Fermatschen Satz.

Sie verstehen

- wieso und wie ganze Zahlen in ihre Primfaktoren zerlegt werden können.
- die modulare Arithmetik.
- den Zusammenhang vom chinesischen Restsatz und der Lösbarkeit von simultanen Kongruenzen.

Sie sind in der Lage

- die Stellenwertsysteme ineinander umzurechnen.
- Systeme simultaner Kongruenzen aufzulösen.

## Literatur und Links

- Euklidischer Algorithmus:  
[http://de.wikipedia.org/wiki/Euklidischer\\_Algorithmus](http://de.wikipedia.org/wiki/Euklidischer_Algorithmus)

Analog zu unserem Vorgehen mit den natürlichen Zahlen wollen wir auch die *ganzen Zahlen* informell einführen. Wir definieren

$$\mathbb{Z} := \{.., -2, -1, 0, 1, 2, ...\}.$$

Die Motivation die Menge  $\mathbb{N}$  zur Menge  $\mathbb{Z}$  erweitern zu wollen fusst auf der Tatsache, dass für feste natürliche Zahlen  $k, k'$  im Allgemeinen die Gleichung

$$k + x = k'$$

keine Lösung in  $\mathbb{N}$  besitzt. Es ist in der Tat so, dass bei der Konstruktion von  $\mathbb{Z}$  aus  $\mathbb{N}$  (was wir nicht tun werden) die Menge  $\mathbb{Z}$  im Prinzip als die Menge aller Lösungen von solchen Gleichungen eingeführt wird.

Wir wollen es als gegeben erachten, dass die Multiplikation und die Addition derart von  $\mathbb{N}$  auf  $\mathbb{Z}$  fortgesetzt werden können, dass folgende Rechenregeln bestehen:

**Bemerkung 50** (Rechenregeln auf  $\mathbb{Z}$ ). Für alle  $r, s, z \in \mathbb{Z}$  gelten folgende Gleichungen.

$-1 \cdot z = -z$	
$-(-z) = z$	
$-z + z = 0$	Inverse Elemente bezüglich +
$0 \cdot z = 0$	Absorbtion
$1 \cdot z = z$	Neutrales Element bezüglich ·
$0 + z = z$	Neutrales Element bezüglich +
$r(sz) = (rs)z$	Assoziativität von ·
$r + (s + z) = (r + s) + z$	Assoziativität von +
$rs = sr$	Kommutativität von ·
$r + s = s + r$	Kommutativität von +
$r(s + z) = rs + sz$	Distributivität
$rx = ry \Rightarrow x = y \vee r = 0$	Kürzbarkeit

**Definition 44.** Wir definieren die *Subtraktion*

$$- : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$$

durch

$$x - y := x + (-y),$$

die *Betragsfunktion*

$$|\cdot| : \mathbb{Z} \rightarrow \mathbb{N}$$

durch

$$|z| = \begin{cases} z & \text{falls } z \in \mathbb{N} \\ -1 \cdot z & \text{sonst} \end{cases}$$

und die Relation  $\leq$  durch

$$x \leq y :\Leftrightarrow \exists n \in \mathbb{N} (x + n = y).$$

## 5.1 Teilbarkeit und Euklidischer Algorithmus

**Definition 45.** Sind  $x, y \in \mathbb{Z}$  ganze Zahlen, so sagen wir, dass  $x$  ein Teiler von  $y$  ist, falls es ein  $k \in \mathbb{Z}$  gibt mit  $xk = y$ . Wir schreiben in diesem Fall  $x|y$ . Es gilt also

$$x|y \Leftrightarrow \exists k \in \mathbb{Z} (y = xk).$$

Mit  $T(y)$  bezeichnen wir die Menge aller natürlichen Zahlen, welche Teiler von  $y$  sind, also  $T(y) = \{x \in \mathbb{N} \mid x|y\}$ .

### Beispiel 57.

- a) Die Zahl 1 ist ein Teiler jeder ganzen Zahl  $z$ , da  $1 \cdot z = z$ .
- b)  $T(0) = \mathbb{N}$ .

**Bemerkung 51.** Die Teilbarkeitsrelation ist reflexiv und transitiv auf der Menge  $\mathbb{Z}$ , auf der Menge  $\mathbb{N}$  ist die Teilbarkeitsrelation sogar eine Halbordnung (wieso nicht auf der Menge  $\mathbb{Z}^?$ ).

**Beweis.** Wir zeigen, dass die Teilbarkeitsrelation reflexiv, transitiv und für natürliche Zahlen auch antisymmetrisch ist.

- Reflexivität: Dies gilt, da jede ganze Zahl sich selbst teilt.
- Transitivität: Seien  $x, y, z$  ganze Zahlen. Aus  $x|y$  und  $y|z$  folgt, dass es ganze Zahlen  $k_1, k_2$  gibt mit  $x \cdot k_1 = y$  und  $y \cdot k_2 = z$ . Es folgt

$$x \cdot (k_1 \cdot k_2) = (x \cdot k_1) \cdot k_2 = y \cdot k_2 = z.$$

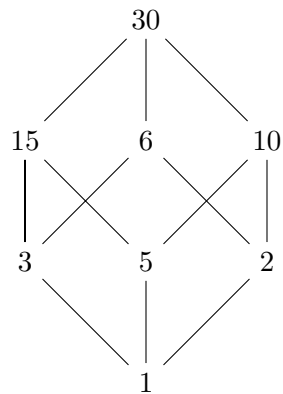
Somit existiert eine ganze Zahl  $k$  (nämlich  $k = k_1 \cdot k_2$ ) mit  $k \cdot x = z$ , also gilt  $x|z$  wie gewünscht.  $\square$

- Antisymmetrie auf  $\mathbb{N}$ : Wir müssen zeigen, dass für natürliche Zahlen  $x$  und  $y$  aus  $x|y$  und  $y|x$  folgt, dass  $x = y$  gilt. Es gelte also  $xk = y$  und  $x = yr$  für ganze Zahlen  $k, r$ . Es folgt

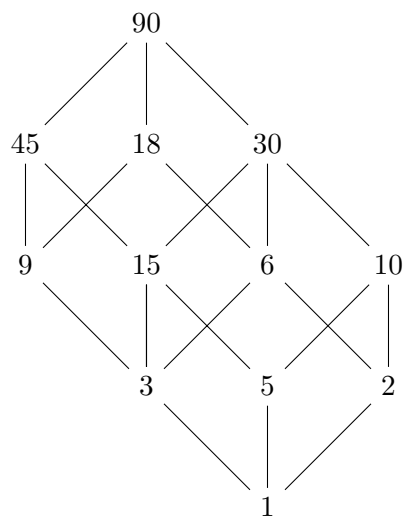
$$x = yr = (xk)r = x(kr)$$

und  $kr = 1$ . Daraus ergeben sich zwei mögliche Fälle;  $k = r = 1$  oder  $k = r = -1$ . Im Fall  $k = r = -1$  folgt  $x = -y$ , was im Widerspruch dazu steht, dass  $x$  und  $y$  natürliche Zahlen sind. Es bleibt also nur der Fall  $k = r = 1$  und somit, wie gewünscht,  $x = y$ .

**Beispiel 58.** Das Hasse-Diagramm der Teilbarkeitsrelation auf der Menge  $T(30)$ :



Das Hasse-Diagramm der Teilbarkeitsrelation auf der Menge  $T(90)$ :



**Bemerkung 52.** Sind  $x, y \in \mathbb{Z}$  und gilt  $x \cdot y = 1$  so gilt  $|x| = |y| = 1$ .

**Satz 23** (Teilen mit Rest). *Sind  $n, m \in \mathbb{N} \setminus \{0\}$ , dann gibt es eindeutig bestimmte Zahlen  $k, r \in \mathbb{N}$ , so dass Folgendes gilt:*

- a)  $m = kn + r$
- b)  $r < n$

*Wir sagen in diesem Zusammenhang, dass die Zahl  $r$  den Rest von der (ganzzahligen) Division von  $m$  durch  $n$  ist.*

**Beweis.** Seien  $n, m \in \mathbb{N} \setminus \{0\}$  beliebig. Die Menge

$$M := \{k \in \mathbb{N} \mid kn \leq m\}$$

ist endlich (da  $n \geq 1$ ), somit gibt es ein maximales Element  $k_0 \in M$ . Wir definieren  $r := m - k_0 n$ . Da  $k_0 \in M$  gilt, ist  $r \in \mathbb{N}$ . Es gilt

$$k_0 n + r = k_0 n + (m - k_0 n) = m.$$



Falls  $r \geq n$  wäre, dann würde

$$m - (k_0 + 1)n = m - (k_0n + n) = r - n \geq 0$$

und somit  $k_0 + 1 \in M$  gelten, was im Widerspruch zur Maximalität von  $k_0$  in  $M$  steht. Wir müssen nun noch die Eindeutigkeit zeigen. Es genügt zu zeigen, dass für  $r, r' < n$

$$(kn + r = k'n + r') \Rightarrow (k = k')$$

gilt. Wir machen einen Beweis durch Widerspruch und nehmen also  $k \neq k'$  an. Aus Symmetriegründen können wir  $k < k'$  und somit  $k' = k + p$  mit  $p > 0$  annehmen. Es gilt also

$$kn + r = k'n + r' = (k + p)n + r' = kn + pn + r'$$

und somit

$$r = pn + r' \geq n,$$

ein Widerspruch. □

**Übung 37.** Schreiben Sie in der Programmiersprache Ihrer Wahl eine Funktion, die zwei positive ganze Zahlen mit Rest teilt (natürlich ohne die Verwendung des Modulo Operators).

**Lösung.** Elektronisch zu lösen.

**Definition 46.** Seien  $n, m \in \mathbb{Z}$ . Wir definieren das *kleinste gemeinsame Vielfache* von  $n$  und  $m$  als

$$kgV(n, m) := \min\{k \in \mathbb{N} \mid n|k \wedge m|k\}.$$

Ist  $n \neq 0$  oder  $m \neq 0$ , dann definieren wir den *grössten gemeinsamen Teiler* von  $n$  und  $m$  als

$$ggT(n, m) := \max\{k \in \mathbb{N} \mid k|n \wedge k|m\}.$$

**Lemma 5.** Sind  $x, y, z \in \mathbb{Z}$ , dann sind folgende Aussagen äquivalent:

1.  $x|y \wedge x|z$
2.  $x|y \wedge x|(y - z)$

**Beweis.** 1.  $\Rightarrow$  2.: Wenn  $x|y \wedge x|z$ , dann gibt es ganze Zahlen  $k, k' \in \mathbb{Z}$ , so dass  $y = kx$  und  $z = k'x$ . Es gilt also  $y - z = kx - k'x = (k - k')x$ .

2.  $\Rightarrow$  1.: Es seien  $k, k' \in \mathbb{Z}$ , so dass  $y = kx$  und  $y - z = k'x$ . Durch Einsetzen erhält man  $kx - z = k'x$  und somit  $z = kx - k'x = x(k - k')$ . □

**Satz 24** (Euklidischer Algorithmus). Für  $n, m \in \mathbb{N}$  mit  $0 < n < m$  gilt

$$ggT(n, m) = ggT(n, m - n) = ggT(m, m - n).$$

*Beweis.* Aus Lemma 5 folgt für  $n, m \in \mathbb{N}$  mit  $n < m$

$$\{k \in \mathbb{N} \mid k|n \wedge k|m\} = \{k \in \mathbb{N} \mid k|n \wedge k|(m - n)\}.$$

Daraus folgt weiter

$$ggT(n, m) = \max\{k \in \mathbb{N} \mid k|n \wedge k|m\} = \max\{k \in \mathbb{N} \mid k|n \wedge k|(m - n)\} = ggT(n, m - n).$$

Die Gleichung

$$ggT(n, m) = ggT(m, m - n)$$

folgt analog aus Lemma 5. □

**Bemerkung 53** (Euklidischer Algorithmus). Aus dem eben bewiesenen Satz 24 erhalten wir direkt einen rekursiven Algorithmus zur Berechnung des  $ggT$ . Beispielhaft geht man dabei wie folgt vor:

$$\begin{aligned} ggT(45, 25) &\stackrel{\text{Satz 24}}{=} ggT(25, 20) \\ &\stackrel{\text{Satz 24}}{=} ggT(20, 5) \\ &\stackrel{\text{Satz 24}}{=} ggT(5, 15) \\ &\stackrel{\text{Satz 24}}{=} ggT(5, 10) \\ &\stackrel{\text{Satz 24}}{=} ggT(5, 5) = 5. \end{aligned}$$

Dieses Vorgehen lässt sich direkt in Java umsetzen:

```
int ggT(int n, int m){
    if (n == m) return n;
    if (n < m) return ggT(n, m - n);
    return ggT(m, n - m);
}
```

Betrachten wir nochmals den Satz 24, dann sehen wir, dass wir mehrere Schritte zu einem einzigen Schritt zusammenfassen können. Bei  $x > y$  wird nämlich, zum Berechnen von  $ggT(y, x)$  so oft  $y$  von  $x$  subtrahiert, bis das Resultat kleiner oder gleich  $y$  ist. Man kann all diese Subtraktionen also durch eine einzige Division mit Rest ersetzen. Die beispielhafte Berechnung von  $ggT(45, 25)$  können wir nun als 2 Divisionen mit Rest darstellen:

$$\begin{aligned} 45 &= 1 \cdot 25 + 20 \\ 25 &= 1 \cdot 20 + \underbrace{5}_{ggT(45, 25)}. \end{aligned}$$

Zusammenfassend stellen wir fest, dass

$$\text{ggT}(y, x) = \text{ggT}(y, R(x, y))$$

mit

$R(x, y)$  = der Rest der Division von  $x$  durch  $y$

gilt. Die Funktion  $R(x, y)$  steht in vielen Programmiersprachen als “modulo Funktion” zur Verfügung und wird im Quellcode oft durch das Prozentzeichen % aufgerufen. Dies eröffnet die Möglichkeit den euklidischen Algorithmus kompakter zu notieren:

```
int ggT(int n, int m){
    if (n == 0) return m;
    if (n < m) return ggT(m % n, n);
    return ggT(n % m, m);
}
```

**Übung 38.** Benutzen Sie den euklidischen Algorithmus um  $\text{ggT}(27, 96)$  auszurechnen (notieren Sie die Zwischenresultate).

**Lösung.**

**Definition 47.** Zwei ganze Zahlen  $x, y$  heissen *teilerfremd*, wenn  $\text{ggT}(x, y) = 1$  gilt.

**Theorem 4** (Lemma von Bézout). *Sind  $x, y \in \mathbb{Z}$  mit  $x, y \neq 0$ , dann gibt es ganze Zahlen  $a, b$  so dass*

$$\text{ggT}(x, y) = ax + by$$

*gilt. Die Zahlen  $a$  und  $b$  werden Bézout Koeffizienten genannt.*

**Beweis.** Wir können ohne Einschränkung der Allgemeinheit  $x, y \geq 1$  annehmen und die Behauptung

$$\forall x, y \geq 1 \exists a, b \in \mathbb{Z} (\text{ggT}(x, y) = ax + by).$$

beweisen. Wir führen den Beweis durch Widerspruch. Es gebe also natürliche Zahlen  $x, y \geq 1$  mit

$$\varphi(x, y) : \Leftrightarrow \forall a, b \in \mathbb{Z} (ax + by \neq \text{ggT}(x, y)).$$

Insbesondere existieren folgende kleinste natürliche Zahlen (Methode des kleinsten Verbrechers):

$$x_0 = \min\{n \geq 1 \mid \exists k \geq 1 \varphi(n, k)\} = \min\{n \geq 1 \mid \exists k \geq 1 \forall a, b \in \mathbb{Z} (an + bk \neq \text{ggT}(n, k))\}$$

$$y_0 = \min\{n \geq 1 \mid \varphi(x_0, n)\} = \min\{n \geq 1 \mid \forall a, b \in \mathbb{Z} (ax_0 + bn \neq \text{ggT}(x_0, n))\}$$

Es gilt offensichtlich  $x_0 \neq y_0$  und  $\varphi(x, y) \Leftrightarrow \varphi(y, x)$ . Wir können daher ohne Einschränkung  $x_0 < y_0$  annehmen. Weil  $1 \leq y_0 - x_0 < y_0$  gilt, gibt es ganze Zahlen  $a, b \in \mathbb{Z}$  mit  $ax_0 + b(y_0 - x_0) = \text{ggT}(x_0, y_0 - x_0)$ . Mit dem Euklidischen Algorithmus folgt daraus der gesuchte Widerspruch (zur Wahl von  $x_0$  und  $y_0$ ):

$$\begin{aligned} (a - b)x_0 + by_0 &= ax_0 - bx_0 + by_0 \\ &= ax_0 + b(y_0 - x_0) \\ &= \text{ggT}(x_0, y_0 - x_0) \\ &= \text{ggT}(x_0, y_0) \end{aligned}$$

□

**Übung 39.** Zeigen Sie, dass Bézout Koeffizienten nicht eindeutig sind.

**Lösung.** Es sei  $a$  und  $b$  Bézout Koeffizienten von  $x$  und  $y$ . Es gilt:

$$\text{ggT}(a, b) = ax + by = ax + by + xy - xy = ax + xy + by - xy = (a + y)x + (b - x)y$$

**Beispiel 59.** Wir wollen ganze Zahlen  $a$  und  $b$  finden, die die Gleichung

$$a \cdot 504 + b \cdot 29 = \text{ggT}(504, 29) = 1$$

erfüllen.

- Schritt 1: Sukzessives Teilen mit Rest.

$$\begin{aligned}
 504 &= 17 \cdot 29 + 11 \\
 29 &= 2 \cdot 11 + 7 \\
 11 &= 1 \cdot 7 + 4 \\
 7 &= 1 \cdot 4 + 3 \\
 4 &= 1 \cdot 3 + \underbrace{1}_{\text{ggT}(504,29)}.
 \end{aligned}$$

- Schritt 2: "Rückwärts einsetzen".

$$\begin{aligned}
 1 &= 4 - 3 \\
 &= (11 - 7) - (7 - 4) \\
 &= ((504 - 17 \cdot 29) - (29 - 2 \cdot 11)) - ((29 - 2 \cdot 11) - (11 - 7)) \\
 &= ((504 - 17 \cdot 29) - (29 - 2 \cdot (504 - 17 \cdot 29))) \\
 &\quad - ((29 - 2 \cdot (504 - 17 \cdot 29)) - ((504 - 17 \cdot 29) - (29 - 2 \cdot 11))) \\
 &= ((504 - 17 \cdot 29) - (29 - 2 \cdot (504 - 17 \cdot 29))) - ((29 - 2 \cdot (504 - 17 \cdot 29)) \\
 &\quad - ((504 - 17 \cdot 29) - (29 - 2 \cdot (504 - 17 \cdot 29)))).
 \end{aligned}$$

- Schritt 3: Zusammenfassen (Zählen der Vorkommen von 504 und 29).

$$\begin{aligned}
 a &= 1 + 2 + 2 + 1 + 2 = 8 \\
 b &= -17 - 1 - (2 \cdot 17) - 1 - (2 \cdot 17) - 17 - 1 - (2 \cdot 17) = -139
 \end{aligned}$$

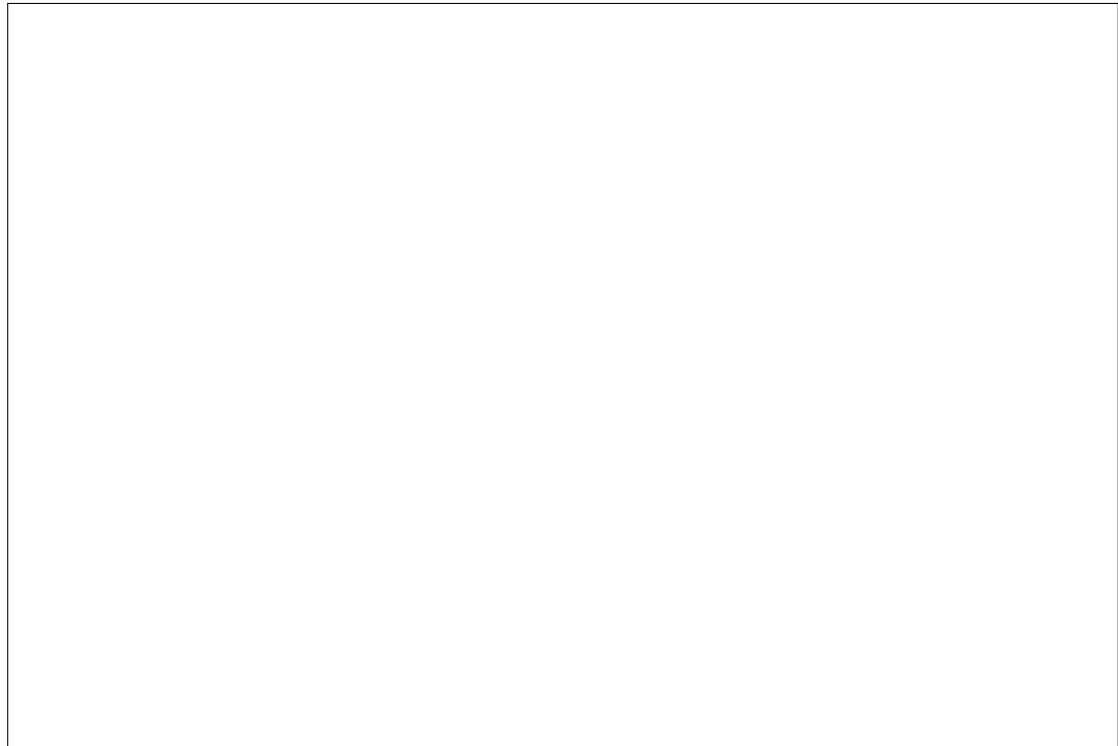
- Test:

$$8 \cdot 504 - 139 \cdot 29 = 1.$$

**Übung 40.** Finden Sie ganze Zahlen  $a$  und  $b$ , die folgende Gleichung erfüllen:

$$a \cdot 3215 + b \cdot 123 = 1.$$

**Lösung.**



## 5.2 Primzahlen

Primzahlen sind natürliche Zahlen, die genau zwei natürliche Zahlen als Teiler haben. Eine dazu äquivalente Formulierung ist, dass eine Primzahl eine von 1 verschiedene natürliche Zahl ist, die (in  $\mathbb{N}$ ) nur durch sich selbst und durch 1 teilbar ist. Die ersten 25 Primzahlen sind:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

**Definition 48.** Eine natürliche Zahl  $p \in \mathbb{N}$  ist eine *Primzahl*, wenn  $|T(p)| = 2$  gilt. Die Menge aller Primzahlen bezeichnen wir mit  $\mathbb{P}$ .

**Bemerkung 54.** Ist  $p$  eine Primzahl, dann gilt  $T(p) = \{1, p\}$ .

*Beweis.* Für jede Zahl  $n \in \mathbb{N}$  gilt offensichtlich  $n \in T(n)$  und  $1 \in T(n)$ . Bei Primzahlen kommt dazu, dass (wegen  $|T(n)| = 2$ ) keine weiteren Teiler existieren.  $\square$

**Bemerkung 55.** Betrachtet man die Teilbarkeitsrelation auf der Menge  $\mathbb{N} \setminus \{1\}$ , dann sind die Primzahlen genau die minimalen Elemente dieser Halbordnung.

Primzahlen haben die Eigenschaft, dass sie mit jedem Produkt auch mindestens einen der Faktoren teilen. Umgekehrt ist auch jede von 1 verschiedene natürliche Zahl mit dieser Eigenschaft eine Primzahl. Diese Tatsache wird als Lemma von Euklid bezeichnet.

**Satz 25** (Lemma von Euklid). *Folgende Aussagen sind für  $p \in \mathbb{N}$  mit  $p \neq 1$  äquivalent:*

1.  $\forall n, m \in \mathbb{N} (p|nm \Rightarrow p|n \vee p|m)$
2.  $p \in \mathbb{P}$

*Beweis.*  $1 \Rightarrow 2$ : Wir müssen zeigen, dass eine natürliche Zahl  $p$  mit der Eigenschaft wie in 1. bereits eine Primzahl ist. Wir nehmen an, dass  $p$  die in 1. postulierte Eigenschaft besitzt und dass  $x \in \mathbb{N}$  ein Teiler von  $p$  ist. Wir müssen zeigen, dass  $x = 1$  oder  $x = p$  gilt. Da  $x$  ein Teiler von  $p$  ist, gibt es eine natürliche Zahl  $y$  mit  $xy = p$ , insbesondere gilt also  $p|xy$ . Wegen 1. gilt also  $p|x$  oder  $p|y$ , daraus folgt  $p = x$  oder  $p = y$  (Antisymmetrie der Teilbarkeit auf  $\mathbb{N}$ ). Es folgt wie gewünscht, dass  $x = 1$  oder  $x = p$  gilt.

$2 \Rightarrow 1$ : Wir nehmen an, dass  $p$  eine Primzahl sei und müssen für beliebige natürliche Zahlen  $n, m$

$$p|(nm) \Rightarrow (p|n) \vee (p|m)$$

zeigen. Wir tun dies, indem wir aus  $p|(nm)$  und  $\neg(p|n)$  folgern, dass  $p|m$  gelten muss. Weil  $|T(p)| = 2$  gilt und da  $p$  kein Teiler von  $n$  ist, sind  $n$  und  $p$  teilerfremd. Nach Theorem 4 (Lemma von Bézout) gibt es also ganze Zahlen  $k, r$  mit

$$1 = pk + nr.$$

Andererseits folgt aus  $p|nm$ , dass es eine natürliche Zahl  $t$  mit

$$nm = pt$$

gibt. Insgesamt gilt also

$$\begin{aligned} m &= m \cdot 1 = m(pk + nr) \\ &= mpk + mnr \\ &= mpk + ptr \\ &= p(mk + tr). \end{aligned}$$

Somit ist also wie gewünscht,  $p$  ein Teiler von  $m$ . □

**Satz 26.** *Jede ganze Zahl  $z$  mit  $z \notin \{-1, 1\}$  besitzt einen Primfaktor (einen Teiler, der eine Primzahl ist). Formal können wir dies als*

$$\forall z \in \mathbb{Z} (z \notin \{-1, 1\} \Rightarrow T(z) \cap \mathbb{P} \neq \emptyset)$$

*ausdrücken.*

*Beweis.* Sei  $z \in \mathbb{Z}$  mit  $z \notin \{-1, 1\}$ . Die Menge  $M := \{n \in \mathbb{N} \mid n > 1 \wedge n|z\}$  ist nicht leer, da sie mindestens  $|z|$  als Element enthält. Nach dem Minimumsprinzip besitzt  $M$  also ein kleinstes Element  $m = \min(M)$ . Wir zeigen durch Widerspruch, dass  $m$  eine Primzahl ist. Wenn wir annehmen, dass  $m$  keine Primzahl ist, dann gibt es einen Teiler  $t \in \mathbb{N}$  von  $m$  mit  $1 < t < m$  (da  $|T(m)| \geq 3$ ). Aus der Transitivität der Teilbarkeitsrelation folgt aus  $t|m$  und  $m|z$ , dass  $t|z$  gilt. Insgesamt ist also  $t < m$  und  $t \in M$ , was im Widerspruch zur Minimalität von  $m$  in  $M$  steht.  $\square$

**Theorem 5.** *Es gibt unendlich viele Primzahlen.*

*Beweis.* Wir machen einen Widerspruchsbeweis. Wir nehmen an, dass es nur endlich viele Primzahlen  $\mathbb{P} = \{p_1, \dots, p_n\}$  gibt. Nach Satz 26 gibt es eine Primzahl  $p_i$  so, dass

$$p_i \mid \left(\prod_{j=1}^n p_j\right) + 1.$$

Es gibt also eine natürliche Zahl  $k$  so, dass

$$p_i \cdot k = \left(\prod_{j=1}^n p_j\right) + 1$$

gilt. Daraus folgt

$$\begin{aligned} 1 &= p_i \cdot k - \left(\prod_{j=1}^n p_j\right) = p_i \cdot k - (p_1 \cdot \dots \cdot p_i \cdot \dots \cdot p_n) \\ &= p_i \cdot k - p_i \underbrace{(p_1 \cdot \dots \cdot p_{i-1} \cdot p_{i+1} \cdot \dots \cdot p_n)}_{:=p} \\ &= p_i(k - p). \end{aligned}$$

Es folgt also, dass  $p_i$  ein Teiler von 1 ist, das steht aber im Widerspruch zu  $p_i \in \mathbb{P}$ .  $\square$

**Theorem 6.** *Jede natürliche Zahl grösser als 1 ist das Produkt von endlich vielen Primzahlen.*

*Beweis.* Wir machen einen Beweis durch Widerspruch. Angenommen es gibt natürliche Zahlen, die sich nicht als Produkt von Primzahlen schreiben lassen, dann ist die Menge

$$M := \{n \in \mathbb{N} \setminus \{0, 1\} \mid n \text{ ist nicht das Produkt von endlich vielen Primzahlen}\}$$

nicht leer. Nach dem Minimumsprinzip gibt es also ein kleinstes Element  $m = \min(M)$ . Nach Satz 26 gibt es eine Primzahl  $p$  mit  $p|m$ . Da  $m$  selbst keine Primzahl ist, gibt es also eine natürliche Zahl  $k$  mit  $1 < k < m$  und  $pk = m$ . Da  $k < m$  gilt, muss es, wegen der Minimalität von  $m$  in  $M$ , eine Darstellung von  $k$  als Produkt von Primzahlen geben. Es gibt also eine natürliche Zahl  $n > 0$  und Primzahlen  $p_1, \dots, p_n$  so, dass

$$k = \prod_{i=1}^n p_i = p_1 \cdot p_2 \cdot \dots \cdot p_n.$$



Daraus folgt aber, dass

$$m = pk = p \cdot \prod_{i=1}^n p_i = p \cdot p_1 \cdot p_2 \cdot \dots \cdot p_n$$

ebenfalls das Produkt von endlich vielen Primzahlen ist, ein Widerspruch zu  $m \in M$ .  $\square$

**Theorem 7** (Primfaktorzerlegung). *Es sei  $p_i$  jeweils die  $i$ -te Primzahl. Für jede natürliche Zahl  $n > 1$  gibt es eine eindeutig bestimmte, endliche Folge  $a_1, \dots, a_k$  von natürlichen Zahlen mit  $a_k \neq 0$ , so dass*

$$n = \prod_{i=1}^k p_i^{a_i}$$

*gilt.*

*Beweis.* Die Existenzaussage folgt sofort aus Theorem 6. Die Eindeutigkeitsaussage folgt indessen aus Satz 25.  $\square$

**Übung 41.** Implementieren Sie in der Programmiersprache Ihrer Wahl einen Algorithmus, der jede gegebene natürliche Zahl ( $> 1$ ) in ihre Primfaktoren zerlegt.

**Lösung.** Elektronisch zu lösen

## 5.3 Modulare Arithmetik

In der modularen Arithmetik geht es darum mit Restklassen, annähernd so wie mit Zahlen, zu rechnen. Die Anwendungen der modularen Arithmetik durchdringen viele Teilgebiete der Informatik:

- Modulare Arithmetik wird oft verwendet, um Prüfsummen nachzurechnen. Im Kontext von IBAN Nummern werden zum Beispiel Eingabefehler durch Summierung modulo 97 erkannt.
- In der Kryptografie findet die modulare Arithmetik direkte Anwendung im *RSA*-Kryptosystem.
- In der Computeralgebra verwendet man modulare Arithmetik für effiziente Algorithmen. Zum Beispiel zur Faktorisierung von Polynomen.
- Modulare Arithmetik wird oft im Kontext von Operationen auf zyklischen Datenstrukturen verwendet (z.B. Bitweise Operationen). Die *XOR*-Operation kann man z.B. durch die Summe der Bits modulo 2 berechnen.

Die Grundlage der modularen Arithmetik ist die “kongruent modulo”-Relation.

**Definition 49.** Es sei  $n \in \mathbb{N}$  beliebig. Wir definieren eine Relation  $\equiv_n$  auf  $\mathbb{Z}$  wie folgt:

$$r \equiv_n s :\Leftrightarrow n \mid (r - s).$$

Gilt für  $r, s \in \mathbb{Z}$  die Relation  $r \equiv_n s$ , dann sagen wir, dass  $r$  gleich  $s$  modulo  $n$  ist und schreiben  $r = s \bmod n$ .

**Bemerkung 56.** Die Relation  $\equiv_n$  ist für jede natürliche Zahl  $n$  eine Äquivalenzrelation auf  $\mathbb{Z}$ .

**Bemerkung 57.** Es sei  $n \in \mathbb{N}$  beliebig. Für je zwei ganze Zahlen  $x$  und  $y$  gilt  $x \equiv_n y$  genau dann, wenn  $x$  und  $y$  denselben Rest bei Division durch  $n$  lassen.

**Folgerung.** Es sei  $n \in \mathbb{N}$  beliebig. Jede ganze Zahl  $z$  steht mit genau einer natürlichen Zahl aus  $\{0, \dots, n-1\}$  in der Relation  $\equiv_n$ .

**Definition 50.** Es sei  $n \in \mathbb{N}$  beliebig. Für jede ganze Zahl  $z$  bezeichnen wir mit

$$[z]_n := \{x \in \mathbb{Z} \mid x \equiv_n z\}$$

die Äquivalenzklasse von  $z$  bezüglich der Relation  $\equiv_n$  und nennen diese auch die *Restklasse* von  $z$ . Abkürzend bezeichnen wir  $[z]_n$  auch mit  $\bar{k}$ , wenn  $k \in \{0, \dots, n-1\}$  und  $z \equiv_n k$  gilt.

**Folgerung.** Es sei  $n \in \mathbb{N}$  beliebig. Es gilt

$$[z]_n = \{z + yn \mid y \in \mathbb{Z}\} = \{\dots, z - 3n, z - 2n, z - n, z, z + n, z + 2n, z + 3n, \dots\}.$$

Damit wir mit Restklassen sinnvoll rechnen können, müssen wir uns davon überzeugen, dass die Rechenoperationen unabhängig von der Wahl von Repräsentanten sind.

**Bemerkung 58.** Es sei  $n \in \mathbb{N}$  beliebig. Für ganze Zahlen  $x, x'$  und  $y, y'$  gelten<sup>1</sup>:

- a)  $[x] = [x'] \wedge [y] = [y'] \Rightarrow [x + y] = [x' + y']$
- b)  $[x] = [x'] \wedge [y] = [y'] \Rightarrow [xy] = [x'y']$

<sup>1</sup>Wenn die natürliche Zahl  $n$  aus dem Kontext klar ersichtlich ist, so lassen wir diese in der Notation  $[x]_n$  auch manchmal weg.

*Beweis.* a) Aus  $[x] = [x']$  und  $[y] = [y']$  folgt, dass  $x - x'$  und  $y - y'$  Vielfache von  $n$  sind. Es folgt also, dass

$$(x + y) - (x' + y') = x - x' + (y - y')$$

auch ein Vielfaches von  $n$  ist und somit, dass  $[x + y] = [x' + y']$  gilt.

b) Wir zeigen zuerst, dass unter der Voraussetzung  $x \equiv_n x'$  für alle  $z \in \mathbb{Z}$  die Gleichung

$$[xz + x] = [x'z + x']$$

gilt. Diese folgt aber aus

$$\begin{aligned} (xz + x) - (x'z + x') &= xz - x'z + x - x' = z(x - x') + (x - x') \\ &= (z + 1) \underbrace{(x - x')}_{\text{ist Vielfaches von } n}. \end{aligned}$$

Daraus folgt für  $[x] = [x']$  und  $[y] = [y']$ :

$$\begin{aligned} [xy] &= [x(y - 1) + x] \\ &= [x'(y - 1) + x'] \\ &= [x'y] = [yx'] \\ &= [y(x' - 1) + y] \\ &= [y'(x' - 1) + y'] \\ &= [x'y']. \end{aligned}$$

□

**Definition 51.** Es sei  $n \in \mathbb{N}$  beliebig. Die Menge aller Restklassen von  $\mathbb{Z}$  modulo  $n$  bezeichnen wir mit

$$\mathbb{Z}/n = \{[z]_n \mid z \in \mathbb{Z}\} = \{\bar{k} \mid 0 \leq k < n - 1 \wedge z \equiv_n k\} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}.$$

Wir definieren zwei Verknüpfungen  $\cdot : (\mathbb{Z}/n)^2 \rightarrow \mathbb{Z}/n$  und  $+: (\mathbb{Z}/n)^2 \rightarrow \mathbb{Z}/n$  durch die Zuordnungen

$$[x]_n + [y]_n := [x + y]_n$$

und

$$[x]_n \cdot [y]_n := [xy]_n.$$

**Beispiel 60.** Die Verknüpfungstabelle der Addition in  $\mathbb{Z}/6$ :

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

Die Verknüpfungstabelle der Multiplikation in  $\mathbb{Z}/6$ :

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

**Bemerkung 59.** Wir betrachten die Gleichung

$$\bar{3} + x = \bar{2}$$

in  $\mathbb{Z}/5$ . Setzen wir

$$x = \bar{2} - \bar{3} = \overline{2-3} = \overline{-1} = \bar{4},$$

dann haben wir eine Lösung für die obige Gleichung:

$$\bar{3} + x = \bar{3} + \bar{4} = \overline{3+4} = \bar{7} = \bar{2}.$$

Dass dieses Vorgehen für jeden Modulo und jede Gleichung zielführend ist, folgt sofort aus

$$\overline{a + (b - a)} = \bar{b}.$$

**Beispiel 61** (Rechnen mit Uhrzeiten). Rechnen mit Uhrzeiten (volle Stunden einer Analoguhr) entspricht mit Restklassen Modulo 12 zu rechnen.

- Es ist 9 Uhr. Wie lange dauert es, bis es das nächste Mal 2 Uhr ist? Wir müssen die Gleichung

$$\bar{9} + x = \bar{2}$$

lösen. Wie vorher gesehen, erhalten wir die Lösung durch

$$x = \bar{2} + \overline{-9} = \overline{2-9} = \overline{-7} = \bar{5}.$$

Es geht also noch 5 Stunden bis 2 Uhr.

**Beispiel 62** (Rechnen mit Wochentagen).

- Es ist Montag. Welcher Wochentag ist in 2454 Tagen? Wir bezeichnen die Wochentage mit Elementen von  $\mathbb{Z}/7$ : Mo.=  $\bar{0}$ , Di.=  $\bar{1}$ , ... Der Wochentag in 2454 Tagen ist also

$$\bar{0} + \overline{2454} = \overline{2454} = \bar{4}$$

ein Freitag.

**Bemerkung 60.** Wir betrachten die Gleichung

$$\bar{2} \cdot x = \bar{3}$$

in  $\mathbb{Z}/5$ . Diese Gleichung besitzt als Lösung  $x = \bar{4}$ , weil

$$\bar{2} \cdot \bar{4} = \overline{2 \cdot 4} = \bar{8} = \bar{3}$$

gilt. Betrachten wir dieselbe Gleichung aber über  $\mathbb{Z}/4$ , dann sehen wir, dass diese Gleichung keine Lösung hat, weil:

$$\begin{aligned}\bar{2} \cdot \bar{0} &= \bar{0} \neq \bar{3} \\ \bar{2} \cdot \bar{1} &= \bar{2} \neq \bar{3} \\ \bar{2} \cdot \bar{2} &= \bar{0} \neq \bar{3} \\ \bar{2} \cdot \bar{3} &= \bar{2} \neq \bar{3}.\end{aligned}$$

Woran liegt dies? Das Problem ist, dass  $\bar{2}$  in  $\mathbb{Z}/2$  nicht "invertierbar" ist, " $\frac{1}{2}$ " existiert in  $\mathbb{Z}/4$  nicht. In  $\mathbb{Z}/5$  hingegen ist  $\bar{2}$  sehr wohl invertierbar, weil  $\bar{2} \cdot \bar{3} = \bar{1}$  gilt (" $\frac{1}{2}$ " ist  $\bar{3}$  in  $\mathbb{Z}/5$ ).

Im nächsten Satz sehen wir, dass in  $\mathbb{Z}/n$  genau dann alle Gleichungen von der Form

$$ax = b$$

(für beliebige aber feste  $a, b \in \mathbb{Z}/n$  mit  $a \neq 0$ ) eine Lösung besitzen, wenn  $n$  eine Primzahl ist.

**Theorem 8.** *Es sei  $n \in \mathbb{N} \setminus \{1\}$  beliebig. Folgende Aussagen sind äquivalent:*

1.  *$n$  ist eine Primzahl.*
2. *Für jedes  $\bar{k} \in \mathbb{Z}/n$  mit  $\bar{k} \neq \bar{0}$  gibt es genau ein  $r \in \{0, \dots, n-1\}$  mit  $\bar{k} \cdot \bar{r} = \bar{1}$ .*

Die zweite Aussage besagt, dass man in  $\mathbb{Z}/n$  Gleichungen von der Form  $ax = b$  stets nach  $x$  auflösen kann. Sind  $\bar{k}, \bar{r} \in \mathbb{Z}/n$  mit  $\bar{k} \cdot \bar{r} = \bar{1}$ , so sagen wir  $\bar{r}$  sei invers (bezüglich der Multiplikation) zu  $\bar{k}$  und schreiben auch  $(\bar{k})^{-1}$  für  $\bar{r}$ .

**Beweis.** Wir beweisen zuerst  $1. \Rightarrow 2.$  und dann  $2. \Rightarrow 1.$

$1. \Rightarrow 2.$  : Es sei  $n$  eine Primzahl und  $\bar{k} \neq \bar{0}$ . Ohne Einschränkung sei  $0 < k < n$ . Weil  $n$  eine Primzahl ist, sind  $n$  und  $k$  teilerfremd. Daraus folgt, dass es ganze Zahlen  $a$  und  $b$  gibt mit

$$ak + bn = 1.$$

Es gilt also

$$\bar{1} = \overline{ak + bn} = \overline{ak} + \underbrace{\overline{bn}}_{=\bar{0}} = \overline{ak} = \bar{a} \cdot \bar{k}.$$

Die gesuchte Zahl  $r$  erhalten wir somit durch den Rest der Division von  $a$  durch  $n$  ( $r = a \% n$ ).

2.  $\Rightarrow$  1. : Es sei  $n \in \mathbb{N} \setminus \mathbb{P}$ . Da wir ohne Einschränkung  $n \notin \{0, 1\}$  annehmen können<sup>2</sup>, gibt es natürliche Zahlen  $1 < r, s < n$  mit  $n | rs$ . Wenn nun die Aussage 2. für  $n$  gelten würde, dann hätten wir

$$\bar{1} = \bar{r}(\bar{r})^{-1}\bar{s}(\bar{s})^{-1} = \underbrace{(\bar{r} \cdot \bar{s})}_{=\bar{0}}(\bar{r})^{-1}(\bar{s})^{-1} = \bar{0},$$

ein Widerspruch. □

**Übung 42.** Es sei  $n \in \mathbb{N}$  beliebig, dann heisst  $\bar{k} \in \mathbb{Z}/n$  invertierbar, falls es zu  $\bar{k}$  inverse Elemente in  $\mathbb{Z}/n$  gibt.

- a) Geben Sie alle invertierbaren Elemente von  $\mathbb{Z}/n$  für  $n = 1, 3, 4, 5$  an.
- b) Lösen Sie  $\bar{3}x = \bar{4}$  in  $\mathbb{Z}/7$ .
- c) Geben Sie das bezüglich  $\cdot$  zu 3 inverse Element in  $\mathbb{Z}/11$  an.

### 5.3.1 Chinesischer Restsatz

Der chinesische Restsatz besagt, dass bei paarweise teilerfremden Zahlen  $n_1, \dots, n_k \in \mathbb{N}_{>1}$  und beliebigen ganze Zahlen  $y_1, \dots, y_k$ , Gleichungssysteme von der Form<sup>3</sup>

$$\begin{aligned} x &\equiv_{n_1} y_1 \\ x &\equiv_{n_2} y_2 \\ &\vdots \\ x &\equiv_{n_k} y_k \end{aligned}$$

eindeutig in  $\mathbb{Z}/(n_1, \dots, n_k)$  lösbar<sup>4</sup> sind.

**Satz 27** (Chinesischer Restsatz). *Es seien  $n_1, \dots, n_k \in \mathbb{N}_{>1}$  paarweise teilerfremd und weiter  $y_1, \dots, y_k \in \mathbb{Z}$  beliebig. Es gibt genau eine natürliche Zahl  $x < \prod_{i=1}^k n_i$  so, dass die*

---

<sup>2</sup>Für  $n = 0$  entspricht  $(\mathbb{Z}/n, \cdot)$  der Struktur  $(\mathbb{Z}, \cdot)$ , für  $n = 1$  der Struktur  $(\{\bar{0}\}, \cdot)$

<sup>3</sup>Solche Gleichungssysteme heissen simultane Kongruenzen.

<sup>4</sup>Damit meinen wir, dass die Lösungsmenge des Gleichungssystems genau ein Element (Äquivalenzklasse) von  $\mathbb{Z}/(n_1, \dots, n_k)$  ist.

*Lösungsmenge des Systems*

$$x \equiv_{n_1} y_1$$

$$x \equiv_{n_2} y_2$$

.

.

.

$$x \equiv_{n_k} y_k$$

der Menge  $[x]_{\prod_{i=1}^k n_i}$  entspricht.

*Beweis.* Vgl. Algorithmus. □

**Beispiel 63.** Wir betrachten folgendes System simultaner Kongruenzen:

$$x \equiv_2 0$$

$$x \equiv_3 2$$

$$x \equiv_5 3$$

Wir sehen, dass 8 das System löst und wissen daher, aufgrund des chinesischen Restsatzes, dass die Lösungsmenge gerade

$$[8]_{30} = \{8 + 30z \mid z \in \mathbb{Z}\} = \{\dots, -22, 8, 38, \dots\}$$

entspricht.

**Übung 43.** Lösen Sie das System

$$x \equiv_4 3$$

$$x \equiv_5 2$$

$$x \equiv_9 1$$

**Bemerkung 61.** Aus dem chinesischen Restsatz folgt, dass wir, um ein System simultaner Kongruenzen zu lösen, bloss eine Lösung davon kennen müssen. Durch sukzessive Substitution genügt es also jeweils eine Lösung von einem System mit zwei Gleichungen zu finden um beliebige Systeme lösen zu können. Wie Sie in der letzten Aufgabe eventuell geahnt haben, kann dies aber immer noch ziemlich mühsam sein, daher wollen wir dieses Teilproblem algorithmisch lösen.

**Algorithmus** (Lösen simultaner Kongruenzen). Wir wollen ein System simultaner Kongruenzen mit zwei Gleichungen lösen, etwa

$$x \equiv_{n_1} y_1$$

$$x \equiv_{n_2} y_2$$

mit  $n_1$  und  $n_2$  teilerfremd. Wir gehen schrittweise wie folgt vor:

a) Durch sukzessives Teilen mit Rest (wie im Beweis von Satz 4) erhalten wir ganze Zahlen  $a, b$  mit  $an_1 + bn_2 = 1$ .

b) Wir setzen  $x := y_1bn_2 + y_2an_1$ .

*Korrektheit des Algorithms:* Wir müssen lediglich überprüfen, dass  $x := y_1bn_2 + y_2an_1$  das System löst, wenn  $an_1 + bn_2 = 1$  ist. Es gilt

$$[1]_{n_1} = [an_1 + bn_2]_{n_1} = [bn_2]_{n_1}$$

und damit

$$[y_1]_{n_1} = [y_1]_{n_1} \cdot [bn_2]_{n_1} = [y_1bn_2]_{n_1} = [y_1bn_2]_{n_1} + \underbrace{[y_2an_1]_{n_1}}_{=[0]} = [y_1bn_2 + y_2an_1]_{n_1}$$

Also gilt  $x = y_1 \bmod n_1$ . Andererseits gilt auch

$$[1]_{n_2} = [an_1 + bn_2]_{n_2} = [an_1]_{n_2}$$

und deshalb

$$[y_2]_{n_2} = [y_2an_1]_{n_2} = [y_1bn_2]_{n_2} + [y_2an_1]_{n_2} = [y_1bn_2 + y_2an_1]_{n_2}.$$

□

**Beispiel 64.** Wir lösen das System

$$x \equiv_7 3$$

$$x \equiv_5 2$$

$$x \equiv_9 6$$

Wir lösen zuerst das Teilsystem

$$x \equiv_7 3$$

$$x \equiv_5 2$$

Wir teilen sukzessive mit Rest und erhalten

$$7 = 1 \cdot 5 + 2 \tag{5.1}$$

$$5 = 2 \cdot 2 + 1 \tag{5.2}$$

und somit

$$\begin{aligned} 1 &\stackrel{(4.2)}{=} 5 - 2 \cdot 2 \\ &\stackrel{(4.1)}{=} 5 - 2(7 - 5) \\ &= 5 - 2 \cdot 7 + 2 \cdot 5 \\ &= \mathbf{3} \cdot 5 + \mathbf{(-2)} \cdot 7 \end{aligned}$$



Wir haben also als Lösung

$$x = 3 \cdot 3 \cdot 5 + 2 \cdot (-2) \cdot 7 = 17$$

und als Lösungsmenge  $[17]_{35}$ . Wir müssen nun noch das System

$$x \equiv_{35} 17$$

$$x \equiv_9 6$$

lösen. Wir teilen sukzessive mit Rest:

$$35 = 3 \cdot 9 + 8$$

$$9 = 1 \cdot 8 + 1.$$

Wir erhalten damit:

$$\begin{aligned} 1 &= 9 - 8 \\ &= 9 - (35 - 3 \cdot 9) \\ &= 4 \cdot 9 + (-1) \cdot 35. \end{aligned}$$

Eine Lösung ergibt sich erneut durch

$$x := 17 \cdot 4 \cdot 9 + 6 \cdot (-1) \cdot 35 = 402.$$

Die Lösungsmenge des ganzen Systems ist also  $[402]_{35 \cdot 9} = [87]_{315}$ .

Der nächste Satz ist der sogenannte “kleine (Satz von) Fermat”. Er findet Verwendung bei (probabilistischen) Primzahltests und bildet die Grundlage des “Shor-Algorithmus”, einem Quantenalgorithmus zur Faktorisierung von ganzen Zahlen.

Zuerst ein Lemma.

**Lemma 6.** *Ist  $a \in \mathbb{Z}/n$  mit  $n > 0$  invertierbar, dann ist die Funktion*

$$\begin{aligned} f : \mathbb{Z}/p &\rightarrow \mathbb{Z}/p \\ f(x) &= \bar{a} \cdot x \end{aligned}$$

*surjektiv.*

**Beweis.** Da die Menge  $\mathbb{Z}/n$  endlich ist, genügt es zu zeigen, dass für alle  $x$  und  $y$  die Implikation

$$f(x) = f(y) \Rightarrow x = y$$

gilt. Sei  $b$  das Inverse von  $a$  (es gilt also  $ab = ba = \bar{1}$ ). Es gilt nun wie gewünscht:

$$\begin{aligned} f(x) &= f(y) \\ \Rightarrow ax &= ay \\ \Rightarrow bax &= bay \\ \Rightarrow x &= y. \end{aligned}$$

□

**Satz 28** (Kleiner Fermat). *Ist  $p \in \mathbb{P}$  und  $a$  kein Vielfaches von  $p$ , dann gilt*

$$a^{p-1} \equiv_p 1.$$

*Beweis.* Da  $a \in \mathbb{Z}$  kein Vielfaches von  $p$  ist, sind  $a$  und  $p$  teilerfremd,  $a$  ist somit invertierbar in  $\mathbb{Z}/p$  (wir dürfen in  $\mathbb{Z}/p$  somit “durch  $a$  teilen”). Wir betrachten die Funktion

$$\begin{aligned} f : \mathbb{Z}/p &\rightarrow \mathbb{Z}/p \\ f(x) &= \bar{a} \cdot x \end{aligned}$$

Weil  $a$  eine Einheit ist, wissen wir aus Lemma 6, dass die Funktion  $f$  surjektiv ist. Es gilt also

$$f(\bar{1}) \cdot \dots \cdot f(\overline{p-1}) = \bar{1} \cdot \dots \cdot \overline{p-1}.$$

und somit

$$\bar{a}\bar{1} \cdot \dots \cdot \bar{a}\overline{p-1} = \bar{1} \cdot \dots \cdot \overline{p-1}$$

also

$$\bar{a}^{p-1}\bar{1} \cdot \dots \cdot \overline{p-1} = \bar{1} \cdot \dots \cdot \overline{p-1}.$$

Da alle Zahlen  $2, \dots, p-1$  zu  $p$  teilerfremd sind, erhalten wir daraus

$$\bar{a}^{p-1} = \bar{1}.$$

□

# Literaturverzeichnis

- [1] Rod Haggarty. *Diskrete Mathematik für Informatiker*. Pearson Studium, 2007.
- [2] Peter Hartmann. *Mathematik für Informatiker – ein praxisbezogenes Lehrbuch*. Mathematik/Informatik. Vieweg, 3 edition, 2004.
- [3] Ulrich Knauer. *Diskrete Strukturen – kurz gefasst*. Spektrum–Hochschultaschenbuch. Spektrum Akademischer Verlag, 2011.
- [4] Bodo Pareigis. *Lineare Algebra für Informatiker*. Springer, 2000.
- [5] H. D. Ebbinghaus / J. Flum / W. Thomas. *Einführung in die mathematische Logik*. Hochschultaschenbuch. Spektrum Akademischer Verlag, 5 edition, 2007.