Justus-Liebig-Universität Gießen
Fachbereich 07
Mathematisches Institut

Vorkurs Mathematik

Einführung in das mathematische Denken

Skript zur Vorlesung

PD Dr. Elena Berdysheva

JUSTUS-LIEBIG-
UNIVERSITÄT
GIESSEN

Vorwort

Dieses Skript ist entstanden aus der Vorlesung im Rahmen des Vorkurses Mathematik (Mathematisches Denken), welche ich seit dem Wintersemester 2016/2017 an der Justus-Liebig-Universität Gießen halte. Die Zielgruppe des Vorkurses sind Studienanfänger der Studiengänge Mathematik B.Sc., Physik B.Sc. sowie Mathematik Lehramt an Gymnasien.

Das Ziel dieses Vorkurses ist es, Studienanfängern den Einstieg in die Hochschulmathematik zu erleichtern. Es werden keine Inhalte aus dem mathematischen Schulunterricht thematisiert (wobei natürlich vorausgesetzt ist, dass die Teilnehmer über Kenntnisse der Schulmathematik verfügen). Vielmehr werden die Zuhörer anhand von mehreren ausgewählten Themen an die Denk- und Arbeitsweise eines Mathematikers herangeführt.

Bei der Vorbereitung meiner Vorlesungen habe ich mehrere Quellen benutzt. Eine von ihnen war das „Skript zum Mathematik-Vorkurs (VEMINT-Vorkurs P2)“ von Frau Dr. Kerstin Hesse von der Universität Paderborn. An dieser Stelle möchte ich Frau Dr. Hesse, die mir ihr Skript zur Verfügung gestellt und sich mit mir über ihre Erfahrungen mit den Vorkursen ausgetauscht hat, herzlichst danken. Das Buch von Hermann Schichl und Roland Steinbauer „Einführung in das mathematische Arbeiten“ (Springer-Verlag Berlin Heidelberg, 2009) diente mir als eine weitere Inspirationsquelle; manche Formulierung und manches Beispiel stammen aus diesem Buch. Das Buch kann ich interessierten Studierenden zum Weiterlesen empfehlen.

Auch weitere Materialien haben eine Verwendung gefunden. So habe ich an einigen Stellen das Skript zum Vorkurs Mathematik an der Universität Hohenheim benutzt, welchen ich viele Jahre lang geleitet habe. Die Originalfassung jenes Skriptums wurde von Frau Prof. Dr. Christine Bescherer und Herrn Rolf Springmann erstellt, später von Herrn Dr. Jens Höchsmann und dann von mir überarbeitet. Auch Skripte von Herren Prof. Dr. Kurt Jetter und Prof. Dr. Georg Zimmermann zu weiteren Lehrveranstaltungen an der Universität Hohenheim wurden von mir teilweise verwendet. Allen diesen Kollegen spreche ich an dieser Stelle einen Dank aus.

Des Weiteren danke ich Herrn Tibor Kovacs, der in früheren Jahren den Vorkurs Mathematik an der Universität Gießen — welcher allerdings nach einem anderen Konzept aufgebaut war — geleitet und mir seine Unterlagen zur Verfügung gestellt hat. Von Frau Prof. Dr. Margareta Heilmann bekam ich Aufgabensammlungen zu den mathematischen Vorkursen an der Universität Wuppertal; auch ihr gilt mein Dank.

Diese Fassung des Skriptes wurde von Herrn David Losacker erstellt. Herr Losacker hat meine handschriftlichen Notizen kritisch gelesen und teilweise überarbeitet sowie die LaTeX-Datei und die Bilder vorbereitet. Für seine fachlich wie technisch ausgezeichnete Arbeit am Skript danke ich ihm herzlichst.

Der Vorkurs wird durch Übungen in kleineren Gruppen begleitet. Ich bedanke mich bei Frau Rebekka Wünch für ihre Arbeit an den Dateien mit den Übungsaufgaben und deren Lösungen.

Ich wünsche allen Vorkursteilnehmern viel Erfolg und viel Spaß beim Studium!

Elena Berdysheva

Gießen, im Herbst 2017

Version des Skriptes: 13.09.2018

Inhaltsverzeichnis

Kapitel 0

Einführung

In der Mathematik verwendet man Definitionen, Sätze und Beweise. Im Folgenden werden diese Begriffe präzisiert und durch Beispiele illustriert.

Definitionen sind terminologische Vereinbarungen. Sie legen eindeutig fest, was unter einem bestimmten mathematischen Begriff zu verstehen ist. Exemplarisch betrachten wir hier die Definition einer Primzahl.

Definition 0.1.

Eine *Primzahl* ist eine natürliche Zahl, die durch genau zwei natürliche Zahlen ohne Rest teilbar ist.

Aufgrund dieser Definition kann man für jede Zahl entscheiden, ob sie eine Primzahl ist oder nicht. Beispielsweise sind $2, 3, 5, 7$ Primzahlen, 4 allerdings nicht, da sie von den drei Zahlen $1, 2$ und 4 geteilt wird. Ebenso ist auch 1 keine Primzahl, da sie nur einen Teiler besitzt.
Die Sprache der Mathematik ist sehr präzise. So kann man z.B. nicht von „schönen Matrizen“ reden (es sei denn, man definiert sie, z.B. „Eine Matrix heißt schön, wenn ihre Einträge nur die Zahlen 0 und 1 sind.“)

Mathematische Sätze bestehen aus Aussagen.

Definition 0.2.

Eine *Aussage* ist ein sprachliches Gebilde, das aufgrund seines Inhaltes entweder wahr oder falsch ist.

Beispiel 0.3.

1) Folgende Phrasen sind Aussagen:

   (a) Köln liegt am Rhein. (wahr)
   (b) Hamburg liegt an der Donau. (falsch)
   (c) $1 + 1 = 2$. (wahr)
   (d) $2 + 2 = 5$.(falsch)
   (e) $2^{859433} - 1$ ist eine Primzahl. (wahr oder falsch, wir wissen es nicht)

2) Das sind keine Aussagen:

   (a) Komm her!
   (b) 2 ist eine interessante Zahl.
   (c) $x + 3 + 8$.

Wir werden uns im Verlaufe des Kurses tiefgehender mit Aussagen beschäftigen (in Kapitel „Logik und Beweise“).

Mathematische *Sätze* sind Aussagen über mathematische Sachverhalte. Man kann sich die Mathematik als Gebäude vorstellen, dessen Fundament von Axiomen gebildet wird. *Axiome* sind Aussagen einer Theorie, die innerhalb dieses Systems nicht hergeleitet oder widerlegt werden können. Diese Aussagen werden als wahr angenommen.

Beispiel 0.4. Beispiele von Axiomen:

1) Fünf Axiome der euklidischen Geometrie.

2) Axiome der Peano-Arithmetik: Beschreibung der natürlichen Zahlen.

Alle anderen Aussagen werden aus Axiomen durch logische Schlussfolgerungen abgleitet. Dieser Vorgang heißt *beweisen*. In der Praxis gehen wir in der Regel nicht von Axiomen aus, sondern von schon bewiesenen Sätzen.

Ein *Satz* bzw. ein *Theorem* ist eine aus den Axiomen oder aus vorangegangenen bewiesenen Sätzen logisch hergeleitete Aussage. Theoreme enthalten *Voraussetzungen* und *Behauptungen*. Die Voraussetzungen nennen dabei die Bedingungen, unter denen die Behauptungen gelten. Als einführende Beispiele betrachten wir die folgenden Sätze und analysieren deren Aufbau.

Satz 0.5.

Jede von 2 verschiedene Primzahl ist ungerade.

Die Voraussetzungen sind hierbei, dass

1) $p \neq 2$,

2) p ist Primzahl,

während die Behauptung lautet, dass p ungerade ist.

Satz 0.6.

Wenn die natürliche Zahl a die natürlichen Zahlen b und c teilt, dann teilt a auch die Summe $b + c$ sowie die Differenz $b - c$ der beiden Zahlen.

In diesem Fall sind die Voraussetzungen:

1) a, b, c sind natürliche Zahlen,

2) a teilt b,

3) a teilt c.

Die Behauptungen sind in diesem Fall

1) a teilt $b + c$,

2) a teilt $b - c$.

Darüber hinaus gibt es noch weitere Namen für mathematische Aussagen. *Lemma* (Plural: Lemmata) bzw. *Hilfssatz* bezeichnet in der Regel ein kleineres Resultat, das im Rahmen des Beweises eines Satzes verwendet wird, selbst allerdings nicht den Rang/ die Wichtigkeit eines Satzes darstellt. Es sei angemerkt, dass die Einteilung in Sätze und Lemmata subjektiv ist. Ein *Korollar* bzw. eine *Folgerung* ist eine Aussage, die sich aus einem schon bewiesenen Satz ohne großen Mehraufwand herleiten lässt. Weiter existieren Haupt- und Fundamentalsätze, Propositionen und so weiter.

Logische Schlussfolgerungen und Beweistechniken werden später, in Kapitel „Logik und Beweise“, besprochen.

Kapitel 1

Mengenlehre

1.1 Mengenbegriff

Definition 1.1.

Eine *Menge* ist eine Zusammenfassung von wohlunterscheidbaren, bestimmten Objekten (*Elementen*) unserer Anschauung oder unseres Denkens zu einem Ganzen.

Beispiel 1.2.

1) Die Menge der im Raum anwesenden Studierenden.

2) Die Menge aller Teiler der Zahl 12.

3) Die Menge $P(M)$ der Teilmengen der Menge $M = \{0, 1, 2, 3\}$.

Das Wort „wohlunterscheidbar“ fordert, dass geklärt wird, was als gleich und was als verschieden anzusehen ist.

Beispiel 1.3.

1) $\frac{3}{2}$ und 1.5 sind gleich, wenn wir Zahlen betrachten.

2) $\frac{3}{2}$ und 1.5 sind verschieden, wenn wir Schreibweisen betrachten.

Das Wort „bestimmt“ bedeutet, dass bei jedem Element eindeutig entscheidbar ist, ob es zur Menge gehört oder nicht. In diesem Sinne ist die Gruppe aller guten Spieler einer Mannschaft keine Menge, es sei denn, es ist formal geklärt, welche Spieler „gut“ sind.

Notation 1.4.

- Ist x ein Element der Menge M, so schreibt man $x \in M$.
- Ist x kein Element der Menge M, so schreibt man $x \notin M$.

Definition 1.5.

Die Menge, die kein Element enthält, heißt *leere Menge*. Wir schreiben hier $\{\}$ oder $\emptyset$.

Mengen können in *aufzählender Form* oder in *beschreibender Form* angegeben werden.

Beispiel 1.6.

Aufzählend:	Beschreibend:
$A = \{1, 2, 3, 4, 6, 12\}$	$A = \{n \in \mathbb{N} : n \text{ teilt } 12\}$
$B = \{2, 4, 6, 8, \ldots\}$	$B = \{n \in \mathbb{N} : n \text{ ist gerade}\} = \{2k : k \in \mathbb{N}\}$
$C = \{0, 1\}$	$C = \{x \in \mathbb{R} : x = x^2\}$

Bei der beschreibenden Form sind die Elemente oft als spezielle Elemente einer weiteren Menge angegeben ($\mathbb{N}, \mathbb{R}$ usw.), für die bestimmte Bedingungen gelten. Die große Menge heißt dabei *Grundmenge*.

Beispiel 1.7.

1) $\{x \in \mathbb{Q} : x^2 = 2\} = \emptyset$

2) $\{x \in \mathbb{R} : x^2 = 2\} = \{\pm\sqrt{2}\}$

Statt „:“ wird auch „|“ geschrieben, z.B. $\{x \in \mathbb{R} \mid x^2 = 2\}$. Gelesen wird: „für die gilt“. Das nächste Beispiel illustriert Notation 1.4.

Beispiel 1.8.

1) $A = \{1, 2, 3, 4, 6, 12\},\ 6 \in A,\ 5 \notin A.$

2) $B = \{n \in \mathbb{N} : n \text{ ist gerade}\},\ 12 \in B,\ 25 \notin B.$

1.2 Mengenrelationen

Definition 1.9.

Zwei Mengen A und B heißen *gleich*, wenn jedes Element von A auch Element von B ist und jedes Element von B auch Element von A ist. Wir schreiben dann $A = B$.
Gilt dies nicht, so schreibt man $A \neq B$.

Beispiel 1.10.

1) Mit $A = \left\{\frac{1}{n} : n \in \mathbb{N}\right\}$ und $B = \left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\right\}$ gilt $A = B$.

2) $\mathbb{N} \neq \mathbb{Q}$, da $\frac{2}{3} \in \mathbb{Q}$, aber $\frac{2}{3} \notin \mathbb{N}$.

Definition 1.11.

Eine Menge A heißt *Teilmenge* einer Menge B, wenn jedes Element von A auch Element von B ist. Wir schreiben $A \subset B$ oder $A \subseteq B$. Die Menge B heißt in diesem Fall *Obermenge*.

Bemerkung 1.12.

1) Jede Menge ist eine Teilmenge von sich selbst. Jede Menge ist eine Obermenge von sich selbst.

2) Die leere Menge ist eine Teilmenge jeder Menge.

Beispiel 1.13.

1) $\{1, 2, 4\} \subseteq \{1, 2, 3, 4, 5\}$

2) $\mathbb{N} \subseteq \mathbb{R}$

3) $\emptyset \subseteq \{1, 2, 4\}$

Ist A eine Teilmenge von B und gibt es mindestens ein Element von B, das nicht zu A gehört, so heißt A eine *echte Teilmenge* von B. Manchmal wird „$\subset$“ nur für echte Teilmengen verwendet. Manchmal benutzt man für echte Teilmengen das Zeichen „$\subsetneq$“. B heißt dann eine *echte Obermenge* von A.

Beispiel 1.14.

1) $\{1, 2, 3\} \subset \{1, 2, 3, 4, 5\}$ ist eine echte Teilmenge.

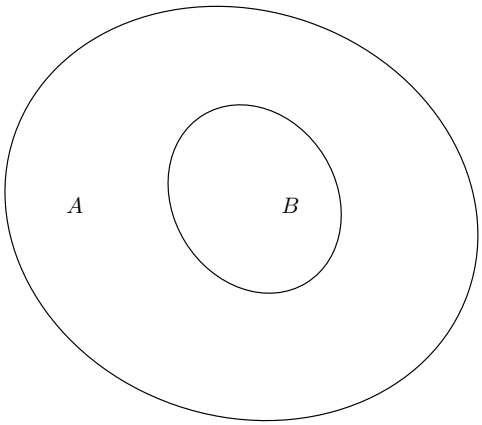

Abbildung 1.1: $B \subseteq A$ dargestellt als Venn-Diagramm.

2) $\{1,2,3\} \subseteq \{1,2,3\}$ ist hingegen keine echte Teilmenge.

Mengen werden oft anhand von *Venn-Diagrammen* wie in Abbildung 1.1 veranschaulicht.

Satz 1.15.

Ist $A \subseteq B$ und $B \subseteq C$, so gilt $A \subseteq C$.

Bemerkung 1.16. Diese Eigenschaft heißt *Transitivität*.

Beweis:
Zu zeigen ist $x \in A \Rightarrow x \in C$. (Mehr zu Implikationen in Kapitel „Logik und Beweise“.)

$$x \in A \ \Rightarrow x \in B \text{ (weil } A \subseteq B),$$
$$x \in B \ \Rightarrow x \in C \text{ (weil } B \subseteq C).$$

Aus $x \in A$ folgt also $x \in C$ und hiermit ist $A \subseteq C$ bewiesen.

□

Bemerkung 1.17. Das Symbol □ wird als Zeichen für das Ende eines Beweises verwendet.

Satz 1.18.

Zwei Mengen A und B sind genau dann gleich, wenn $A \subseteq B$ und $B \subseteq A$.

Beweis:
Die Aussage ist eine Äquivalenz, denn zu zeigen ist

$$(A = B) \Leftrightarrow (A \subseteq B \text{ und } B \subseteq A).$$

(Mehr zu Äquivalenzen in Kapitel „Logik und Beweise“.) In diesem Fall muss man beide Implikationsrichtungen beweisen. Wir beginnen mit der ersten Implikation.
$\Rightarrow$ Zu zeigen: $(A = B) \Rightarrow (A \subseteq B \text{ und } B \subseteq A)$. Dies folgt sofort aus $A \subseteq A$.
$\Leftarrow$ Zu zeigen: $(A \subseteq B \text{ und } B \subseteq A) \Rightarrow (A = B)$. Aus der Definition der Teilmenge folgt, dass $x \in A \Rightarrow x \in B$ und $x \in B \Rightarrow x \in A$. Daraus folgt, dass $x \in A \Leftrightarrow x \in B$, das heißt: x ist genau dann Element von A, wenn x Element von B ist. Das ist die Definition der Relation $A = B$.

□

Um zu zeigen, dass $A = B$, zeigt man oft die beiden Inklusionen $A \subseteq B$ und $B \subseteq A$.

Beispiel 1.19. (Teilbarkeit)

Definition 1.20.

Seien $a, b \in \mathbb{Z}$. a *teilt* b, wenn es ein $n \in \mathbb{Z}$ gibt, sodass $na = b$ gilt. Man sagt auch: a ist ein *Teiler* von b. Wir schreiben dann $a|b$ (gelesen „a teilt b“).

Beispiel 1.21.

1) $3|27$, da $9 \cdot 3 = 27$.

2) $-5|25$, da $(-5) \cdot (-5) = 25$.

3) 1 teilt jede Zahl $a \in \mathbb{Z}$, da $a \cdot 1 = a$.

Definition 1.22.

Eine Zahl $a \in \mathbb{Z}$ heißt *gerade*, wenn $2|a$. Eine Zahl, die nicht gerade ist, heißt *ungerade*.

Aufgabe:
Beweisen Sie: Die Menge aller geraden Zahlen, die durch 3 teilbar sind, und die Menge aller ganzen Zahlen, die durch 6 teilbar sind, sind gleich.
Lösung:
a ist gerade $\Leftrightarrow 2|a$. Wir betrachten also die Mengen $A = \{a \in \mathbb{Z} : 2|a \text{ und } 3|a\}$ und $B = \{a \in \mathbb{Z} : 6|a\}$. Zu zeigen ist demnach $A = B$. Wie angemerkt, genügt es zu zeigen, dass $A \subseteq B$ und $B \subseteq A$.
$A \subseteq B$: Zu zeigen ist also $a \in A \Rightarrow a \in B$. Aus $a \in A$ folgt, dass $2|a$ und $3|a$. Aus $2|a$ folgt, dass es ein $n \in \mathbb{Z}$ gibt mit $a = 2n$, insbesondere also $3|2n$. Wir benutzten den folgenden Fakt: Eine Primzahl p teilt $x \cdot y$ genau dann, wenn p eine der Zahlen x, y teilt. Da nun gelten muss, dass $3|2n$, aber $3 \nmid 2$, folgt es, dass $3|n$. Folglich existiert ein $m \in \mathbb{Z}$ mit $n = 3m$. Dann gilt $a = 2n = 2 \cdot 3m = 6m$, also $6|a$ und somit $a \in B$.
$B \subseteq A$: $a \in B \Rightarrow 6|a \Rightarrow a = 6n$ mit $n \in \mathbb{Z}$. Dann gilt aber $a = 2 \cdot (3n) = 2m$ mit $m = 3n \in \mathbb{Z}$ und auch $a = 3 \cdot (2n) = 3\ell$ mit $\ell = 2n \in \mathbb{Z}$. Also $2|a$ und $3|a \Rightarrow a \in A$.

□

Über Teilbarkeit werden wir in Kapitel „Elementare Zahlentheorie“ genauer reden!

Definition 1.23.

Sei M eine Menge. Die *Potenzmenge* $P(M)$ von M ist die Menge aller Teilmengen von M.

Beispiel 1.24. $M = \{0, 1\}$, $P(M) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.

Bemerkung 1.25. $P(\emptyset) = \{\emptyset\}$ (die Menge, die die leere Menge enthält).

1.3 Mengenoperationen

Definition 1.26.

Seien A und B Mengen.

(i) Die *Vereinigung* $A \cup B$ von A und B besteht aus allen Elementen, die in A oder in B liegen:

$$A \cup B = \{x : x \in A \text{ oder } x \in B\}.$$

(ii) Die *Schnittmenge* (der *Durchschnitt*) von A und B besteht aus allen Elementen, die sowohl in A als auch in B liegen:

$$A \cap B = \{x : x \in A \text{ und } x \in B\}.$$

(iii) Die *Differenzmenge* $A \backslash B$ besteht aus allen Elementen, die in A aber nicht in B liegen:

$$A \backslash B = \{x : x \in A \text{ und } x \notin B\}.$$

-

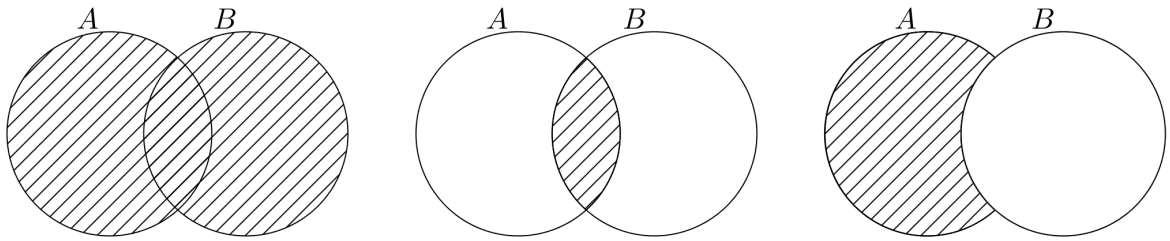

Abbildung 1.2: Von links nach rechts: $A \cup B,\ A \cap B, A \backslash B$.

Beispiel 1.27. Es seien $A = \{1, 2, 3, 6\}$ und $B = \{1, 2, 5, 10\}$. Dann ergeben sich als Vereinigung, Schnitt, sowie Differenz die Mengen

$$A \cup B = \{1, 2, 3, 5, 6, 10\},\ A \cap B = \{1, 2\},\ A \backslash B = \{3, 6\},\ B \backslash A = \{5, 10\}.$$

Definition 1.28.

Die *Komplementmenge* $\overline{A}$ der Menge A bezüglich einer Grundmenge G ist die Menge aller Elemente in G, die nicht zu A gehören:

$$\overline{A} = \{x \in G : x \notin A\}.$$

Weitere Schreibweisen für $\overline{A}$ sind $\complement A,\ A^{\complement},\ A'$.

Bemerkung 1.29. $\overline{A} = G \backslash A$.

Beispiel 1.30.

1) Es sei $G = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Dann sind mit A und B wie oben

$$\overline{A} = \{4, 5, 7, 8, 9, 10\}, \ \overline{B} = \{3, 4, 6, 7, 8, 9\}.$$

2) Mit $G = \mathbb{Z}$ und $C = \{n \in \mathbb{Z} : n \text{ gerade}\}$ folgt $\overline{C} = \{n \in \mathbb{Z} : n \text{ ungerade}\}$.
Betrachtet man aber $G = \mathbb{R}$, so folgt $\overline{C} = \bigcup_{n \in \mathbb{Z}} (2n, 2n + 2)$.

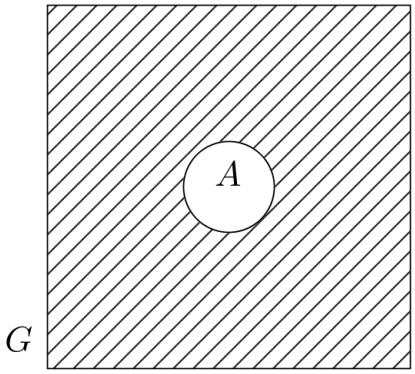

Abbildung 1.3: Komplementmenge $\overline{A}$ mit zugehöriger Grundmenge G.

Definition 1.31.

Die *symmetrische Differenz* der Mengen A und B ist definiert durch die Formel

$$A \triangle B = (A \backslash B) \cup (B \backslash A).$$

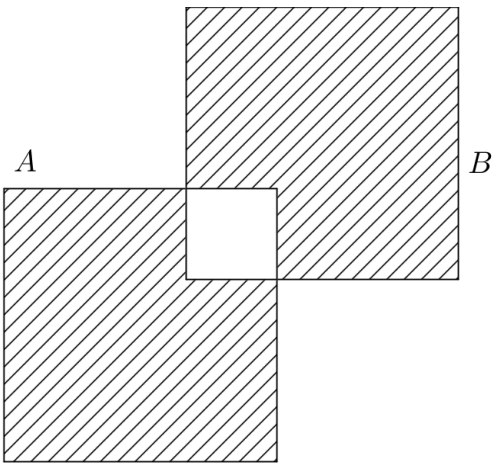

Abbildung 1.4: Symmetrische Differenz $A \triangle B$.

Beispiel 1.32. Unter Wiederbenutzung der obigen Mengen ergibt sich $A \triangle B = \{3, 5, 6, 10\}$.

Wir sehen in der Abbildung, dass die symmetrische Differenz der Mengen A und B die Menge aller Elemente ist, die in A oder in B, aber nicht in den beiden Mengen liegen. Diese Tatsache formulieren wir als Satz.

Satz 1.33.

Es gilt $A \triangle B = (A \cup B) \backslash (A \cap B)$.

Beweis:
Wir nehmen an, dass $x \in A \triangle B$ und nehmen einige elementare Umformungen vor:

$$\begin{aligned} x \in A \triangle B \Leftrightarrow & x \in (A \backslash B) \cup (B \backslash A) \\ \Leftrightarrow & x \in A \backslash B \text{ oder } x \in B \backslash A \\ \Leftrightarrow & (x \in A \text{ und } x \notin B) \text{ oder } (x \in B \text{ und } x \notin A) \\ \Leftrightarrow & (x \in A \text{ oder } x \in B) \text{ und } x \notin A \cap B \\ \Leftrightarrow & x \in A \cup B \text{ und } x \notin A \cap B \\ \Leftrightarrow & x \in (A \cup B) \backslash (A \cap B) \text{ (was zu zeigen war).} \end{aligned}$$

In Kapitel „Logik und Beweise“ werden wir kennenlernen, wie man mit den Verknüpfungen „und“ und „oder“ systematisch arbeitet. Spätestens da wird man in der Lage sein, diesen Beweis komplett nachzuvollziehen.

Alternativ kann man diese Aussage unter Verwendung einer Wahrheitstafel beweisen. In den Spalten der Wahrheitstafel wird der Wahrheitswert jeweiliger Aussage angegeben („w“ für wahr und „f“ für falsch. Die Zeilen entsprechen verschiedenen Fällen.

$x \in A$	$x \in B$	$x \in A \setminus B$	$x \in B \backslash A$	$x \in A \triangle B$	$x \in A \cup B$	$x \in A \cap B$	$x \in (A \cup B) \backslash (A \cap B)$
w	w	f	f	f	w	w	f
w	f	w	f	w	w	f	w
f	w	f	w	w	w	f	w
f	f	f	f	f	f	f	f

Die Spalten für die linke Seite und für die rechte Seite stimmen überein. Das bedeutet, dass die entsprechenden Mengen gleich sind.

□

Die symmetrische Differenz wird nicht oft verwendet.

Eine besondere Rolle spielen **Zahlenmengen:**

1) $\mathbb{N} = \{1, 2, 3, \ldots\}$ bezeichnet die Menge der *natürlichen Zahlen*.
2) $\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\}$ bezeichnet die Menge der natürlichen Zahlen mit Null.
3) $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ bezeichnet die Menge der *ganzen Zahlen*.
4) $\mathbb{Q} = \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N} \right\}$ bezeichnet die Menge der *rationalen Zahlen*.
5) $\mathbb{R}$ bezeichnet die Menge der *reellen Zahlen*. Um diese formal korrekt einzuführen, benötigt man allerdings Analysis.

Notation 1.34.

Um spezielle Teilmengen von $\mathbb{R}$ kompakter schreiben zu können, definieren wir sogenannte *Intervalle*. Seien $a, b \in \mathbb{R}$. Zunächst sprechen wir von *endlichen Intervallen*:

$$\begin{aligned} \text{abgeschlossen } [a,b] &= \{x \in \mathbb{R} : a \leq x \leq b\}, \\ \text{offen } (a,b) &=]a,b[= \{x \in \mathbb{R} : a < x < b\}, \\ \text{halboffen } (a,b] &=]a,b] = \{x \in \mathbb{R} : a < x \leq b\}, \\ [a,b) &= [a,b[= \{x \in \mathbb{R} : a \leq x < b\}. \end{aligned}$$

Nun führen wir *unendliche Intervalle* ein:

$$\begin{aligned} (-\infty, a) &= \{x \in \mathbb{R} : x < a\}, \\ (-\infty, a] &= \{x \in \mathbb{R} : x \leq a\}, \\ (a, \infty) &= \{x \in \mathbb{R} : x > a\}, \\ [a, \infty) &= \{x \in \mathbb{R} : x \geq a\}, \\ (-\infty, \infty) &= \mathbb{R}. \end{aligned}$$

Dabei sind die Zeichen „$(-\infty$“ und „$\infty)$“ als Symbole zu verstehen.

Beispiel 1.35. (Mengenoperationen für Zahlenmengen)

1) $(2,4) \cup (3,7) = (2,7)$
2) $(2,4) \backslash (3,7) = (2,3]$
3) $(2,4) \cap (3,7) = (3,4)$
4) $\overline{(2,4)} = (-\infty, 2] \cup [4, \infty)$
5) $(3,7) \cap \mathbb{N} = \{4,5,6\}$
6) $\mathbb{Z} \backslash [2,4] = \{\ldots, -2, -1, 0, 1, 5, 6, 7, \ldots\}$
7) $\mathbb{R} \backslash [-2, \infty) = (-\infty, -2)$
8) $(-\infty, 1] \cup [0, \infty) = \mathbb{R}$
9) $(-\infty, 1) \triangle [0, \infty) = (-\infty, 0) \cup (1, \infty)$

Nun beschäftigen wir uns mit Rechenregeln für Mengenoperationen.

Satz 1.36. *Rechenregeln für Mengenoperationen*

Seien A, B und C Mengen in einer Grundmenge G. Die mengentheoretischen Operationen $\cup, \cap$ und $\complement$ erfüllen die folgenden Rechengesetze:

- Kommutativität: $A \cup B = B \cup A,\ A \cap B = B \cap A$.
- Assoziativität: $A \cup (B \cup C) = (A \cup B) \cup B,\ A \cap (B \cap C) = (A \cap B) \cap C$.
- Distributivität: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C),\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
- Verschmelzungsgesetze: $A \cup (B \cap A) = A,\ A \cap (B \cup A) = A$.
- Idempotenzgesetze: $A \cup A = A,\ A \cap A = A$.
- Neutralität: $A \cup \emptyset = A,\ A \cap G = A$.
- Absorption: $A \cup G = G,\ A \cap \emptyset = \emptyset$.
- Komplementarität: $A \cup \overline{A} = G,\ A \cap \overline{A} = \emptyset$.
- Dualität: $\overline{\emptyset} = G,\ \overline{G} = \emptyset$.
- Gesetze von De Morgan: $\overline{A \cup B} = \overline{A} \cap \overline{B},\ \overline{A \cap B} = \overline{A} \cup \overline{B}$.

Bemerkung 1.37. Die Mengen in einer Grundmenge G bilden mit den Operationen $\cup, \cap$ und $\complement$ eine Struktur, welche „Boolesche Algebra“ heißt.

Bemerkung 1.38. Die Gesetze, die das Komplement enthalten, können für Differenzen umgeschrieben werden.

Beweis:
Die Beweise erfolgen exemplarisch, weitere Beispiele folgen in den Übungen.

1) Wir zeigen zunächst $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. Sei dazu $x \in A \cup (B \cap C)$

$$
\begin{aligned}
&\Leftrightarrow x \in A \text{ oder } (x \in B \cap C)\\
&\Leftrightarrow x \in A \text{ oder } (x \in B \text{ und } x \in C)\\
&\Leftrightarrow (x \in A \text{ oder } x \in B) \text{ und } (x \in A \text{ oder } x \in C)\\
&\Leftrightarrow x \in A \cup B \text{ und } x \in A \cup C\\
&\Leftrightarrow x \in (A \cup B) \cap (A \cup C).
\end{aligned}
$$

Zum tieferen Verständnis gehen wir nun der Frage nach, wie man die Äquivalenz $x \in A$ oder $(x \in B$ und $x \in C) \Leftrightarrow (x \in A$ oder $x \in B)$ und $(x \in A$ oder $x \in C)$ begründen kann, ohne die Rechenregeln für „und“ und „oder“ zu benutzen.
$\Rightarrow$ Zu zeigen: $x \in A$ oder $(x \in B$ und $x \in C) \Rightarrow (x \in A$ oder $x \in B)$ und $(x \in A$ oder $x \in C)$.

1. Fall: $x \in A$

$x \in A$ oder $x \in B$	w
$x \in A$ oder $x \in C$	w
$(x \in A$ oder $x \in B)$ und $(x \in A$ oder $x \in C)$	w

2. Fall: $x \in B$ und $x \in C$

$x \in A$ oder $x \in B$	w
$x \in A$ oder $x \in C$	w
$(x \in A$ oder $x \in B)$ und $(x \in A$ oder $x \in C)$	w

$\Leftarrow$ Zu zeigen ($x \in A$ oder $x \in B$) und ($x \in A$ oder $x \in C$) $\Rightarrow x \in A$ oder ($x \in B$ und $x \in C$).

1. Fall: $x \in A \Rightarrow x \in A$ oder ($x \in B$ und $x \in C$) ist wahr, da die vordere Bedingung aufgrund $x \in A$ immer erfüllt ist.
2. Fall: $x \in B$ und $x \in A \Rightarrow x \in A$ oder ($x \in B$ und $x \in C$) ist wahr, da auch hier $x \in A$.
3. Fall: $x \in B$ und $x \in C \Rightarrow x \in A$ oder ($x \in B$ und $x \in C$) ist wahr, da die zweite Bedingung sicher erfüllt ist.

2) Im folgenden Schritt zeigen wir $A \cap (B \cup A) = A$. Wir wählen also $x \in A \cap (B \cup A)$

$$\begin{aligned}
&\Leftrightarrow x \in A \text{ und } x \in B \cup A \\
&\Leftrightarrow x \in A \text{ und } (x \in B \text{ oder } x \in A) \\
&\Leftrightarrow (x \in A \text{ und } x \in B) \text{ oder } x \in A \\
&\Leftrightarrow x \in A.
\end{aligned}$$

3) Zu zeigen: $A \cup \overline{A} = G$. Wähle also $x \in A \cup \overline{A}$

$$\begin{aligned}
&\Leftrightarrow x \in A \text{ oder } x \in \overline{A} \\
&\Leftrightarrow x \in A \text{ oder } x \notin A,
\end{aligned}$$

was für alle x erfüllt ist. Also $x \in G$.

4) Zu zeigen: $\overline{(\overline{A})} = A$.

$$x \in \overline{(\overline{A})} \Leftrightarrow x \notin \overline{A} = \{y : y \notin A\} \Leftrightarrow x \in A.$$

5) Zu zeigen: $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

$$\begin{aligned}
x \in \overline{A \cup B} &\Leftrightarrow x \notin A \cup B = \{y : y \in A \text{ oder } y \in B\} \\
&\Leftrightarrow x \notin A \text{ und } x \notin B \Leftrightarrow x \in \overline{A} \cap \overline{B}.
\end{aligned}$$

□

Aufgabe:
Prüfen Sie anhand von Venn-Diagrammen, ob nachfolgende Mengenidentitäten stimmen. Wenn eine Mengenidentität richtig ist, beweisen Sie diese. Sollte sie falsch sein, geben Sie ein Gegenbeispiel an.

1) Behauptet wird, dass $(A \backslash B) \cup (A \backslash C) \subset A$. Diese Formel ist korrekt. Sei also $x \in (A \backslash B) \cup (A \backslash C)$

$$\begin{aligned}
&\Rightarrow x \in A \backslash B \text{ oder } x \in A \backslash C \\
&\Rightarrow x \in A \backslash B \text{ oder } x \in A \backslash C \\
&\Rightarrow (x \in A \text{ und } x \notin B) \text{ oder } (x \in A \text{ und } x \notin C) \\
&\Rightarrow x \in A.
\end{aligned}$$

2) Weiter betrachten wir die Behauptung $(A \backslash B) \cup (A \backslash C) = A$. Abbildung 1.5 zeigt eine Situation, in der diese Identität gilt. Aber Vorsicht: Die Mengen in Abbildung 1.5 sind nicht in allgemeiner Lage, die Mengen B und C schneiden sich nicht! Abbildung 1.6 zeigt, dass die Identität im allgemeinen Fall falsch ist. Wir konstruieren darauf aufbauend ein Gegenbeispiel, da die Behauptung insbesondere nicht stimmt, insofern $B \cap C \neq \emptyset$. Wir wählen also dementsprechend unsere Mengen.

$$\begin{aligned}
A = \{1,2,3,4,5\},\ B = \{2,3\},\ C = &\{3,4\},\ A \backslash B = \{1,4,5\},\ A \backslash C = \{1,2,5\} \\
\Rightarrow (A \backslash B) \cup (A \backslash C) = &\{1,2,4,5\} \neq A.
\end{aligned}$$

Wie korrigiert man die Formel, damit sie stimmt? Wir vermuten, dass $(A\backslash B)\cup(A\backslash C) = A\backslash(B\cap C)$ gilt und versuchen diese Vermutung zu beweisen. Sei also $x \in (A\backslash B) \cup (A\backslash C)$

$$\begin{aligned}
&\Leftrightarrow x \in A\backslash B \text{ oder } x \in A\backslash C\\
&\Leftrightarrow (x \in A \text{ und } x \notin B) \text{ oder } (x \in A \text{ und } x \notin C)\\
&\Leftrightarrow x \in A \text{ und } (x \notin B \text{ oder } x \notin C)\\
&\Leftrightarrow x \in A \text{ und } (x \notin B \cap C = \{y : y \in B \text{ und } y \in C\})\\
&\Leftrightarrow x \in A \text{ und } x \notin B \cap C\\
&\Leftrightarrow x \in A\backslash(B \cap C).
\end{aligned}$$

3) Zuletzt betrachten wir $M\cup N = (M\backslash N)\cup(M\cap N)\cup(N\backslash M)$ und beweisen diese Identität mittels Wahrheitstafel. Sei dazu $A := M\backslash N,\ B := x \in M \cap N,\ C := N\backslash M$.

$x \in M$	$x \in N$	$x \in M \cup N$	$x \in M\backslash N$	$x \in M \cap N$	$x \in N\backslash M$	$x \in A \cup B \cup C$
w	w	w	f	w	f	w
w	f	w	w	f	f	w
f	w	w	f	f	w	w
f	f	f	f	f	f	f

Also insgesamt $x \in M \cup N \Leftrightarrow x \in (M\backslash N) \cup (M \cap N) \cup (N\backslash M)$.

□

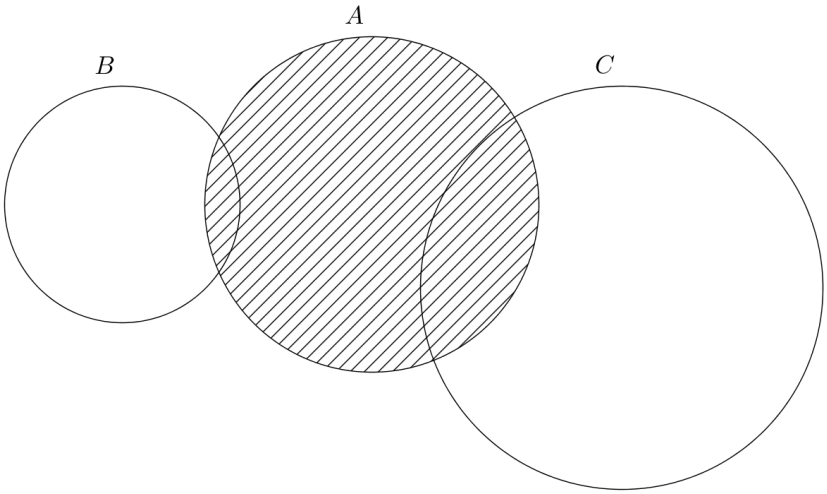

Abbildung 1.5: $(A\backslash B) \cup (A\backslash C) = A$, wenn $B \cap C = \emptyset$.

Definition 1.39.

Zwei Mengen A und B heißen *disjunkt* (*elementfremd*), wenn $A \cap B = \emptyset$.

Definition 1.40.

Eine Familie $\{A_1, \ldots, A_n\}$ der Teilmengen einer Menge M heißt *Partition*, wenn

1) $A_1 \cup A_2 \cup \ldots \cup A_n = M$ und

2) $A_i \cap A_j = \emptyset,\ i \neq j$.

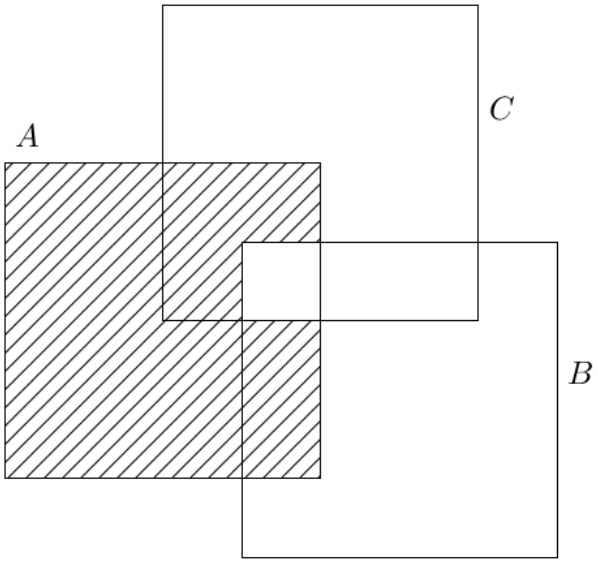

Abbildung 1.6: $(A \backslash B) \cup (A \backslash C) \neq A$ für Mengen in allgemeiner Lage.

Beispiel 1.41.

1. Es sei $M = \{1, 2, 3, 4, 5\}$. Dann ist $\{\{1, 2\}, \{3\}, \{4, 5\}\}$ eine Partition.
2. $\{M \backslash N, M \cap N, N \backslash M\}$ ist eine Partition von $M \cup N$. Denn es folgt aus der Wahrheitstafel, dass die Mengen $M \backslash N, M \cap N$ und $N \backslash M$ paarweise elementfremd sind.

1.4 Kartesisches Produkt zweier Mengen

Gegeben seien zwei Mengen A und B. Die Paare der Form (a, b) mit $a \in A$ und $b \in B$ heißen *geordnete Paare*. An erster Stelle steht ein Element von A, an der zweiten ein Element von B. Zwei geordnete Paare (a, b) und (a', b') sind gleich, wenn $a = a'$ und $b = b'$.

Definition 1.42.

Das *kartesische Produkt* zweier Mengen A und B ist die Menge aller geordneten Paare (a, b) mit $a \in A$ und $b \in B$:

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

Bemerkung 1.43. Im Allgemeinen gilt $A \times B \neq B \times A$.

Beispiel 1.44.

1) Sei $A = \{1\},\ B = \{2\}$. Dann ist $A \times B = \{(1,2)\}$ und $B \times A = \{(2,1)\}$.

2) Sei $A = \{1,2,3\},\ B = \{2,4\}$. Dann ist
$$A \times B = \{(1,2),(1,4),(2,2),(2,4),(3,2),(3,4)\}.$$

3) $[0,1] \times [0,1]$ ist das Quadrat $\{(x,y) : 0 \leq x \leq 1 \text{ und } 0 \leq y \leq 1\}$.

4) $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ ist die Ebene.

Sind A und B Zahlenmengen, kann man das kartesische Produkt $A \times B$ auf der Ebene veranschaulichen.

1.5 Kardinalität einer endlichen Menge

Definition 1.45.

Sei M eine endliche Menge. Die Anzahl der Elemente in M heißt die *Kardinalität* (*Mächtigkeit*) der Menge M. Schreibweise: $|M|$ oder $\#M$.
Insbesondere hat die leere Menge die Kardinalität Null: $|\emptyset| = 0$.

Beispiel 1.46. $A = \{1,2,3,4,5\},\ |A| = 5$.
$B =$die Menge der Buchstaben des Wortes „Vorkurs“. $B = \{v,o,r,k,u,s\},\ |B| = 6$.

Lemma 1.47.

Sind A und B disjunkt, also $A \cap B = \emptyset$, so gilt
$$|A \cup B| = |A| + |B|.$$

Beweis:
Es bestehe A aus n Elementen und B bestehe aus m Elementen:
$$|A| = n,\ |B| = m.$$
Da nun nach Annahme A und B keine gemeinsamen Elemente haben, folgt es, dass $A \cup B$ aus genau $n + m$ Elementen besteht:
$$|A + B| = n + m.$$
□

Satz 1.48.

Seien A und B Mengen, dann gilt

(i) $|A \backslash B| = |A| - |A \cap B|$,

(ii) $|A \cup B| = |A| + |B| - |A \cap B|$.

Beweis:
Wir beweisen die beiden Aussagen in zwei separaten Teilen.

(i) Betrachten wir zunächst die erste Behauptung und schreiben $A \backslash B = \{x : x \in A \text{ und } x \notin B\} = \{x : x \in A \text{ und } x \notin A \cap B\}$. Seien $|A| = n$ und $|A \cap B| = m$, also haben A und B genau m gemeinsame Elemente. Dann besteht $A \backslash B = \{x : x \in A \text{ und } x \notin A \cap B\}$ aus genau $n - m$ Elementen, also
$$|A \backslash B| = n - m = |A| - |A \cap B|.$$

(ii) Wie wir in einer Aufgabe oben gesehen haben, gilt $A \cup B = (A \backslash B) \cup (A \cap B) \cup (B \backslash A)$. Darüber hinaus sind diese Mengen disjunkt. Nach (i) gelten die Gleichungen

$$|A \backslash B| = |A| - |A \cap B| \text{ und } |B \backslash A| = |B| - |A \cap B|.$$

Mit dem Lemma folgt dann, dass

$$\begin{aligned} |A \cup B| =& |A \backslash B| + |A \cap B| + |B \backslash A| \\ =& |A| - |A \cap B| + |A \cap B| + |B| - |A \cap B| \\ =& |A| + |B| - |A \cap B|. \end{aligned}$$

□

Kapitel 2

Logik und Beweise

2.1 Aussagen und logische Operatoren

Definition 2.1.

Eine *Aussage* ist ein sprachliches Gebilde, das aufgrund seines Inhaltes entweder wahr oder falsch ist.

Beispiel 2.2. Beispiele für Aussagen sind exemplarisch:

1) $-7 > 5$.

2) Es gibt unendlich viele Primzahlen.

Keine Aussagen sind hingegen:

1) Wer geht heute in die Cafeteria?

2) $2 + 2$.

3) Frohe Ostern!

Logische Operationen sind Verknüpfungen von Aussagen. Diese werden mithilfe von Wahrheitstafeln definiert.

Definition 2.3.

Seien A und B zwei Aussagen.

(i) Die *Negation* ordnet der Aussage A ihr logisches Gegenteil zu. Wir schreiben $\overline{A}$ oder $\neg A$. Formal ist sie durch die folgende Wahrheitstafel definiert:

A	$\neg A$
w	f
f	w

(ii) Die Verknüpfung von Aussagen mit der *Und-Verknüpfung* (*Konjunktion*) ist genau dann wahr, wenn beide damit verknüpften Aussagen wahr sind. Das zugehörige Symbol ist $\wedge$. Formal ist sie durch die folgende Wahrheitstafel definiert:

A	B	$A \wedge B$
w	w	w
w	f	f
f	w	f
f	f	f

(iii) Die Verknüpfung von Aussagen mit der *Oder-Verknüpfung* (*Disjunktion*) ist genau dann wahr, wenn mindestens eine der Aussagen wahr ist. Wir nutzen hier als Symbol $\vee$. Formal ist sie durch die folgende Wahrheitstafel definiert:

A	B	$A \vee B$
w	w	w
w	f	w
f	w	w
f	f	f

Beispiel 2.4.

1) A: Gießen liegt an der Lahn.
$\neg A$: Gießen liegt nicht an der Lahn.

2) $B : 2 + 2 = 5$.
$\neg B : 2 + 2 \neq 5$.

3) C: Alle Vögel könne fliegen.
$\neg C$: Es gibt Vögel, die nicht fliegen können.

4) $M : 3$ ist ungerade, $N : 3$ ist eine Primzahl, $P : 4$ ist gerade, $Q : 4$ ist eine Primzahl.
$M \wedge N : 3$ ist ungerade und eine Primzahl. (w)
$M \vee N : 3$ ist ungerade oder eine Primzahl. (w)
$P \wedge Q : 4$ ist gerade und eine Primzahl. (f)
$P \vee Q : 4$ ist gerade oder eine Primzahl. (w)

Bemerkung 2.5. Die Oder-Verknüpfung $\vee$ ist ein einschließendes Oder: $A \vee B$ bedeutet A oder B oder beides.

Satz 2.6. *Rechenregeln für logische Operationen*

Seien a, b, c drei Aussagen. Für die logischen Operationen $\wedge, \vee$ und $\neg$ gelten die folgenden Rechenregeln:

- Kommutativität: $a \vee b = b \vee a,\ a \wedge b = b \wedge a.$
- Assoziativität: $a \vee (b \vee c) = (a \vee b) \vee c,\ a \wedge (b \wedge c) = (a \wedge b) \wedge c.$
- Distributivität: $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c),\ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$
- Verschmelzungsgesetze: $a \vee (b \wedge a) = a,\ a \wedge (b \vee a) = a.$
- Idempotenzgesetze: $a \vee a = a,\ a \wedge a = a.$
- Neutralität: $a \vee \mathrm{f} = a,\ a \wedge \mathrm{w} = a.$
- Absorption: $a \vee \mathrm{w} = \mathrm{w},\ a \wedge \mathrm{f} = \mathrm{f}.$
- Komplementarität: $a \vee \neg a = \mathrm{w},\ a \wedge \neg a = \mathrm{f}.$
- Dualität: $\neg \mathrm{f} = \mathrm{w},\ \neg \mathrm{w} = \mathrm{f}.$
- Doppelnegationsgesetz: $\neg(\neg a) = a.$
- Gesetze von De Morgan: $\neg(a \vee b) = \neg a \wedge \neg b,\ \neg(a \wedge b) = \neg a \vee \neg b.$

Bemerkung 2.7. Die Gesetze für Aussagen mit den Operationen $\wedge, \vee$ und $\neg$ sind genau die gleichen wie für Mengen mit den Operationen $\cap, \cup$ und $\complement$. Dabei entspricht Und der Schnittmenge, Oder der Vereinigung und Negation dem Komplement.

Beweis:
Exemplarisch folgen einige Beweise zu den obigen Aussagen. Die Beweise erfolgen mithilfe von Wahrheitstafeln. Weitere Beispiele folgen in den Übungen.

1) Wir wollen zeigen: $a \vee b = b \vee a$. Stimmen die jeweiligen Spalten überein, gilt Gleichheit.

a	b	$a \vee b$	$b \vee a$
w	w	w	w
w	f	w	w
f	w	w	w
f	f	f	f

2) Zu zeigen: $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

a	b	c	$b \wedge c$	$a \wedge (b \wedge c)$	$a \wedge b$	$(a \wedge b) \wedge c$
w	w	w	w	w	w	w
w	w	f	f	f	w	f
w	f	w	f	f	f	f
w	f	f	f	f	f	f
f	w	w	w	f	f	f
f	w	f	f	f	f	f
f	f	w	f	f	f	f
f	f	f	f	f	f	f

3) Zu zeigen: $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee b)$.

a	b	c	$b \wedge c$	$a \vee (b \wedge c)$	$a \vee b$	$a \vee c$	$(a \vee b) \wedge (a \vee c)$
w	w	w	w	w	w	w	w
w	w	f	f	w	w	w	w
w	f	w	f	w	w	w	w
w	f	f	f	w	w	w	w
f	w	w	w	w	w	w	w
f	w	f	f	f	w	f	f
f	f	w	f	f	f	w	f
f	f	f	f	f	f	f	f

4) Zu zeigen: $\neg(\neg a) = a$.

a	$\neg a$	$\neg(\neg a)$
w	f	w
f	w	f

5) Zu zeigen: $\neg(a \vee b) = \neg a \wedge \neg b$.

a	b	$a \vee b$	$\neg(a \wedge b)$	$\neg a$	$\neg b$	$\neg a \wedge \neg b$
w	w	w	f	f	f	f
w	f	w	f	f	w	f
f	w	w	f	w	f	f
f	f	f	w	w	w	w

□

Die Gesetze von De Morgan helfen, Negationen von Und- und Oder-Verknüpfungen zu bilden.

Beispiel 2.8.

1) A: „Abends gehe ich in eine Pizzeria oder in einen Dönerladen.“ Setze $A = A_1 \vee A_2$ mit:
A_1: „Ich gehe in eine Pizzeria“ und
A_2: „Ich gehe in einen Dönerladen“. Dann ist
$\neg A = \neg A_1 \wedge \neg A_2$: „Abends gehe ich weder in eine Pizzeria noch in einen Dönerladen.“

2) B: „Ich kaufe ein belegtes Brötchen und ein Getränk.“ $B = B_1 \wedge B_2$ mit:
B_1: „Ich kaufe ein belegtes Brötchen“ und
B_2: „Ich kaufe ein Getränk“.
$\neg B = \neg B_1 \vee \neg B_2$: „Ich kaufe kein belegtes Brötchen oder kein Getränk.“

3) C: „Sie kennt mich nicht oder sie hat mich vergessen.“ $C = C_1 \vee C_2$ mit:
C_1: „Sie kennt mich nicht“ und
C_2: „Sie hat mich vergessen“.
$\neg C = \neg C_1 \wedge \neg C_2$: „Sie kennt mich und hat mich nicht vergessen.“

Definition 2.9.

Eine *Boolesche Algebra* (oder ein *Boolescher Verband*) ist eine nichtleere Menge B mit drei Verknüpfungen $\wedge, \vee$ und $\neg$ sowie zwei neutralen Elementen $0, 1 \in B$, sodass folgende Rechengesetze gelten: 1) Kommutativität, 2) Distributivität, 3) Neutralitätsgesetze, 4) Komplementaritätsgesetze.

Bemerkung 2.10. Alle anderen Rechengesetze lassen sich aus den oben genannten Gesetzen herleiten.

Beispiel 2.11. Beispiele der Booleschen Algebren sind

1) Aussagen mit den Operationen $\wedge, \vee$ und $\neg$, $0 = \text{f}$, $1 = \text{w}$.

2) Teilmengen einer Grundmenge G mit den Operationen $\cap, \cup$ und $\complement$, $0 = \emptyset$, $1 = G$.

Es gibt auch weitere Beispiele, auf die wir hier allerdings nicht näher eingehen.

Definition 2.12.

- Eine Aussage, die notwendigerweise wahr ist, unabhängig von den Wahrheitswerten anderer Aussagen, nennt man *Tautologie*.
- Eine Aussage, die notwendigerweise falsch ist, unabhängig von den Wahrheitswerten anderer Aussagen, nennt man *Widerspruch* (*Kontradiktion*).

Beispiel 2.13. Zu Tautologien: $\neg a \vee a$.

1) Es regnet oder es regnet nicht.

2) Eine reelle Zahl x ist positiv oder negativ oder gleich Null.

Zu Widersprüchen: $a \wedge \neg a$.

1) Eine ganze Zahl x ist gerade und ungerade.

2) In der Geldbörse sind weniger als zehn, aber mehr als 30 Euro.

Bemerkung 2.14. Zum Zuweisen von Mengenidentitäten: Beim Beweis der Mengenidentitäten haben wir Und- und Oder-Verknüpfungen bearbeitet. Dies erfolgt mit den Rechenregeln für logische Operationen. Wir wiederholen hier einige Beweise aus dem vorherigen Kapitel, wobei wir die o.g. Rechenregeln formal anwenden. Übersichtlichkeitshalber verwenden wir hier die Wörter „und “ und „oder “ statt die Symbole „$\wedge$“ und „$\vee$“.

Beispiel 2.15.

1) Zu zeigen: $A \triangle B = (A \cup B) \backslash (A \cap B)$. Sei $x \in A \triangle B$

$\Leftrightarrow x \in (A \backslash B) \cup (B \backslash A)$
$\Leftrightarrow x \in A \backslash B$ oder $x \in B \backslash A$
$\Leftrightarrow (x \in A$ und $x \notin B)$ oder $(x \in B$ und $x \notin A)$
$\Leftrightarrow (x \in A$ oder $(x \in B$ und $x \notin A))$ und $(x \notin B$ oder $(x \in B$ und $x \notin A))$
$\Leftrightarrow (x \in A$ oder $x \in B)$ und $(x \in A$ oder $x \notin A)$ und $(x \notin B$ oder $x \in B)$ und $(x \notin B$ oder $x \notin A)$
$\Leftrightarrow (x \in A$ oder $x \in B)$ und w und w und $(x \notin A$ oder $x \notin B)$
$\Leftrightarrow x \in A \cup B$ und $(\neg(x \in A)$ oder $\neg(x \in B))$
$\Leftrightarrow x \in A \cup B$ und $\neg(x \in A$ und $x \in B)$
$\Leftrightarrow x \in A \cup B$ und $\neg(x \in A \cap B)$
$\Leftrightarrow x \in A \cup B$ und $x \notin A \cap B$
$\Leftrightarrow x \in (A \cup B) \backslash (A \cap B)$.

2) Zu zeigen: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. Sei also $x \in A \cup (B \cap C)$

$\Leftrightarrow x \in A$ oder $x \in B \cap C$
$\Leftrightarrow x \in A$ oder $(x \in B$ und $x \in C)$
$\Leftrightarrow (x \in A$ oder $x \in B)$ und $(x \in A$ oder $x \in C)$
$\Leftrightarrow x \in A \cup B$ und $x \in A \cup C$
$\Leftrightarrow x \in (A \cup B) \cap (A \cup C)$.

3) Zu zeigen: $\overline{A \cup B} = \overline{A} \cap \overline{B}$. Sei also $x \in \overline{A \cup B}$

$$\begin{aligned}
&\Leftrightarrow x \notin A \cup B \\
&\Leftrightarrow \neg(x \in A \cup B) \\
&\Leftrightarrow \neg(x \in A \text{ oder } x \in B) \\
&\Leftrightarrow \neg(x \in A) \text{ und } \neg(x \in B) \\
&\Leftrightarrow x \in \overline{A} \text{ und } x \in \overline{B} \\
&\Leftrightarrow x \in \overline{A} \cap \overline{B}.
\end{aligned}$$

4) Zu zeigen: $M \cup N = (M \backslash N) \cup (M \cap N) \cup (N \backslash M)$. Sei also $x \in (M \backslash N) \cup (M \cap N) \cup (N \backslash M)$

$$\begin{aligned}
&\Leftrightarrow x \in M \backslash N \text{ oder } x \in M \cap N \text{ oder } x \in N \backslash M \\
&\Leftrightarrow (x \in M \text{ und } x \in \overline{N}) \text{ oder } (x \in M \text{ und } x \in N) \text{ oder } (x \in N \text{ und } x \in \overline{M}).
\end{aligned}$$

An dieser Stelle wenden wir nun die elementaren Rechengesetze der Aussagenlogik an und schreiben

$$\begin{aligned}
&(a \wedge b) \vee (c \wedge d) \vee (g \wedge h) \\
=&[a \vee (c \wedge d) \vee (g \wedge h)] \wedge [b \vee (c \wedge d) \vee (g \wedge h)] \\
=&[a \vee c \vee (g \wedge h)] \wedge [a \vee d \vee (g \wedge h)] \wedge [b \vee c \vee (g \wedge h)] \wedge [b \vee d \vee (g \wedge h)] \\
=&[a \vee c \vee g] \wedge [a \vee c \vee h] \wedge [a \vee d \vee g] \wedge [a \vee d \vee h] \wedge [b \vee c \vee g] \wedge [b \vee c \vee h] \wedge [b \vee d \vee g] \\
&\wedge [b \vee d \vee h]
\end{aligned}$$

Und damit folglich

$$\begin{aligned}
\ldots \Leftrightarrow &(x \in M \text{oder } x \in M \text{ oder } x \in N) \text{ und } (x \in M \text{ oder } x \in M \text{ oder } x \in \overline{M}) \text{ und} \\
&(x \in M \text{ oder } x \in N \text{ oder } x \in N) \text{ und } (x \in M \text{ oder } x \in N \text{ oder } x \in \overline{M}) \text{ und} \\
&(x \in \overline{N} \text{ oder } x \in M \text{ oder } x \in N) \text{ und } (x \in \overline{N} \text{ oder } x \in M \text{ oder } x \in \overline{M}) \text{ und} \\
&(x \in \overline{N} \text{ oder } x \in N \text{ oder } x \in N) \text{ und } (x \in \overline{N} \text{ oder } x \in N \text{ oder } x \in \overline{M}) \\
\Leftrightarrow &x \in M \cup N \text{ und w und } x \in M \cup N \text{ und w und w und w und w und w} \\
\Leftrightarrow &x \in M \cup N.
\end{aligned}$$

2.2 Implikation und Äquivalenz

Definition 2.16.

Seien A, B zwei Aussagen. Die *Implikation* $A \Rightarrow B$ ist definiert durch die Wahrheitstafel:

A	B	$A \Rightarrow B$
w	w	w
w	f	f
f	w	w
f	f	w

Sprechweise: „aus A folgt B“, „A impliziert B“, „wenn A gilt, dann gilt B“.

Bemerkung 2.17. Wenn A wahr ist, dann ist die Implikation $A \Rightarrow B$ genau dann wahr, wenn B wahr ist. Wenn A falsch ist, ist die Implikation $A \Rightarrow B$ immer wahr (aus Falschem folgt alles).

Da die obere Definition im Fall, wenn A falsch ist, intuitiv nicht so klar ist, wollen wir den Sachverhalt anhand eines Beispiels illustrieren.

Beispiel 2.18. Es sei $A : x > 0$ und $B : 2x + 1 > 0$. Dann ist intuitiv klar, dass $A \Rightarrow B$ gilt. Wie erklären wir nun an diesem Beispiel die Definition durch die Wahrheitstafel?

1) Es seien A und B wahr. Also muss gelten: Wenn A wahr ist, dann ist auch B wahr, also $x > 0$ impliziert $2x > 0$ impliziert $2x + 1 > 0$. Die Implikation $A \Rightarrow B$ ist also gefühlt wahr.

2) Der Fall A wahr, B falsch kommt nicht vor. Sonst wäre die Implikation $A \Rightarrow B$ im Allgemeinen falsch.

3) Es sei A falsch, aber B wahr. Dies ist exemplarisch für $x = -\frac{1}{4}$ erfüllt. Hier ist $x < 0$, aber $2x + 1 = -\frac{1}{2} + 1 = \frac{1}{2} > 0$. Das stört die Implikation $A \Rightarrow B$ gefühlt nicht.

4) Sind A und B falsch, wie zum Beispiel für $x = -1$, denn hier ist $x < 0$ und $2x + 1 = -2 + 1 = -1 < 0$, so stört auch dies die Implikation $A \Rightarrow B$ gefühlt nicht.

Betrachten wir nun eine falsche Implikation: $(x^2 > 0 \Rightarrow x > 0)$. Hier lautet die Aussage $A : x^2 > 0$ und die Aussage $B : x > 0$. A ist aber beispielsweise für $x = -1$ wahr, während B für $x = -1$ falsch ist. Somit ist auch die Implikation $A \Rightarrow B$ falsch.

Bemerkung 2.19. Um zu beweisen, dass eine Implikation $A \Rightarrow B$ wahr ist, genügt es, anzunehmen, dass A wahr ist und dann zu zeigen, dass auch B wahr ist. Den Fall, wenn A falsch ist, braucht man nicht zu betrachten.

Beispiel 2.20. Wir wollen nun exemplarisch eine Implikation beweisen. Die Behauptung lautet:

$$a, b \text{ sind beide ungerade } \Rightarrow a + b \text{ ist gerade.}$$

Wir beweisen dies, indem wir annehmen, dass a, b ungerade Zahlen sind.

$$\begin{aligned}
&a, b \text{ sind beide ungerade} \\
\Rightarrow\ &\text{es gibt } n, m \in \mathbb{Z} \text{ derart, dass } a = 2n + 1,\ b = 2m + 1 \\
\Rightarrow\ &a + b = (2n + 1) + (2m + 1) = 2n + 2m + 2 = 2(n + m + 1) = 2\ell \text{ mit } n + m + 1 = \ell \in \mathbb{Z} \\
\Rightarrow\ &a + b \text{ ist gerade.}
\end{aligned}$$

Bemerkung 2.21. Um zu zeigen, dass eine Implikation $A \Rightarrow B$ falsch ist, reicht es, ein *Gegenbeispiel* anzugeben. Das heißt, dass wir ein Beispiel konstruieren müssen, in welchem A wahr und B falsch ist.

Beispiel 2.22. Wir widerlegen nun eine Implikation durch ein Gegenbeispiel. Die Behauptung lautet hier: $x > 0 \Rightarrow 100x - 1 > 0$. Für das Gegenbeispiel wählen wir $x = \frac{1}{200}$. Dann ist $x > 0$ erfüllt, aber $100x - 1 = 100 \cdot \frac{1}{200} - 1 = -\frac{1}{2}$ und $-\frac{1}{2} > 0$ ist falsch. Somit ist auch die Implikation falsch.

Definition 2.23.

Seien A und B zwei Aussagen. Die *Äquivalenz* $A \Leftrightarrow B$ ist definiert durch die Wahrheitstafel:

A	B	$A \Rightarrow B$
w	w	w
w	f	f
f	w	f
f	f	w

Sprechweise: „A und B sind äquivalent“, „A ist genau dann wahr, wenn B wahr ist“.

Beispiel 2.24.

1) Für $n \in \mathbb{N}$ gilt: n ist gerade $\Leftrightarrow n^2$ ist gerade.

2) Für $x \in \mathbb{R}$ gilt: $2x + 1 > 0 \Leftrightarrow x > -\frac{1}{2}$.

Satz 2.25.

$[A \Leftrightarrow B] = [(A \Rightarrow B) \wedge (B \Rightarrow A)]$.

Beweis:
Der Beweis erfolgt mittels Wahrheitstafel:

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$	$A \Leftrightarrow B$
w	w	w	w	w	w
w	f	f	w	f	f
f	w	w	f	f	f
f	f	w	w	w	w

□

Satz 2.26.

Die Implikation und die Äquivalenz kann man wie folgt umformulieren:

(i) $(A \Rightarrow B) = (\neg A \vee B)$

(ii) $(A \Leftrightarrow B) = (\neg A \wedge \neg B) \vee (A \vee B)$.

Beweis:

(i) Beweis mit der Wahrheitstafel:

A	B	$A \Rightarrow B$	$\neg A$	$\neg A \vee B$
w	w	w	f	w
w	f	f	f	f
f	w	w	w	w
f	f	w	w	w

(ii) Auch mit der Wahrheitstafel oder unter der Nutzung der Rechenregeln wie folgt:

$$\begin{aligned}(A \Leftrightarrow B) =& [(A \Rightarrow B) \wedge (B \Rightarrow A)] \\ =& [(\neg A \vee B) \wedge (\neg B \vee A)] \\ =& [(\neg A \wedge \neg B) \vee (\neg A \wedge A) \vee (B \wedge \neg B) \vee (B \wedge A)] \\ =& [(\neg A \wedge \neg B) \vee \mathrm{f} \vee \mathrm{f} \vee (B \wedge A)] \\ =& (\neg A \wedge \neg B) \vee (A \wedge B).\end{aligned}$$

□

Satz 2.27.

Die *Negation einer Implikation* lautet:

$$\neg(A \Rightarrow B) = A \wedge \neg B.$$

Beweis:

$$\neg(A \Rightarrow B) = \neg(\neg A \vee B) = \neg(\neg A) \wedge \neg B = A \wedge \neg B.$$

□

Beispiel 2.28. Wir negieren folgende Aussagen:

1) Wenn die Sonne scheint, ist es warm. Also A: Die Sonne scheint, B: es ist warm. Dann lautet die Negation von $A \Rightarrow B$ nach obiger Feststellung $A \wedge \neg B$ und somit in Worten: Die Sonne scheint und es ist nicht warm.

2) Wenn $x > 0$ ist, dann ist $100x - 1 > 0$. Negation: Es ist $x > 0$ und $100x - 1 \leq 0$.

3) Wenn es regnet, nehme ich einen Regenschirm. Negation: Es regnet und ich nehme keinen Regenschirm.

Satz 2.29.

$[A \Rightarrow B] = [\neg B \Rightarrow \neg A]$.

Beweis:
Wir beweisen die Aussage des Satzes auf zwei verschiedene Arten. Zunächst mittels Wahrheitstafel, anschließend mit den uns bekannten Rechenregeln.

1) Beweis mit der Wahrheitstafel:

A	B	$A \Rightarrow B$	$\neg B$	$\neg A$	$\neg B \Rightarrow \neg A$
w	w	w	f	f	w
w	f	f	w	f	f
f	w	w	f	w	w
f	f	w	w	w	w

2) Beweis mit den Rechenregeln:

$$[\neg B \Rightarrow \neg A] = [\neg(\neg B) \vee \neg A] = [B \vee \neg A] = [\neg A \vee B] = [A \Rightarrow B].$$

□

Definition 2.30.

Die Aussage $\neg B \Rightarrow \neg A$ heißt *Kontraposition* der Aussage $A \Rightarrow B$.

Der obige Satz besagt, dass eine Implikation und ihre Kontraposition äquivalent sind.

Beispiel 2.31.

1) Implikation: $x > 0 \Rightarrow 2x + 1 > 0$.
Kontraposition: $2x + 1 \leq 0 \Rightarrow x \leq 0$, beide Aussagen sind wahr.

2) Implikation: $x^2 > 0 \Rightarrow x > 0$.
Kontraposition: $x \leq 0 \Rightarrow x^2 \leq 0$, beide Aussagen sind falsch.

3) Implikation: a, b sind ungerade $\Rightarrow a + b$ ist gerade.
Kontraposition: $a + b$ ist ungerade $\Rightarrow$ eine der Zahlen a, b ist gerade, beide Aussagen sind wahr.

4) Implikation: Wenn die Sonne scheint, ist es warm.
Kontraposition: Wenn es nicht warm ist, scheint die Sonne nicht.

5) Implikation: Wenn es regnet, nehme ich einen Regenschirm.
Kontraposition: Wenn ich keinen Regenschirm nehme, regnet es nicht.

2.3 Quantoren

Definition 2.32.

Sei X eine Menge. Eine Abbildung $A : X \to \{\mathrm{w}, \mathrm{f}\},\ x \mapsto A(x)$ heißt eine *Aussageform*. Das heißt $A(x)$ ist eine Aussage, deren Wert vom Wert der Variable $x \in X$ abhängt.

Beispiel 2.33.

1) $X = \mathbb{N},\ A(n) =$ „n ist gerade.“ Dann ist $A(1)$ falsch, $A(2)$ wahr, $A(3)$ falsch und so weiter.
2) $X = \mathbb{R},\ A(x) =$ „$x > 0$.“ $A(1.3), A(\pi), A(2)$ sind wahr, $A(0), A(-1), A(-3.2)$ sind falsch.
3) $X = \mathbb{N},\ A(n) =$ „$n > 0$.“ $A(n)$ ist wahr für alle $n \in \mathbb{N}$.

Definition 2.34.

(i) $A(x)$ heißt *allgemeingültige Aussageform*, wenn $A(x)$ für alle $x \in X$ wahr ist. Wir schreiben

$$\forall x \in X : A(x)$$

und sprechen: „Für alle $x \in X$ gilt $A(x)$“. Das Symbol $\forall$ heißt *Allquantor*.

(ii) $A(x)$ heißt *erfüllbare Aussageform*, wenn es (mindestens) ein $x \in X$ gibt, für welches $A(x)$ wahr ist. Wir schreiben

$$\exists x \in X : A(x)$$

und sprechen: „Es existiert ein $x \in X$, für welches $A(x)$ wahr ist“. Das Symbol $\exists$ heißt *Existenzquantor*.

Beispiel 2.35.

1) $\forall n \in \mathbb{N} : n > 0$.
2) $\exists n \in \mathbb{N} : n$ ist gerade.
3) $\forall x \in \mathbb{R} : x^2 \geq 0$.
4) $\exists x \in \mathbb{R} : x^2 \leq 0$.

   Man kann Quantoren auch aneinander reihen.
5) $\forall n \in \mathbb{N} : \forall m \in \mathbb{N} : n \cdot m \in \mathbb{N}$.
6) $\forall n \in \mathbb{N} : \forall m \in \mathbb{N} : \frac{n}{m} \in \mathbb{N}$ (falsch).
7) $\exists n \in \mathbb{N} : \exists m \in \mathbb{N} : \frac{n}{m} \notin \mathbb{N}$.
8) $\forall n \in \mathbb{N} : \exists m \in \mathbb{N} : \frac{n}{m} \notin \mathbb{N}$.
9) $\forall \varepsilon > 0 : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |a_n - a| < \varepsilon$, dies ist die Definition des Grenzwertes einer Folge a_n mit $\lim\limits_{n \to \infty} a_n = a$.

Bemerkung 2.36. Die Negation einer Allaussage ist eine Existenzaussage und umgekehrt:

$$\neg\big(\forall x \in X : A(x)\big) = \big(\exists x \in X : \neg A(x)\big),$$
$$\neg\big(\exists x \in X : A(x)\big) = \big(\forall x \in X : \neg A(x)\big).$$

Beispiel 2.37.

1) $\forall n \in \mathbb{N} : n > 0$.
   Negation: $\exists n \in \mathbb{N} : n \leq 0$.

2) $\exists n \in \mathbb{N} : n$ ist gerade.
   Negation: $\forall n \in \mathbb{N} : n$ ist ungerade.

3) $\forall x \in \mathbb{R} : x^2 \geq 0$.
   Negation: $\exists x \in \mathbb{R} : x^2 < 0$.

4) $\exists x \in \mathbb{R} : x^2 \leq 0$.
   Negation: $\forall x \in \mathbb{R} : x^2 > 0$.

5) Jedes Auto hat genau vier Räder.
   Negation: Es gibt Autos, welche nicht genau vier Räder haben (weniger oder mehr als vier Räder).

6) $\forall n \in \mathbb{N} : \forall m \in \mathbb{N} : n \cdot m \in \mathbb{N}$.
   Negation: $\exists n \in \mathbb{N} : \neg(\forall m \in \mathbb{N} : n \cdot m \in \mathbb{N}) = \exists n \in \mathbb{N} : \exists m \in \mathbb{N} : n \cdot m \notin \mathbb{N}$.

7) $\exists n \in \mathbb{N} : \exists m \in \mathbb{N} : \frac{n}{m} \notin \mathbb{N}$.
   Negation: $\forall n \in \mathbb{N} : \forall m \in \mathbb{N} : \frac{n}{m} \in \mathbb{N}$.

8) $\forall n \in \mathbb{N} : \exists m \in \mathbb{N} : \frac{n}{m} \notin \mathbb{N}$.
   Negation: $\exists n \in \mathbb{N} : \forall m \in \mathbb{N} : \frac{n}{m} \in \mathbb{N}$.

2.4 Beweise

Die Aufgabe des Beweises besteht darin, durch logisches Schließen die Gültigkeit einer Implikation $A \Rightarrow B$ nachzuweisen. Dies kann grundsätzlich auf unterschiedliche Arten erreicht werden. Wir betrachten hier einige wichtige Beweistypen.

2.4.1 Direkter Beweis

Beim direkten Beweis wird von der Voraussetzung A direkt auf die Behauptung B geschlossen, möglicherweise in mehreren Schritten:

$$A \Rightarrow B_1 \Rightarrow B_2 \Rightarrow \ldots \Rightarrow B.$$

Wir betrachten nun exemplarisch einige kurze Sätze, um mit der Beweisart vertraut zu werden.

Beispiel 2.38. $x \geq 1 \Rightarrow 5x + 5 \geq 10$.

Beweis:
$x \geq 1 \Rightarrow 5x \geq 5 \Rightarrow 5x + 5 \geq 10$.

□

Beispiel 2.39. Das Quadrat einer geraden Zahl ist gerade.

Beweis:
Sei $n \in \mathbb{Z}$, n gerade. Nach der Definition einer geraden Zahl gibt es ein $m \in \mathbb{Z}$ mit $n = 2m$. Dann gilt $n^2 = 4m^2 = 2(2m^2) = 2\ell$ mit $\ell = 2m^2 \in \mathbb{Z}$. Es folgt, dass n^2 gerade ist.

□

Beispiel 2.40. Das Quadrat jeder ungeraden Zahl ergibt bei Division durch 8 den Rest 1.

Beweis:
Zunächst verdeutlichen wir uns die obige Behauptung anhand von einigen Beispielrechnungen:

$$\begin{aligned} 1^2 &= 1 = 0 \cdot 8 + 1, \\ 3^2 &= 9 = 1 \cdot 8 + 1, \\ 5^2 &= 25 = 3 \cdot 8 + 1, \\ 7^2 &= 49 = 6 \cdot 8 + 1. \end{aligned}$$

Dies ist im Allgemeinen auch hilfreich, wenn man sich nicht sicher ist, ob die Aussage überhaupt wahr ist (natürlich keine Garantie). Nehmen wir nun also an, dann n ungerade ist. Dann existiert ein $m \in \mathbb{Z}$ mit $n = 2m + 1$. Somit folgt

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

Von den beiden Zahlen ist entweder m oder $m+1$ gerade $\Rightarrow m(m+1)$ ist gerade $\Rightarrow \exists \ell \in \mathbb{Z} : m(m+1) = 2\ell$. Dann gilt $n^2 = 4 \cdot 2\ell + 1 = 8\ell + 1$, also ergibt die Division von n^2 durch 8 den Rest 1.

□

2.4.2 Beweis durch Kontraposition

Wir wissen, dass $(A \Rightarrow B) = (\neg B \Rightarrow \neg A)$ gilt. Beim Beweis durch Kontraposition zeigt man, dass die Kontraposition $\neg B \Rightarrow \neg A$ wahr ist. Damit wird dann auch die Implikation $A \Rightarrow B$ bewiesen.

In manchen Situationen ist die Kontraposition $\neg B \Rightarrow \neg A$ einfacher zu beweisen als die Implikation $A \Rightarrow B$.

Auch hier betrachten wir einige Beispielsätze zur Verdeutlichung.

Beispiel 2.41. Das Quadrat einer ungeraden Zahl ist ungerade.

Beweis:
Wir beweisen den Satz zunächst mit einem direkten Beweis und anschließend mit dem Beweis durch Kontraposition.

1) Direkter Beweis: Nehme an, dass n ungerade ist

   $\Rightarrow \exists m \in \mathbb{Z} : n = 2m + 1$

   $\Rightarrow n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2(2m(m+1)) + 1 = 2\ell + 1$ mit $\ell = 2m(m+1) \in \mathbb{Z}$

   $\Rightarrow n^2$ ist ungerade.

2) Beweis durch Kontraposition:
   Wir formulieren zunächst die Kontraposition. Zu zeigen ist: n ungerade $\Rightarrow n^2$ ungerade. Dann lautet die Kontraposition: n^2 gerade $\Rightarrow n$ gerade.

   Ist n^2 gerade, so gilt $2 | n \cdot n$. Das Produkt $a \cdot b$ zweier ganzer Zahlen ist genau dann durch eine Primzahl p teilbar, wenn eine der beiden Zahlen a, b durch p teilbar ist (mehr über Teilbarkeit in Kapitel „Elementare Zahlentheorie“). Damit gilt $2 | n \Rightarrow n$ gerade.

□

Beispiel 2.42. Für alle $r \geq 0$ gilt: r irrational $\Rightarrow \sqrt{r}$ irrational.

Beweis:
Die Kontraposition lautet in diesem Fall: $\sqrt{r}$ rational $\Rightarrow r$ rational. Es sei also $\sqrt{r}$ rational

$$\begin{aligned} &\Rightarrow \exists n, m \in \mathbb{N} : \sqrt{r} = \frac{n}{m} \\ &\Rightarrow r^2 = \frac{n^2}{m^2} = \frac{\ell}{k},\ \ell, k \in \mathbb{N} \\ &\Rightarrow r^2 \text{ rational.} \end{aligned}$$

□

2.4.3 Beweis durch Widersrpuch

In diesem Fall gehen wir davon aus, dass B falsch ist. Man geht also von $\neg B$ aus und leitet daraus weitere Aussagen her, bis man eine Aussage erhält, die — zumindest beim Vorliegen der Aussage A — falsch ist (man sagt: man kommt zu einem Widerspruch). Da man beim logischen Schließen keinen Fehler gemacht hat, muss der Fehler in der Annahme $\neg B$ liegen. Also ist $\neg B$ falsch und demnach B wahr. Wir leiten also aus der Annahme $A \wedge \neg B$ einen Widerspruch her.

Exemplarisch betrachten wir nun erneut einige Beispielsätze mit den dazugehörigen Widerspruchsbeweisen.

Satz 2.43. *(Euklid, 300 v. Chr.)*

Es gibt unendlich viele Primzahlen.

Beweis:
Wir nehmen an, dass es nur endlich viele — nämlich N — Primzahlen gibt. Wir nummerieren und ordnen diese: $p_1 < p_2 < \ldots < p_N$. Betrachten wir nun die Zahl

$$m = p_1 p_2 \ldots p_N + 1.$$

m ist keine Primzahl, da sie größer als die größte Primzahl p_N ist. Jede Zahl kann als Produkt von Primzahlen geschrieben werden (diese Eigenschaft besprechen wir im Kapitel „Elementare Zahlentheorie“). Folglich gibt es eine Primzahl p_i mit $p_i | m$. Es gilt aber auch $p_i | p_1 p_2 \ldots p_N$. Es folgt, dass $p_i | 1$. Der einzige positive Teiler von 1 ist $1 \Rightarrow p_i = 1 \Rightarrow p_i$ ist keine Primzahl. Widerspruch! Der Widerspruch zeigt, dass die Annahme, dass es nur endlich viele Primzahlen gibt, falsch ist. Wir haben also bewiesen, dass es unendlich viele Primzahlen gibt.

□

Satz 2.44.

Die Zahl $\sqrt{2}$ ist irrational.

Beweis:
Wir nehmen an, dass $\sqrt{2}$ eine rationale Zahl ist

$$\begin{aligned}
&\Rightarrow \sqrt{2} = \frac{n}{m} \text{ mit } n, m \in \mathbb{N},\ n \text{ und } m \text{ teilerfremd} \\
&\Rightarrow 2 = \frac{n^2}{m^2} \Rightarrow n^2 = 2m^2 \Rightarrow 2 | n^2 \\
&\Rightarrow 2 | n \Rightarrow \exists k \in \mathbb{N} : n = 2k.
\end{aligned}$$

Damit ist $n^2 = 4k^2 = 2m^2$ und folglich $m^2 = 2k^2$. Nun gilt $2 | m^2 \Rightarrow 2 | m$. Es folgt, dass n und m beide durch 2 teilbar sind. Das widerspricht der Tatsache, dass n und m teilerfremd sind. Widerspruch $\Rightarrow$ die Annahme, dass $\sqrt{2}$ eine rationale Zahl ist, ist falsch $\Rightarrow \sqrt{2}$ ist eine irrationale Zahl.

□

Der Beweis durch Kontraposition und der Beweis durch Widerspruch sind Beispiele für indirekte Beweise.

Bemerkung 2.45. Es besteht ein Unterschied zwischen einem Beweis durch Kontraposition und einem Beweis durch Widerspruch. Beispielsweise sei A: „Es regnet“ und B: „Die Straße ist nass “. Zu beweisen ist die Implikation $A \Rightarrow B$, Es regnet $\Rightarrow$ Die Straße ist nass. Beim Beweis durch Kontraposition ist zu zeigen, dass $\neg B \Rightarrow \neg A$, Die Straße ist nicht nass $\Rightarrow$ Es regnet nicht. Der Beweis durch Widerspruch führt die Annahme $\neg B \wedge A$ zum Widerspruch. $\neg B \wedge A$: „Es regnet und die Straße ist nicht nass.“ Widerspruch.

2.4.4 Widerlegen von Allaussagen durch ein Gegenbeispiel

Man betrachte eine Aussage der Form $\forall x \in X : A(x)$. Man möchte beweisen, dass diese Aussage falsch ist, beziehungsweise dass $\neg(\forall x \in X : A(x))$ wahr ist. Wie wir wissen, gilt $\neg(\forall x \in X : A(x)) = \exists x \in X : \neg A(x)$. Es reicht also, die äquivalente Aussage $\exists x \in X : \neg A(x)$ zu beweisen. Das heißt, dass man ein $x \in X$ finden muss, für welches $A(x)$ falsch ist.

Beispiel 2.46.

1) Wir behaupten, dass alle Primzahlen ungerade sind, d.h.

$$\forall n \in \mathbb{N} : n \text{ ist Primzahl } \Rightarrow n \text{ ist ungerade.}$$

Gegenbeispiel: $\exists n \in \mathbb{N} : \neg(n \text{ ist Primzahl} \Rightarrow n \text{ ist ungerade}) = \exists n \in \mathbb{N} : n$ ist Primzahl und n ist gerade. $n = 2$ ist ein Gegenbeispiel.

2) $\forall n \geq 2$ ist die Zahl $2^n - 1$ eine Primzahl.

$n = 2$: $2^2 - 1 = 3$ Primzahl.

$n = 3$: $2^3 - 1 = 7$ Primzahl.

$n = 4$: $2^4 - 1 = 15$ keine Primzahl $\rightarrow$ Gegenbeispiel.

Es ist allerdings eine interessante Beobachtung, dass exemplarisch $2^5 - 1 = 31$, $2^7 - 1 = 127$ auch Primzahlen sind. Viele Zahlen der Form $2^n - 1$ sind Primzahlen.

2.5 Vollständige Induktion

Wir werden zunächst die Menge $\mathbb{N}$ axiomatisch beschreiben.

Axiom 2.47. Peano-Axiome

Die Menge $\mathbb{N}$ der natürlichen Zahlen ist eine Menge, die die sogenannten *Peano-Axiome* erfüllt:

(A1) $1 \in \mathbb{N}$.

(A2) Zu jeder natürlichen Zahl $n \in \mathbb{N}$ gibt es genau einen Nachfolger $S(n)$, welcher wieder eine natürliche Zahl ist.

(A3) Es gibt keine natürliche Zahl, deren Nachfolger 1 ist.

(A4) Sind zwei natürliche Zahlen verschieden, so sind auch ihre Nachfolger verschieden.

(A5) Enthält eine Menge natürlicher Zahlen die Zahl 1 und mit jeder Zahl ihren Nachfolger, so enthält sie alle natürlichen Zahlen.

Den Nachfolger von 1 nennt man 2, den Nachfolger von 2 nennt man 3 und so weiter.

Bemerkung 2.48.

1) Es gibt unendlich viele natürliche Zahlen.

Beweis:
Aus (A1) folgt, dass $1 \in \mathbb{N}$. Aus (A2) folgt, dass es einen Nachfolger von 1 gibt: $2 = S(1) \in \mathbb{N}$. Dabei gilt $S(1) \neq 1$, da sonst 1 der Nachfolger der Zahl 1 wäre, was (A3) widerspricht. Die Menge $\mathbb{N}$ besteht also aus mindestens zwei (verschiedenen) Element $1, 2$. Nach (A2) gibt es $3 = S(2)$ und nach (A3) $3 = S(2) \neq 1$. Nach (A4) $1 \neq 2 \Rightarrow S(1) \neq S(2)$. Es gibt also mindestens drei Elemente $1, 2, 3$. Mit jedem Nachfolger wird die Menge erweitert. Es gibt also unendlich viele natürliche Zahlen.

□

2) $\mathbb{N}$ ist eine geordnete Menge:
$n < m$, wenn n in der Reihenfolge der Nachfolger vor m steht,
$n \leq m$, wenn $n < m$ oder $n = m$,
$n > m$, wenn $m < n$,
$n \geq m$, wenn $m \leq n$.

3) Man definiert die arithmetischen Operationen auf $\mathbb{N}$ folgendermaßen:

Definition 2.49.

Die *Addition* der natürlichen Zahlen ist definiert durch:

$$a + 1 = S(a) \quad \text{und} \quad a + S(b) = S(a + b).$$

Insbesondere gilt:

$$a + 2 = a + S(1) = S(a + 1) = S(S(a)),$$
$$a + 3 = a + S(2) = S(a + 2) = S(S(S(a))) \quad \text{und so weiter.}$$

Definition 2.50.

Die *Multiplikation* der natürlichen Zahlen ist definiert durch:

$$a \cdot 1 = a \quad \text{und} \quad a \cdot S(b) = a + a \cdot b.$$

Insbesondere gilt:

$$a \cdot 2 = a \cdot S(1) = a + a \cdot 1 = a + a$$
$$a \cdot 3 = a \cdot S(2) = a + a \cdot 2 = a + a + a \quad \text{und so weiter.}$$

4) (A5) ist das Axiom der *vollständigen Induktion*.

Definition 2.51.

Wir definieren nun, was wir unter dem *Prinzip der vollständigen Induktion* (für Aussagen) verstehen. Sei $A(n) : \mathbb{N} \to \{\mathrm{w}, \mathrm{f}\}$ eine Aussageform. Gilt

(1) $A(1)$ und

(2) $\forall n \in \mathbb{N} : A(n) \Rightarrow A(n + 1)$,

so gilt $\forall n \in \mathbb{N} : A(n)$.

Die Aussage „$A(1)$ ist wahr“ heißt der *Induktionsanfang* (IA) (oder die *Induktionsverankerung*). Der Nachweis von (2) heißt *Induktionsschritt* (IS). Die Aussage „$A(n)$ ist wahr“ heißt *Induktionsvoraussetzung* (IV), die Aussage „$A(n + 1)$ ist wahr“ heißt *Induktionsbehauptung*.

Beispiel 2.52.

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

Beweis:

IA: Für $n = 1$ folgt $\sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2}$.

IS: Wir betrachten $\sum_{k=1}^{n+1} k$ und wollen zeigen, dass dieser Ausdruck mit $\frac{(n+1)(n+2)}{2}$ übereinstimmt. Insbesondere gehen wir nun davon aus, dass $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ für ein konkretes $n \in \mathbb{N}$ gilt (dies ist unsere Induktionsvoraussetzung).

$$\begin{aligned}\sum_{k=1}^{n+1} k =& \sum_{k=1}^{n} k + (n+1) = \frac{n(n+1)}{2} + (n+1)\\ =&(n+1)\left(\frac{n}{2}+1\right) = (n+1)\frac{(n+2)}{2}\\ =&\frac{(n+1)(n+2)}{2},\end{aligned}$$

also gilt die Formel auch für $n+1$.

Nach dem Prinzip der vollständigen Induktion gilt die Formel für alle $n \in \mathbb{N}$.

□

Bevor wir weitere Beispiele besprechen, betrachten wir folgende *Varianten der Induktion*.

Es kann vorkommen, dass eine Aussage nur für $n \geq n_0$ gilt. In diesem Fall betrachtet man als Induktionsanfang $A(n_0)$:
$(1')$ $A(n_0)$ ist wahr.
Die Aussage gilt dann für alle $n \geq n_0$. Insbesondere kann aber $n_0 = 0$ ebenfalls eintreten.

Darüber hinaus ist es möglich, dass man im Induktionsschritt nicht nur $A(n)$, sondern auch beispielsweise auch $A(n-1), A(n-2)$ etc. benötigt. Man kann (2) dann so formulieren:
$(2')$: $\forall n \in \mathbb{N} : A(k)$ ist wahr für alle $1 \geq k \geq n \Rightarrow A(n+1)$ ist wahr.

2) Behauptet wird nun, dass $\sum_{k=1}^{n} k(k+1) = \frac{1}{3}n(n+1)(n+2)$.

Beweis:

IA: Für $n = 1$ folgt $\sum_{k=1}^{1} k(k+1) = 1 \cdot 2 = 2 = \frac{1}{3} \cdot 1(1+1)(1+2)$.

IS: Wir betrachten nun $\sum_{k=1}^{n+1} k(k+1)$ und möchten die Gleichheit zu $\frac{1}{3}(n+1)(n+2)(n+3)$ zeigen. Dazu nutzen wieder unsere Induktionsvoraussetzung.

$$\begin{aligned}\sum_{k=1}^{n+1} k(k+1) =& \sum_{k=1}^{n} k(k+1) + (n+1)(n+2)\\ =&\frac{1}{3}n(n+1)(n+2) + (n+1)(n+2)\\ =&(n+1)(n+2)\left(\frac{1}{3}n+1\right) = \frac{1}{3}(n+1)(n+2)(n+3).\end{aligned}$$

Nach dem Prinzip der vollständigen Induktion gilt die Formel für alle $n \in \mathbb{N}$.

□

3) Als drittes Beispiel widmen wir uns der Bernoullischen Ungleichung

$$(1+x)^n \geq 1 + nx \quad \text{für} \quad x \geq -1 \text{ und } n \in \mathbb{N}.$$

Beweis:

IA: Für $n = 1$ folgt $(1+x)^1 \geq 1 + 1 \cdot x$.

IS: Im Induktionsschritt beschäftigen wir uns mit Problematik, ob $(1+x)^{n+1} \geq 1+(n+1)x$ gilt. Auch hier nutzen wir unsere Induktionsvoraussetzung.

$$\begin{aligned}(1+x)^{n+1} =& (1+x)^n \cdot (1+x)\\ \geq& (1+nx)(1+x) = 1+x+nx+nx^2\\ \geq& 1+(n+1)x,\end{aligned}$$

wobei die letzte Ungleichung gilt, da $nx^2 \geq 0$.

Nach dem Prinzip der vollständigen Induktion gilt die Formel also für alle $n \in \mathbb{N}$.

□

4) Um uns mit den verschiedenen angesprochenen Varianten der Induktion zu beschäftigen, fragen wir uns, für welche $n \geq 0$ die Ungleichung $2^n > n^2$ gilt.

$n = 0$: $2^0 = 1 > 0^2 = 0$.

$n = 1$: $2^1 = 2 > 1^2 = 1$.

$n = 2$: $2^2 = 4 = 2^2$.

$n = 3$: $2^3 = 8 < 3^2 = 9$.

$n = 4$: $2^4 = 16 = 4^2 = 16$.

$n = 5$: $2^5 = 32 > 5^2 = 25$.

$n = 6$: $2^6 = 64 > 6^2 = 36$.

Vermutung: Für $n = 0, 1$ und $n \geq 5$ gilt $2^n > n^2$. Wir beweisen nun diese Ungleichung für $n \geq 5$ mit der vollständigen Induktion.

Beweis:

IA: Für $n = 5$ gilt $2^5 = 32 > 5^2 = 25$.

IS: Wir betrachten 2^{n+1} und zeigen, dass dieser Ausdruck größer als $(n+1)^2$ ist.

$$2^{n+1} = 2^n \cdot 2 > n^2 \cdot 2 = n^2 + n^2 \geq n^2 + 2n + 1 = (n+1)^2,$$

wobei $2^n > n^2$ unsere Induktionsvoraussetzung war und die letzte Ungleichung gilt, da $n^2 \geq 2n+1$ für $n \geq 5$, was wegen

$$n^2 - 2n - 1 \geq 0,\ n_{1,2} = 1 \pm \sqrt{2},\ n_1 = 1 - \sqrt{2} < 0,\ n_2 = 1 + \sqrt{2} < 5,\ \text{da } \sqrt{2} < 4,$$

einsichtig ist.

Nach dem Prinzip der vollständigen Induktion gilt die Formel für alle $n \geq 5$.

Auch die Ungleichung $n^2 \geq 2n+1$ für $n \geq 5$ kann man mit der vollständigen Induktion beweisen:

IA: Für $n = 5$ gilt $5^2 = 25 \geq 2 \cdot 5 + 1 = 11$.

IS: Hier ist zu zeigen, dass $(n+1)^2 \geq 2(n+1) + 1 = 2n + 3$ gilt.

$$(n+1)^2 = n^2 + 2n + 1 \geq 2n + 1 + 2n + 1 = 2n + 2n + 2 \geq 2n + 3,$$

da $2n \geq 1$ ist.

Die Ungleichung gilt also für alle $n \geq 5$ nach dem Prinzip der vollständigen Induktion. Bemerkt sei, dass die Herleitung im Induktionsschritt in diesem Beispiel für alle $n \geq 1$ gilt, die Behauptung $n^2 \geq 2n + 1$ aber nicht! Für $n = 1$ ist $n^2 = 1 < 2n + 1 = 3$. Für die Ungleichung $n^2 \geq 2n + 1$ würde dann der Induktionsanfang fehlen.

$n = 2$: $n^2 = 4 < 2n + 1 = 5$.

$n = 3$: $n^2 = 9 \geq 2n + 1 = 7$.

Die Ungleichung $n^2 \geq 2n + 1$ gilt also für alle $n \geq 3$.

□

5) Als vorerst letztes Beispiel schauen wir uns eine andere typische Anwendung der Induktion im Bereich der Teilbarkeit an. Behauptet wird, dass $\forall n \in \mathbb{N} : 6|(n^3 - n)$.

Beweis:

IA: Für $n = 1$ ist $n^3 - n = 0$ und $6|0$.

IS: Betrachtet wird der Ausdruck $(n + 1)^3 - (n + 1)$. Wir nehmen nun einige elementare Umformungen vor:

$$\begin{aligned}(n+1)^3 - (n+1) &= n^3 + 3n^2 + 3n + 1 - n - 1 \\ &= n^3 + 3n^2 + 2n \\ &= (n^3 - n) + 3n^2 + 3n \\ &= (n^3 - n) + 3n(n+1),\end{aligned}$$

nun gilt $6|(n^3 - n)$ nach unserer Induktionsvoraussetzung. Bei dem Ausdruck $3n(n + 1)$ ist zwangsläufig entweder n oder $n + 1$ gerade. Demnach ist auch $n(n + 1)$ gerade, also gilt $6|3n(n + 1)$. Damit teilt 6 auch die Summe $(n^3 - n) + 3n(n + 1)$.

Nach dem Prinzip der vollständigen Induktion ist $n^3 - n$ für alle $n \in \mathbb{N}$ durch 6 teilbar.

□

Kapitel 3

Abbildungen

3.1 Der Begriff einer Abbildung

Definition 3.1.

Seien X und Y zwei nichtleere Mengen.

1) Eine *Abbildung* (*Funktion*) f von X nach Y ist eine Vorschrift, die jedem $x \in X$ genau ein $y \in Y$ zuordnet.

2) Das dem Element x zugeordnete Element y bezeichnet man mit $f(x)$ und nennt man den *Wert der Funktion* f an der Stelle x.

3) X heißt der *Definitionsbereich* (die *Definitionsmenge*) und Y heißt der *Wertebereich* (die *Zielmenge*).

Weitere Terminologie:
x heißt das *Argument* von f. Man sagt auch: x ist die *unabhängige Variable* und y ist die *abhängige Variable*. Die Zuordnung $x \mapsto f(x)$ heißt die *Abbildungsvorschrift* (die *Funktionsvorschrift*). Wir schreiben dann

$$f : X \to Y,\ x \mapsto f(x).$$

Zu jeder Abbildung gehören also drei Elemente: der Definitionsbereich, der Wertebereich und die Abbildungsvorschrift.

Beispiel 3.2.

1) $f_1 : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$ mit dem Definitionsbereich $\mathbb{R}$, dem Wertebereich $\mathbb{R}$ und der Funktionsvorschrift $f_1(x) = x^2$.

2) $f_2 : [0, \infty) \to \mathbb{R},\ x \mapsto x^2$ mit dem Definitionsbereich $[0, \infty)$, dem Wertebereich $\mathbb{R}$ und der Funktionsvorschrift $f_2(x) = x^2$.

3) $\tilde{f} : \mathbb{N} \to \mathbb{N}, n \mapsto n^2$ mit dem Definitionsbereich $\mathbb{N}$, dem Wertebereich $\mathbb{N}$ und der Funktionsvorschrift $\tilde{f}(n) = n^2$.

4) $g : \{1, 2, 3\} \to \{-2, -1, 0, 1, 2\}$ mit dem Definitionsbereich $\{1, 2, 3\}$ und dem Wertebereich $\{-2, -1, 0, 1, 2\}$. Die Funktionsvorschrift laute $1 \mapsto 1,\ 2 \mapsto 2,\ 3 \mapsto 0$. Abbildung 3.1 visualisiert diese Funktion.

5) $h : \{\square, \triangle, \star \circ \bullet\} \to \{r, e\}$ mit Definitionsbereich $\{\square, \triangle, \star \circ \bullet\}$ und dem Wertebereich $\{r, e\}$ (rund, eckig). Die Funktionsvorschrift laute $\square \mapsto e,\ \triangle \mapsto e,\ \star \mapsto e,\ \circ \mapsto r,\ \bullet \mapsto r$. Visualisiert wird die Funktion ebenfalls an Abbildung 3.1.

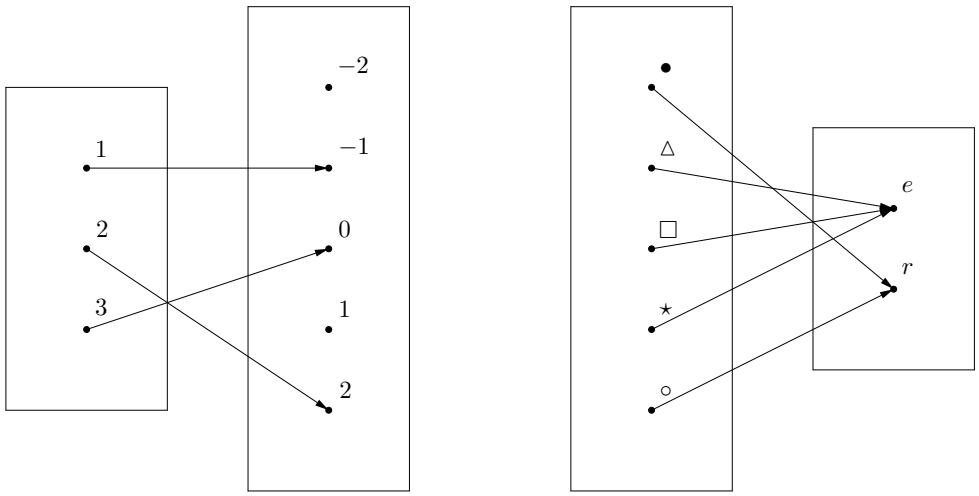

Abbildung 3.1: Funktion g (links) und Funktion h (rechts) aus dem obigen Beispiel.

Bemerkung 3.3. Zwei Abbildungen sind genau dann gleich, wenn ihre Definitionsbereiche, ihre Wertebereiche und ihre Abbildungsvorschriften gleich sind.

So sind die Funktionen f_1, f_2 und $\tilde{f}$ aus den Beispielen nicht gleich. Insbesondere sind f_1 und f_2 nicht gleich, da ihre Definitionsbereiche verschieden sind. Sie haben auch unterschiedliche Eigenschaften, so ist beispielsweise f_2 monoton, f_1 hingegen nicht. Auch die Funktionen $F_1 : \mathbb{R}\backslash\{0\} \to \mathbb{R},\ x \mapsto \frac{1}{x}$ und $F_2 : \mathbb{R}\backslash\{0\} \to \mathbb{R}\backslash\{0\},\ x \mapsto \frac{1}{x}$ sind formal nicht gleich.

Definition 3.4.

Die Menge $G(f) = \{(x, f(x)) : x \in X\} \subseteq X \times Y$ heißt der *Graph* der Abbildung f. Dieser ist eine Teilmenge des kartesischen Produktes $X \times Y$.

Beispiel 3.5.

1) $f_1 : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$, dann ist $G(f_1) = \{(x, x^2) : x \in \mathbb{R}\}$.

2) $f_2 : [0, \infty) \to \mathbb{R},\ x \mapsto x^2$, dann ist $G(f_2) = \{(x, x^2) : x \in [0, \infty)\}$.

3) $\tilde{f} : \mathbb{N} \to \mathbb{N},\ n \mapsto n^2$, dann ist $G(\tilde{f}) = \{(n, n^2) : n \in \mathbb{N}\} = \{(1, 1), (2, 4), (3, 9), \ldots\}$.

4) $g : \{1, 2, 3\} \to \{-2, -1, 0, 1, 2\}$ mit $g(1) = -1,\ g(2) = 2,\ g(3) = 0$, dann ist $G(g) = \{(1, -1), (2, 2), (3, 0)\}$.

5) $h : \{\square, \triangle, \star \circ \bullet\} \to \{r, e\}$ mit $h(\square) = e,\ h(\triangle) = e,\ h(\star) = e,\ h(\circ) = r,\ h(\bullet) = r$, dann ist $G(h) = \{(\square, e), (\triangle, e), (\star, e), (\circ, r), (\bullet, r)\}$.

Definition 3.6.

Die mengentheoretische Definition des Funktionsbegriffs lautet wie folgt: Eine *Abbildung* (eine *Funktion*) ist ein Tripel (X, Y, G) bestehend aus einer Menge X (der *Definitionsbereich*), einer Menge Y (der *Wertebereich*) und einer Teilmenge G des kartesischen Produkts $X \times Y$ (der *Graph*) mit den Eigenschaften:

(i) $\forall x \in X : \exists y \in Y : (x, y) \in G$.

(ii) $\forall x \in X : \forall y_1, y_2 \in Y : (x, y) \in G \wedge (x, y_2) \in G \Rightarrow y_1 = y_2$.

Bemerkung 3.7. Die erste Bedingung bedeutet, dass jedes $x \in X$ als erste Komponente eines Paares in G auftritt. Das heißt, dass die Funktion jedem $x \in X$ einen Wert $y = f(x)$ zuordnet. Die zweite Bedingung garantiert die Eindeutigkeit der Zuordnung, da für zwei Werte $y_1 = f(x)$ und $y_2 = f(x)$ gelten muss, dass $y_1 = y_2$.

3.2 Bild und Urbild

Definition 3.8.

Sei $f : X \to Y$ eine Abbildung.

1) Für eine Menge $A \subseteq X$ heißt die Menge $f(A) = \{y \in Y : (\exists x \in A : f(x) = y)\} = \{f(x) : x \in A\}$ das *Bild* der Menge A unter f. Die Menge $f(X)$ heißt das *Bild von* f.

2) Für eine Menge $B \subseteq Y$ heißt die Menge $f^{-1}(B) = \{x \in X : f(x) \in B\}$ das *Urbild* der Menge B unter f.

Bemerkung 3.9. Für ein Element $y \in Y$ ist das Urbild von y die Menge

$$f^{-1}(\{y\}) = \{x \in X : f(x) = y\}.$$

Beispiel 3.10.

1) Sei $f : \mathbb{R} \to \mathbb{R},\ f(x) = x^2$, wir betrachten nun exemplarisch einige Bilder und Urbilder.

$f([0,1]) = [0,1],\ f([-1,1]) = [0,1],\ f((-1,2)) = [0,4),\ f(\{0,1\}) = \{0,1\},$
$f(\{-1,0,1\}) = \{0,1\},\ f((5,\infty)) = (25,\infty),\ f(\mathbb{R}) = [0,\infty),\ f^{-1}([0,1]) = [-1,1],$
$f^{-1}([-1,1]) = [-1,1],\ f^{-1}(\{0,1\}) = \{-1,0,1\},\ f^{-1}((0,4)) = (-2,0) \cup (0,2),\ f^{-1}((-3,2)) = \emptyset,$
$f^{-1}(\{1\}) = \{-1,1\},\ f^{-1}(\{0\}) = \{0\},\ f^{-1}(\{-1\}) = \emptyset,\ f^{-1}(\mathbb{R}) = \mathbb{R}.$

2) Sei $g : \{1,2,3\} \to \{-2,-1,0,1,2\}$ mit $g(1) = -1,\ g(2) = 2,\ g(3) = 0$. Einige Bilder und Urbilder lauten dann:

$$g(\{1\}) = \{-1\},\ g(\{1,3\}) = \{-1,0\},\ g^{-1}(\{0\}) = \{3\}, g^{-1}(\{1\}) = \emptyset,\ g^{-1}(\{-2,-1,0\}) = \{1,3\}.$$

Satz 3.11.

Sei $f : X \to Y$ eine Abbildung und seien $A, A_1, A_2 \subseteq X$ sowie $B, B_1, B_2 \subseteq Y$. Dann gilt:

1) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
2) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.
3) $f(A_1 \backslash A_2) \supseteq f(A_1) \backslash f(A_2)$.
4) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.
5) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.
6) $f^{-1}(B_1 \backslash B_2) = f^{-1}(B_1) \backslash f^{-1}(B_2)$.
7) $A \subseteq f^{-1}(f(A))$.
8) $f(f^{-1}(B)) \subseteq B$.

Beweis:
Die Beweise erfolgen exemplarisch, weitere Regeln werden in den Übungen bewiesen.

1) Sei $y \in f(A_1 \cup A_2)$

$$\begin{aligned}
&\Leftrightarrow \exists x \in A_1 \cup A_2 : f(x) = y \\
&\Leftrightarrow (\exists x \in A_1 : f(x) = y) \vee (\exists x \in A_2 : f(x) = y) \\
&\Leftrightarrow y \in f(A_1) \vee y \in f(A_2) \\
&\Leftrightarrow y \in f(A_1) \cup f(A_2).
\end{aligned}$$

□

4) Sei $x \in f^{-1}(B_1 \cup B_2)$

$$\begin{aligned}
&\Leftrightarrow f(x) \in B_1 \cup B_2 \\
&\Leftrightarrow f(x) \in B_1 \vee f(x) \in B_2 \\
&\Leftrightarrow x \in f^{-1}(B_1) \vee x \in f^{-1}(B_2) \\
&\Leftrightarrow x \in f^{-1}(B_1) \cup f^{-1}(B_2).
\end{aligned}$$

□

2) Sei $y \in f(A_1 \cap A_2)$

$$\begin{aligned}
&\Leftrightarrow \exists x \in A_1 \cap A_2 : f(x) = y \\
&\Rightarrow y \in f(A_1) \wedge y \in f(A_2) \\
&\Leftrightarrow y \in f(A_1) \cap f(A_2).
\end{aligned}$$

Gleichheit gilt nicht, da aus $y \in f(A_1)$ und $y \in f(A_2)$ im Allgemeinen nicht folgt, dass es mit dem gleichen $x \in A_1 \cap A_2$ erreicht werden kann, also dass $\exists x \in A_1 \cap A_2 : f(x) = y$ gilt. Exemplarisch gilt für $f : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$ und den Mengen $A_1 = [-1, 0],\ A_2 = [0, 1],\ A_1 \cap A_2 = \{0\}$:

$$f(A_1 \cap A_2) = \{0\},\ f(A_1) = [0, 1],\ f(A_2) = [0, 1],\ f(A_1) \cap f(A_2) = [0, 1].$$

□

6) Sei $x \in f^{-1}(B_1 \backslash B_2)$

$$\begin{aligned}
&\Leftrightarrow f(x) \in B_2 \backslash B_2 \\
&\Leftrightarrow f(x) \in B_1 \wedge f(x) \notin B_2 \\
&\Leftrightarrow x \in f^{-1}(B_1) \wedge x \notin f^{-1}(B_1) \\
&\Leftrightarrow x \in f^{-1}(B_1) \backslash f^{-1}(B_2).
\end{aligned}$$

□

7) Sei $x \in A \Rightarrow \exists y \in Y : f(x) = y$. Für dieses y gilt: $y \in f(A)$. Insbesondere gilt $f(x) \in f(A) \Rightarrow x \in f^{-1}(f(A))$.

Auch hier gilt im Allgemeinen keine Gleichheit, was wir exemplarisch wieder mit $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ und dem Intervall $A = [0, 1]$ deutlich wird, denn hier ist

$$f(A) = [0, 1] \text{ aber } f^{-1}(f(A)) = [-1, 1] \supseteq A.$$

□

3.3 Injektivität, Surjektivität, Bijektivität und die Umkehrfunktion

Definition 3.12.

Sei $f : X \to Y$ eine Abbildung.

1) Die Abbildung f heißt *injektiv*, wenn für jedes $y \in Y$ das Urbild $f^{-1}(\{y\})$ von y höchstens ein Element enthält. Das ist äquivalent dazu, dass

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

oder dass

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

2) Die Abbildung f heißt *surjektiv*, wenn für jedes $y \in Y$ das Urbild $f^{-1}(\{y\})$ von y nicht leer ist: $f^{-1}(\{y\}) \neq \emptyset$. Das heißt

$$\forall y \in Y : \exists x \in X : f(x) = y.$$

3) Die Abbildung f heißt *bijektiv*, wenn f injektiv und surjektiv ist.

Bemerkung 3.13. Eine Abbildung f ist genau dann bijektiv, wenn für jedes $y \in Y$ das Urbild $f^{-1}(\{y\})$ von y genau ein Element enthält.

Bemerkung 3.14. Ist f surjektiv, so sagt man auch „f ist eine Abbildung auf Y“.

Beispiel 3.15.

1) $f_1 : \mathbb{R} \to \mathbb{R}$, $f_1(x) = x^2$ ist

- nicht injektiv, da beispielsweise $f_1^{-1}(\{1\}) = \{-1, 1\}$ aus mehr als einem Element besteht.
- nicht surjektiv, da beispielsweise $f_1^{-1}(\{-1\}) = \emptyset$.

2) $f_2 : [0, \infty) \to \mathbb{R}$, $f_2(x) = x^2$ ist

- injektiv, da für $x_1, x_2 \geq 0$ gilt: $x_1 \neq x_2 \Rightarrow x_1^2 \neq x_2^2$.
- nicht surjektiv, da beispielsweise $f_2^{-1}(\{-1\}) = \emptyset$.

3) $f_3 : \mathbb{R} \to [0, \infty),\ f_3(x) = x^2$ ist

- nicht injektiv, da beispielsweise $f_3^{-1}(\{1\}) = \{-1, 1\}$ aus mehr als einem Element besteht.
- surjektiv: $\forall y \geq 0 : \exists x \in \mathbb{R} : x^2 = y$.

4) $f_4 : [0, \infty) \to [0, \infty),\ f_4(x) = x^2$ ist

- injektiv, surjektiv und folglich bijektiv.

Ist f injektiv, so gilt für jedes $x \in X$:

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

In der Tat ist $f(\{x\}) = \{f(x)\}$ und wegen der Injektivität gibt es kein anderes $x' \in X$ mit $f(x') = f(x)$, folglich ist $f^{-1}(f(\{x\})) = \{x\}$. Ist f zusätzlich surjektiv, so gilt $f(X) = Y$. In diesem Fall kann f auf Y invertiert werden.

Definition 3.16.

Sei $f : X \to Y$ eine bijektive Abbildung. Die *inverse Abbildung* (die *Umkehrfunktion*) von f ist die Funktion

$$f^{-1} : Y \to X,\ y \mapsto x \text{ mit } f(x) = y.$$

Für jedes $y \in Y$ ist ein solches $x \in X$ eindeutig bestimmt.

Bemerkung 3.17. Das Symbol f^{-1} wird gleichzeitig für das Urbild und für die Umkehrfunktion benutzt. Im ersten Fall ist das Argument eine Menge $B \subseteq Y$ und im zweiten Fall ein Element $y \in Y$. Insbesondere ist

$$\begin{aligned} f^{-1}(y) &= x \in X \text{ ein Element und} \\ f^{-1}(\{y\}) &= \{x\} \subseteq X \text{ eine Menge.} \end{aligned}$$

Beispiel 3.18.

1) Wir betrachten $f_4 : [0, \infty) \to [0, \infty) : f(x) = x^2$ (bijektiv). Dann ist die Umkehrfunktion f_4^{-1} gegeben durch

$$f_4^{-1} : [0, \infty) \to [0, \infty) : f_4^{-1}(y) = \sqrt{y}$$

beziehungsweise auch $f_4^{-1}(x) = \sqrt{x}$.

2) Es sei $F : \{1, 2, 3, 4, \ldots\} \to \{1, \frac{1}{2}, \frac{1}{3}, \ldots\} : F(x) = \frac{1}{x}$. Die Umkehrfunktion lautet dann:

$$F^{-1} : \left\{1, \frac{1}{2}, \frac{1}{3}, \ldots\right\} \to \{1, 2, 3, \ldots\} : F^{-1}(x) = \frac{1}{x}.$$

Beachte: F und F^{-1} sind unterschiedliche Funktionen (sie haben verschiedene Definitions- und Wertebereiche).

Bemerkung 3.19. Ist $f : X \to Y$ bijektiv, so ist auch $f^{-1} : Y \to X$ bijektiv.

3.4 Verkettung von Abbildungen

Definition 3.20.

Seien X_1, Y_1, X_2, Y_2 nichtleere Mengen und $f : X_1 \to Y_1$ sowie $g : X_2 \to Y_2$ zwei Abbildungen, wobei gilt: $f(X_1) \subseteq X_2$. Die *Verkettung* (die *Komposition*, die *Hintereinanderausführung*) von f und g ist die Abbildung

$$g \circ f : X_1 \to Y_2,\ x \mapsto g(f(x)).$$

Beispiel 3.21. Es sei $f : \mathbb{N} \to \mathbb{N},\ f(n) = n^2$ und $g : \mathbb{N} \to \mathbb{N},\ g(n) = 5n$. Dann sind die möglichen Kompositionen:

$$g \circ f : \mathbb{N} \to \mathbb{N},\ (g \circ f)(n) = 5n^2$$
$$f \circ g : \mathbb{N} \to \mathbb{N},\ (f \circ g)(n) = (5n)^2.$$

Bemerkung 3.22. Wie wir sehen, gilt im Allgemeinen $f \circ g \neq g \circ f$. Das heißt die Komposition ist nicht kommutativ.

Bemerkung 3.23. Zu beachten ist die Reihenfolge der Funktionen in der Verkettung. Die Schreibweise $g \circ f$ entspricht $g(f(x))$ (wir wenden also f zuerst an).

Beispiel 3.24. Es seien $a : \mathbb{R} \to \mathbb{R},\ a(x) = x + 1$ und $b : [0, \infty) \to \mathbb{R},\ b(x) = \sqrt{x}$. Zunächst stellen wir fest, dass $a(\mathbb{R}) = \mathbb{R} \not\subseteq [0, \infty)$. Damit ist die Verkettung $b \circ a$ nicht möglich. Es gilt aber, dass $b([0, \infty)) = [0, \infty) \subseteq \mathbb{R}$. Also ist die Verkettung $a \circ b$ möglich und lautet:

$$a \circ b : [0, \infty) \to \mathbb{R},\ (a \circ b)(x) = \sqrt{x} + 1.$$

Satz 3.25.

Seien $f : X \to Y,\ g : Y \to Z$ und $h : Z \to W$ drei Abbildungen. Dann gilt:

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

Das heißt die Komposition ist assoziativ.

Beweis: Für die linke Seite gilt:

$$h \circ g : Y \to W,\ (h \circ g)(y) = h(g(y)) \quad \text{und}$$
$$(h \circ g) \circ f : X \to W,\ ((h \circ g) \circ f)(x) = h(g(f(x))).$$

Analog erhalten wir für die rechte Seite

$$g \circ f : X \to Z,\ (g \circ f) = g(f(x)) \quad \text{und}$$
$$h \circ (g \circ f) : X \to W,\ (h \circ (g \circ f))(x) = h(g(f(x)),$$

was mit der Formel für die linke Seite übereinstimmt.

□

Definition 3.26.

Sei X eine Menge. Die Abbildung

$$I_X : X \to X,\ x \mapsto x$$

heißt die *Identität* (die *identische Abbildung*).

Bemerkung 3.27. Die identische Abbildung spielt die Rolle eines Einselements bezüglich der Komposition: Für $f : X \to Y$ gilt $f \circ I_X = f$ und für $f : U \to X$ gilt $I_X \circ f = f$.

Bemerkung 3.28. Sei $f : X \to Y$ bijektiv. Dann gilt

$$f^{-1} \circ f = I_X,\ f \circ f^{-1} = I_Y.$$

3.5 Mächtigkeit

Definition 3.29.

Zwei Mengen A und B heißen *gleichmächtig*, wenn es eine bijektive Abbildung von A auf B gibt. In diesem Fall sagt man auch: A und B haben die gleiche *Kardinalität* beziehungsweise die gleiche *Kardinalzahl*.

Bemerkung 3.30. Da aus der Bijektivität der Ausgangsfunktion auch die Bijektivität der Umkehrfunktion folgt, ist es irrelevant, ob A auf B oder B auf A abgebildet wird.

Lemma 3.31.

Zwei endliche Mengen sind genau dann gleichmächtig, wenn sie gleich viele Elemente enthalten.

Beweis:
Es seien M, N endliche Mengen mit $|M| = m,\ |N| = n$. Zu zeigen ist hier eine Äquivalenz.
$\Leftarrow$ Wir nehmen an, dass $m = n$ und wollen zeigen, dass M und N gleichmächtig sind. Wir nummerieren die Elemente von M und N durch:

$$M = \{a_1, \ldots, a_m\} \text{ und } N = \{b_1, \ldots b_m\}.$$

Nun konstruieren wir eine Abbildung $f : M \to N,\ f(a_1) = b_1,\ f(a_2) = b_2,\ \ldots,\ f(a_m) = b_m$. Diese Abbildung ist bijektiv, also sind M und N gleichmächtig.
$\Rightarrow$ Diese Richtung beweisen wir durch Kontraposition. Gehen wir davon aus, dass M und N nicht gleich viele Elemente haben, dann müsste folgen, dass M und N nicht gleichmächtig sind. O.B.d.A (ohne Beschränkung der Allgemeinheit) sei $m > n$. Weiter sei f eine Abbildung von M nach N. $\{f(a_1), \ldots, f(a_m)\} \subseteq N \Rightarrow$ diese Menge hat höchstens $n < m$ Elemente $\Rightarrow\ \exists a_i \neq a_j$ mit $f(a_i) = f(a_j)$. Damit ist jede Abbildung $f : M \to N$ also nicht injektiv und folglich insbesondere nicht bijektiv. Es folgt, dass keine Bijektion von M auf N existiert, womit M und N nicht gleichmächtig sind.

□

Für endliche Mengen definiert man die *Mächtigkeit* (*Kardinalität*) als die Anzahl der Elemente. $0 = |\emptyset|, 1, 2, 3, \ldots$ sind also Kardinalzahlen für endliche Mengen. Die Mächtigkeit soll die „Größe“ der Menge charakterisieren.

Für unendliche Mengen ist es möglich, dass eine echte Teilmenge gleichmächtig zur gesamten Menge ist.

Beispiel 3.32. Die Menge aller natürlichen Zahlen $\mathbb{N}$ und die Menge aller geraden natürlichen Zahlen sind gleichmächtig.

Beweis:
Die Abbildung $f : \{1, 2, 3, 4, \ldots\} \to \{2, 4, 6, 8, \ldots\},\ f(n) = 2n$ ist eine Bijektion.

□

Ein interessanter Fakt (ohne Beweis) ist die Tatsache, dass eine Menge genau dann unendlich groß ist, wenn sie eine gleichmächtige Teilmenge besitzt.

Auch unendliche Mengen sind nicht alle gleich groß!

Definition 3.33.

Jede Menge, die gleichmächtig mit $\mathbb{N}$ ist, heißt *abzählbar*. Die Mächtigkeit von $\mathbb{N}$ bezeichnet man mit $|\mathbb{N}| = \aleph_0$ („Aleph-Null“).

$\aleph_0$ ist die kleinste Mächtigkeit einer unendlichen Menge, das heißt „zwischen“ den endlichen Zahlen und $\aleph_0$ gibt es keine Kardinalzahlen (ohne Beweis).

Satz 3.34.

$|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, das heißt $|\mathbb{N} \times \mathbb{N}|$ ist abzählbar.

Beweis:
Die Paare (n, m) lassen sich nach dem Diagonalverfahren von Cantor anordnen:

$$\begin{array}{cccccc} (1,1) & \to & (1,2) & & (1,3) & & (1,4) & \ldots \\ & \swarrow & & \swarrow & & \swarrow & & \\ (2,1) & & (2,2) & & (2,3) & & (2,4) & \ldots \\ & \swarrow & & \swarrow & & \swarrow & & \\ (3,1) & & (3,2) & & (3,3) & & (3,4) & \ldots \\ \vdots & & \vdots & & \vdots & & & \end{array}$$

Die Bijektion: $f : (n, m) \mapsto \frac{1}{2}(n + m - 2)(n + m - 1) + n$ ordnet dabei einem Paar (n, m) die Nummer seiner Position in der Reihenfolge. In der Tat,

$$\begin{aligned} (1,1) &\mapsto \frac{1}{2}(2-2)(2-1)+1 = 1 \\ (1,2) &\mapsto \frac{1}{2}(3-2)(3-1)+1 = 1+1 = 2 \\ (2,1) &\mapsto \frac{1}{2}(3-2)(3-1)+2 = 1+2 = 3 \\ (1,3) &\mapsto \frac{1}{2}(4-2)(4-1)+1 = 3+1 = 4 \\ (2,2) &\mapsto \frac{1}{2}(4-2)(4-1)+2 = 3+2 = 5 \\ (3,1) &\mapsto \frac{1}{2}(4-2)(4-1)+3 = 3+3 = 6 \\ (1,4) &\mapsto \frac{1}{2}(5-2)(5-1)+1 = 6+1 = 7 \text{ usw.} \end{aligned}$$

Da wir nur eine Bijektion von $\mathbb{N} \times \mathbb{N}$ auf $\mathbb{N}$ konstruiert haben, sind diese Mengen gleichmächtig.

□

Korollar 3.35.

$|\mathbb{Q}| = |\mathbb{N}|$, das heißt $\mathbb{Q}$ ist abzählbar.

Beweis:
Es ist $\mathbb{Q} = \{0\} \cup \{q \in \mathbb{Q} : q > 0\} \cup \{q \in \mathbb{Q} : q < 0\}$. Es gilt $\mathbb{N} \subseteq \{q \in \mathbb{Q} : q > 0\} = \left\{\frac{n}{m} : n, m \in \mathbb{N}\right\}$ und die letzte Menge kann als eine Teilmenge von $\mathbb{N} \times \mathbb{N}$ aufgefasst werden. Es folgt, dass $\aleph_0 \leq |\{q \in \mathbb{Q} : q > 0\}| \leq \aleph_0$. Also ist die Menge $\{q \in \mathbb{Q} : q > 0\} = \{q_1, q_2, \ldots\}$ abzählbar. Dann ist auch $\{q \in \mathbb{Q} : q < 0\} = \{-q_1, -q_2, -q_3, \ldots\}$ und schließlich ist auch

$$\mathbb{Q} = \{0, q_1, -q_1, q_2, -q_2, \ldots\}$$

abzählbar.

□

Es gibt aber unendliche Mengen, welche nicht abzählbar sind. So ist $(0, 1)$ überabzählbar (ohne Beweis). Die Mengen $(0, 1)$ und $\mathbb{R}$ sind gleichmächtig. In der Tat, $f : \mathbb{R} \to (0, 1),\ f(x) = \frac{1}{\pi}(\arctan x + \frac{\pi}{2})$ ist eine Bijektion.

Die Mächtigkeit von $\mathbb{R}$ ist $|\mathbb{R}| = c$, die *Mächtigkeit des Kontinuums*. Es stellt sich die Frage, ob c die nächste Kardinalzahl nach $\aleph_0$ ist: $c = \aleph_1$? Man kann zeigen, dass man das weder beweisen noch widerlegen kann. Die Aussage $c = \aleph_1$ ist die sogenannte *Kontinuumshypothese*. Sie ist unabhängig von den Axiomen der Mengenlehre. Es gibt Modelle der axiomatischen Mengenlehre mit $c = \aleph_1$ sowie andere Modelle mit $c \neq \aleph_1$.

Kapitel 4

Elementare Zahlentheorie

4.1 Teilbarkeit

Definition 4.1.

Seien $a, b \in \mathbb{Z}$. a *teilt* b genau dann, wenn es ein $n \in \mathbb{Z}$ gibt mit $n \cdot a = b$. In diesem Fall ist a ein *Teiler* von b. Wir schreiben $a|b$.

Beispiel 4.2.

1) $3|(-21)$, da $3 \cdot (-7) = -21$.
2) $2 \nmid 13$, das es keine Zahl $n \in \mathbb{Z}$ gibt, für die $13 = 2n$ gilt.
3) $\forall n \in \mathbb{Z} : 1|n$, da $1 \cdot n = n$.
4) $\forall n \in \mathbb{Z} : n|0$, da $n \cdot 0 = 0$.
5) $\forall n \in \mathbb{Z}\backslash\{0\} : 0 \nmid n$, da $0 \cdot k = 0 \neq n$ für alle $k \in \mathbb{Z}$.

Satz 4.3. *Teilbarkeitsregeln*

Es gelten folgende elementare Teilbarkeitsregeln. Für $a, b, c, p, q \in \mathbb{Z}$ gilt:

1) $a|a$ (jede Zahl ist Teiler von sich selbst).
2) $a|b \wedge b|c \Rightarrow a|c$.
3) $a|b \wedge a|c \Rightarrow a|(b + c)$.
4) $a|b \Rightarrow a|(b \cdot c)$.
5) $a|p \wedge b|q \Rightarrow (ab)|pq$.

Beweis:

1) $a \cdot 1 = a \Rightarrow a|a$.
2) $a|b \Rightarrow \exists n \in \mathbb{Z} : b = na$, $b|c \Rightarrow \exists m \in \mathbb{Z} : c = mb$. Dann gilt aber $c = mb = mna = (mn)a = ka$ mit $k = m \cdot n \in \mathbb{Z} \Rightarrow a|c$.
3) $a|b \Rightarrow \exists n \in \mathbb{Z} : b = na$, $a|c \Rightarrow \exists m \in \mathbb{Z} : c = ma$. Dann ist $b + c = na + ma = (n + m)a = ka$ mit $k \in \mathbb{Z} \Rightarrow a|(b + c)$.

Weitere Beweise folgen in der Übung.

□

Definition 4.4.

Für eine Zahl $a \in \mathbb{Z}$ ist ihre *Teilermenge* $T(a)$ die Menge aller Teiler von a:

$$T(a) = \{p \in \mathbb{Z} : p|a\}.$$

Beispiel 4.5. $T(2) = \{\pm 1, \pm 2\},\ T(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\},\ T(0) = \mathbb{Z}.$

Lemma 4.6.

Für $a, b \in \mathbb{Z}$ gilt:

(i) Ist $b \neq 0$, so folgt aus $a|b$, dass $|a| \leq |b|$.

(ii) $a|b \Leftrightarrow T(a) \subseteq T(b)$.

Beweis:

(i) Ist $b \neq 0$ und $a|b \Rightarrow\ \exists n \in \mathbb{N} : b = na$, wobei $n \neq 0$. Dann gilt

$$a = \frac{b}{n} \text{ und mit } |n| \geq 1 \text{ folgt } |a| = \frac{|b|}{|n|} \leq \frac{|b|}{|1|} = |b|.$$

(ii) $\Rightarrow$ Zu zeigen: $a|b \Rightarrow T(a) \subseteq T(b)$.

Sei $a|b$. Wir zeigen nun, dass $p \in T(a) \Rightarrow p \in T(b)$. Gilt $p|a$ und $a|b \Rightarrow p|b \Rightarrow p \in T(b)$ und die Behauptung folgt.

$\Leftarrow$ Wir beweisen diese Richtung durch Kontraposition. Zu zeigen: $a \nmid b \Rightarrow T(a) \not\subseteq T(b)$.

$a \nmid b \Rightarrow a \in T(a)$ und $a \notin T(b) \Rightarrow T(a) \not\subseteq T(b)$.

□

Korollar 4.7.

Ist $a \neq 0$, so ist die Menge $T(a)$ endlich.

Beweis:
$\forall p \in T(a) : |p| \leq |a|$. Es folgt, dass $T(a) \subseteq \{\pm 1, \pm 2, \ldots, \pm a\} \Rightarrow T(a)$ ist endlich.

□

Definition 4.8.

Seien $a, b \in \mathbb{Z}$ und nicht beide Null. Der *größte gemeinsame Teiler* von a und b ist die größte natürliche Zahl d mit $d|a$ und $d|b$. Wir schreiben $d = \mathrm{ggT}(a, b)$.

Bemerkung 4.9.

1) $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a) = \mathrm{ggT}(|a|, |b|)$.

2) Für $a \neq 0$ gilt $\mathrm{ggT}(a, 0) = |a|$, da $T(a) = \{\pm 1, \ldots, \pm a\}$ und $T(0) = \mathbb{Z}$.

3) Seien a und b beide Null, so ist jede ganze Zahl ein gemeinsamer Teiler von a und b. In diesem Fall kann man also nicht von einem größten gemeinsamen Teiler reden.

Satz 4.10. *Division mit Rest*

Seien $a \in \mathbb{Z},\ b \in \mathbb{N}$.

1) Es existieren eindeutig bestimme Zahlen $q, r \in \mathbb{Z}$, sodass

$$a = q \cdot b + r, \quad 0 \leq r < b. \tag{$*$}$$

2) q in der Darstellung $(*)$ ist die größte Zahl in $\mathbb{Z}$ mit $qb \leq a$.

3) $b|a \Leftrightarrow r = 0$.

Beweis:

1) Wir beweisen zunächst die Eindeutigkeit der Darstellung $(*)$. Es sei

$$a = q_1 b + r_1 = q_2 b + r_2 \text{ mit } q_1, q_2, r_1, r_2 \in \mathbb{Z},\ 0 \leq r_1 < b,\ 0 \leq r_2 < b.$$

Dann gilt

$$q_1 b - q_2 b = r_2 - r_1 \Leftrightarrow r_2 - r_1 = (q_1 - q_2)b,\ q_1 - q_2 \in \mathbb{Z} \Rightarrow b|(r_2 - r_1).$$

Für die beiden Reste r_1 und r_2 bekommen wir

$$0 \leq r_2 < b,\ -b < -r_1 \leq 0 \Rightarrow -b < r_2 - r_1 < b.$$

Insbesondere gilt $|r_2 - r_1| < b$. Aus $b|(r_2 - r_1)$ folgt dann $r_2 - r_1 = 0 \Rightarrow r_1 = r_2$. Dann ist aber auch $(q_1 - q_2)b = 0$ und wegen $b \neq 0$ muss auch $q_1 = q_2$ gelten. Die Darstellung ist also eindeutig.

2) Jetzt beweisen wir die Existenz und die Struktur der Darstellung $(*)$. Sei $q \in \mathbb{Z}$ die größte Zahl in $\mathbb{Z}$ mit $qb \leq a$.

1. Fall: $qb = a$ (äquivalent: $b|a$). Dann ist $a = qb + 0$ mit $r = 0$. Andererseits folgt aus $r = 0$, dass $a = qb$ und $b|a$.

2. Fall: $qb < a$, insbesondere $b \nmid a$. Definiere $r = a - qb > 0$. Dann gilt $a = qb + r$ und $r > 0$. Es bleibt zu zeigen, dass $r < b$, was wir mittels Widerspruchsbeweis zeigen. Dazu nehmen wir an, dass $r \geq b$. Dann ist $r = b + s$ mit $s \geq 0$ und es folgt

$$a = qb + r = qb + b + s = (q+1)b + s \Rightarrow (q+1)b = a - s \leq a,$$

was einen Widerspruch zur Wahl von q darstellt: q ist die größte Zahl in $\mathbb{Z}$ mit $qb \leq a$. Es gilt also $r < b$.

□

Beispiel 4.11.

1) Sei $a = 12,\ b = 5$. Dann ist $12 = 5 \cdot 2 + 2$, also $q = 2,\ r = 2$.

2) Sei $a = 15,\ b = 5$. Dann ist $15 = 5 \cdot 3 + 0$, also $q = 3,\ r = 0$, und $5|15$.

3) Sei $a = 3,\ b = 5$. Dann ist $3 = 5 \cdot 5 + 3$, also $q = 0,\ r = 3$.

4) Sei $a = -12,\ b = 5$. Dann ist $-12 = 5 \cdot (-3) + 3$, also $q = -3,\ r = 3$.

Lemma 4.12.

Seien $a, b \in \mathbb{N}$. Seien weiter $q, r \in \mathbb{N} \cup \{0\}$ die Zahlen mit

$$a = qb + r \text{ und } 0 \leq r < b.$$

Dann gilt: $\text{ggT}(a, b) = \text{ggT}(b, r)$.

Beweis:
Seien $d = \text{ggT}(a, b)$ und $t = \text{ggT}(b, r)$. Zu zeigen ist dann, dass $t = d$.
Da $d = \text{ggT}(a, b)$, gilt $d|a$ und $d|b$. Es ist

$$r = a - qb = a + (-q)b \text{ mit } -q \in \mathbb{Z}.$$

Weiter gilt $d|(-q)b$ und schließlich $d|r$. Somit ist d ein gemeinsamer Teiler von b und r und hiermit $d \leq \text{ggT}(b, r) = t$. Andererseits gilt für $t = \text{ggT}(b, r)$

$$t|b,\ t|r \Rightarrow t|qb \Rightarrow t|(qb + r) = a,$$

t ist also ein gemeinsamer Teiler von a und b und damit folgt $t \leq \text{ggT}(a, b) = d$. Wir haben also gezeigt, dass $d \leq t$ und $t \leq d$. Es folgt, dass $t = d$.

□

Wir beschäftigen uns nun mit dem *Euklidischen Algorithmus*. Dies ist ein Verfahren zur Bestimmung des $\text{ggT}(a, b)$ für gegebene $a, b \in \mathbb{N}$.

Satz 4.13. *Euklidischer Algorithmus*

Seien $a, b \in \mathbb{N}$ und sei $a \geq b$. Der $\text{ggT}(a, b)$ kann mittels wiederholter Division mit Rest nach folgendem Schema — dem sogenannten Euklidischen Algorithmus — berechnet werden:

$$\begin{aligned}
a &= q_1 b + r_1, && q_1, r_1 \in \mathbb{N} \cup \{0\}, && 0 \leq r_1 < b, \\
b &= q_2 r_1 + r_2, && q_2, r_2 \in \mathbb{N} \cup \{0\}, && 0 \leq r_2 < r_1, \\
r_1 &= q_3 r_2 + r_3, && q_3, r_3 \in \mathbb{N} \cup \{0\}, && 0 \leq r_3 < r_2 \quad \text{usw.}
\end{aligned}$$

Der Algorithmus bricht nach endlich vielen Schritten ab: Es gibt ein kleinstes n mit $r_{n+1} = 0$, also

$$r_{n-1} = q_{n+1} r_n, \quad q_{n+1} \in \mathbb{N} \cup \{0\}, \quad r_{n+1} = 0.$$

Dann gilt $\text{ggT}(a, b) = r_n$.

Beispiel 4.14. Gesucht ist der $\text{ggT}(682, 418)$. Wir wenden den Euklidischen Algorithmus wie folgt an

$$\begin{aligned}
682 &= 1 \cdot 418 + 264,\ q_1 = 1,\ r_1 = 264 \\
418 &= 1 \cdot 264 + 154,\ q_2 = 1,\ r_2 = 154 \\
264 &= 1 \cdot 154 + 110,\ q_3 = 1,\ r_3 = 110 \\
154 &= 1 \cdot 110 + 44,\ q_4 = 1,\ r_4 = 44 \\
110 &= 2 \cdot 44 + 22,\ q_5 = 2,\ r_5 = 22 \\
44 &= 2 \cdot 22 + 0,\ q_6 = 2,\ r_6 = 0
\end{aligned}$$

Damit ist $\text{ggT}(682, 418) = 22$.

Bemerkung 4.15. Da $\text{ggT}(a, b) = \text{ggT}(|a|, |b|)$ und $\text{ggT}(a, 0) = |a|$, genügt es, $a, b \in \mathbb{N}$ zu betrachten.

Beweis des Satzes:

1) Der Algorithmus endet in endlich vielen Schritten, da in jedem Schritt $r_{i+1} < r_i$ gilt.

2) Nach dem vorherigen Lemma gilt:

$$\text{ggT}(a, b) = \text{ggT}(b, r_1) = \text{ggT}(r_1, r_2) = \ldots = \text{ggT}(r_n, r_{n+1}).$$

Da aber $r_{n+1} = 0$ ist, gilt $\text{ggT}(a, b) = \text{ggT}(r_n, 0) = r_n$.

□

Definition 4.16.

Zwei Zahlen $a, b \in \mathbb{Z}$ heißen *teilerfremd* (*relativ prim*), wenn $\text{ggT}(a, b) = 1$.

Satz 4.17. *Lemma von Bezout*

Seien $a, b \in \mathbb{N}$. Dann gibt es $k, m \in \mathbb{Z}$, sodass $\text{ggT}(a, b) = ka + mb$.

Beweis:
Wir betrachten die Zeilen des Euklidischen Algorithmus von unten nach oben. Die vorletzte Zeile lautet:

$$\begin{aligned} r_{n-2} &= q_n r_{n-1} + r_n \quad \text{und} \quad r_n = \text{ggT}(a, b). \\ \Rightarrow r_n &= r_{n-2} - q_n r_{n-1}. \quad (*) \end{aligned}$$

Die vorvorletzte Zeile liefert

$$\begin{aligned} r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\ \Rightarrow r_{n-1} &= r_{n-3} - q_{n-1} r_{n-2}, \text{ eingesetzt in } (*) \text{ ergibt} \\ r_n &= r_{n-2} - q_n(r_n - 3 - q_{n-1} r_{n-2}) \\ &= (1 + q_n q_{n-1}) r_{n-2} - q_n r_{n-3}. \end{aligned}$$

Es gilt also

$$r_n = m_{n-2} r_{n-2} + k_{n-2} r_{n-3} \quad (**) \quad \text{mit } m_{n-2}, k_{n-2} \in \mathbb{Z}.$$

Mit der nächsten Zeile erhalten wir

$$\begin{aligned} r_{n-4} &= q_{n-2} r_{n-3} + r_{n-2} \\ \Rightarrow r_{n-2} &= r_{n-4} - q_{n-2} r_{n-3}, \text{ eingesetzt in } (**) \text{ ergibt} \\ r_n &= m_{n-3} r_{n-3} + k_{n-3} r_{n-4} \quad \text{mit } m_{n-3}, k_{n-3} \in \mathbb{Z}. \end{aligned}$$

Fahren wir so fort, erhalten wir $r_n = m_0 b + k_0 a$ mit $m_0, k_0 \in \mathbb{Z}$, was der gewünschten Darstellung entspricht.

□

4.2 Primzahlen

Definition 4.18.

Eine *Primzahl* ist eine natürliche Zahl, die durch genau zwei natürliche Zahlen teilbar ist.

Beispiel 4.19. Exemplarisch listen wir die Primzahlen ≤ 100 auf. Diese lauten:
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$.

Satz 4.20. *Satz von Euklid*

Es gibt unendlich viele Primzahlen.

Diesen Satz haben wir bereits in Kapitel „Logik und Beweise“ bewiesen.

Lemma 4.21. *Lemma von Euklid*

Seien $a, b \in \mathbb{N}$ und p eine Primzahl. Es gilt:

$$p|ab \Rightarrow p|a \text{ oder } p|b.$$

Beweis:
Es gelte also $p|ab$.

1. Fall: Gilt $p|a$, so ist die Aussage beweisen.

2. Fall: Gilt $p \nmid a$, so müssen wir zeigen, dass $p|b$ gilt. Es ist $T(p) = \{\pm 1, \pm p\}$ und $p \nmid a \Rightarrow \text{ggT}(p, a) = 1$. Nach dem Lemma von Bezout gilt:

$$\text{ggT}(p, a) = 1 = np + ma \text{ mit } n, m \in \mathbb{Z}.$$

Multiplizieren wir diese Gleichung mit b, so erhalten wir

$$b = npb + mab.$$

Da $p|ab \Rightarrow \ \exists k \in \mathbb{Z}$ mit $ab = kp$. Dann gilt

$$b = npb + mkp = p(nb + mk) = p\ell \text{ mit } \ell \in \mathbb{Z} \Rightarrow p|b,$$

was zu zeigen war.

□

Satz 4.22. *Charakterisierung der Primzahlen*

Eine natürliche Zahl $p > 1$ ist genau dann eine Primzahl, wenn

$$\forall a, b \in \mathbb{N}\backslash\{1\} : (p|ab \Rightarrow p|a \vee p|b).$$

Beweis:
Die direkte Richtung folgt aus dem Lemma von Euklid. Wir beweisen nun die umgekehrte Richtung. Es gelte:

$$\forall a, b \in \mathbb{N}\backslash\{1\} : (p|ab \Rightarrow p|a \vee p|b).$$

Zu zeigen: p ist eine Primzahl. Dazu nehmen wir an, dass p keine Primzahl ist. Dann gibt es $r, s \in \mathbb{N},\ 1 < r, s < p$, sodass $p = rs$. Für das Produkt rs gilt:

$$p|rs, \text{ aber } p \nmid r \text{ (weil } r < p) \text{ und } p \nmid s \text{ (weil } s < p).$$

Dies ist ein Widerspruch zur Voraussetzung, p ist also eine Primzahl.

□

Bemerkung 4.23. Warum haben wir in der Formulierung $\forall a, b \in \mathbb{N}\backslash\{1\}$ die Zahl 1 ausgeschlossen? Sei z.B. $a = 1$. Die Implikation

$$p|1 \cdot b \Rightarrow p|b \quad \text{ gilt für alle } p,$$

p braucht also nicht Primzahl zu sein.

Satz 4.24. *Fundamentalsatz der Arithmetik*

Sei $n > 1$ eine natürliche Zahl. Dann kann n als Produkt endlich vieler Primzahlen dargestellt werden. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Faktoren.

Bemerkung 4.25. Diese Darstellung heißt *Primfaktorenzerlegung* (oder *Primfaktorzerlegung*).

Beweis:

1) Zunächst beweisen wir die Existenz der Zerlegung.

   1. Fall: n ist eine Primzahl. Dann ist $n = n$ eine Primfaktorzerlegung von n (mit einem Faktor).
   2. Fall: n ist keine Primzahl. Widerspruchsbeweis: Wir nehmen an, dass es Zahlen gibt, die nicht als Produkt von Primzahlen dargestellt werden können. Sei $n_0 \in \mathbb{N}$ die kleinste Zahl mit dieser Eigenschaft. n_0 ist keine Primzahl (sonst wäre $n_0 = n_0$ eine Primfaktorzerlegung). n_0 ist also keine Primzahl $\Rightarrow n_0 = ab$ mit $a, b \in \mathbb{N},\ 1 < a, b < n_0$. Die Zahlen a und b können aber als Produkte von Primzahlen dargestellt werden, da sie kleiner als n_0 sind und n_0 der Annahme nach die kleinste Zahl mit dieser Eigenschaft ist. Es gilt also

   $$a = p_1 \dots p_s \text{ und } b = p_{s+1} \dots p_k$$

   für gewisse Primzahlen $p_1, \dots, p_k$. Dann gilt aber

   $$n_0 = ab = p_1 \dots p_s p_{s+1} \dots p_k.$$

   Somit kann n_0 also als Produkt von Primzahlen dargestellt werden. Widerspruch. Jede Zahl kann also als Produkt von Primzahlen dargestellt werden.

2) Beweisen wir nun die Eindeutigkeit der Zerlegung.

   1. Fall: n ist eine Primzahl. Dann ist $n = n$ und es gibt keine weitere Primfaktorzerlegung, da n durch keine weiteren Primzahlen teilbar ist.
   2. Fall: n ist keine Primzahl. Widerspruchsbeweis: Wir nehmen an, dass es Zahlen gibt, die (mindestens) zwei unterschiedliche Primfaktorenzerlegungen haben. Sei $n_0 \in \mathbb{N}$ die kleinste Zahl mit dieser Eigenschaft. Seien nun $n_0 = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ zwei verschiedene Darstellungen der Zahl n_0, wobei wir die Faktoren der Größe nach geordnet haben: $p_1 \leq p_2 \leq \dots \leq p_r,\ q_1 \leq q_2 \leq \dots \leq q_s$. Dann gilt $p_1 \neq q_1$, da wir ansonsten für $a = \frac{n_0}{p_1} < n_0$ zwei verschiedene Darstellungen $a = p_2 \dots p_r = q_2 \dots q_s$ hätten. Dies widerspricht der Tatsache, dass n_0 die kleinste Zahl mit dieser Eigenschaft ist. Es gilt also $p_1 \neq q_1$. Dann ist

   $$n_0 = p_1 a = q_1 b \text{ mit } a, b \in \mathbb{N},\ a \neq b,\ a, b < n_0.$$

   Es gilt weiter

   $$p_1 | n_0 \Rightarrow p_1 | q_1 b \Rightarrow p_1 | q_1 \text{ oder } p_1 | b.$$

   Da aber q_1 eine Primzahl ist und $q_1 \neq p_1$, kann p_1 kein Teiler von q_1 sein $\Rightarrow p_1 | b$. Damit ist p_1 ein gemeinsamer Faktor in den beiden Zerlegungen

   $$n_0 = p_1 \dots p_r = q_1 \dots q_s,$$

   das heißt $\exists i, 1 < i \leq s$, mit $p_1 = q_i$. Dann gilt für $a = \frac{n_0}{p_1}$:

   $$a = p_2 \dots p_r = q_1 \dots q_{i-1} q_{i+1} \dots q_s.$$

   Da die Faktoren der Größe nach geordnet sind und $q_1 \neq p_1$, gilt $q_1 < q_i = p_1$, aber auch $p_2 \geq p_1$. Es gilt also $p_2 \neq q_1$. Die Zahl a hat also zwei verschiedene Primfaktorenzerlegungen und $a = \frac{n_0}{p_1} < n_0$, was unserer Annahme, dass n_0 die kleinste Zahl mit dieser Eigenschaft ist, widerspricht. Die Zerlegung ist also eindeutig.

□

Beispiel 4.26. Betrachten wir exemplarisch einige Primfaktorenzerlegungen.

1) $52 = 2 \cdot 26,\ 26 = 2 \cdot 13,\ 13$ ist eine Primzahl, also $52 = 2 \cdot 2 \cdot 2 \cdot 13$.

2) $2520 = 2 \cdot 1260,\ 1260 = 2 \cdot 630,\ 630 = 2 \cdot 315$. 315 ist nicht mehr durch 2 teilbar, wir testen also 3. Es gilt $315 = 3 \cdot 105,\ 105 = 3 \cdot 35$. 35 ist nicht mehr durch 3 teilbar, wir testen also 5. $35 = 5 \cdot 7,\ 7$ ist eine Primzahl. Es folgt also $2520 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7$.

Bemerkung 4.27. Seien $a = \prod_{j=1}^{M} p_j^{k_j}$ und $b = \prod_{j=1}^{M} p_j^{\ell_j}$ Zerlegungen von a und b, wobei $p_1, \ldots, p_M$ alle Primzahlen sind, die in den Primfaktorenzerlegungen von a und b vorkommen, mit passenden Potenzen (die Exponenten k_j, ℓ_j können auch 0 sein; die Zerlegungen oben bestehen also aus Primfaktoren und Faktoren 1). Dann gilt:

$$\mathrm{ggT}(a, b) = \prod_{j=1}^{M} p_j^{\min(k_j, \ell_j)}.$$

Beispiel 4.28. Wie wir wissen ist $\mathrm{ggT}(682, 418) = 22$. Die jeweiligen Primfaktorenzerlegungen lauten:

$$682 = 2 \cdot 341 = 2 \cdot 11 \cdot 31 \text{ und } 418 = 2 \cdot 209 = 2 \cdot 11 \cdot 19$$
$$\text{also folgt } \mathrm{ggT}(682, 418) = 2 \cdot 11 = 22.$$

4.3 Kongruenz modulo m und Restklassen

4.3.1 Relationen

Betrachten wir zunächst ein einführendes Beispiel.

Beispiel 4.29. Sei M die Menge aller im Hörsaal anwesenden Studierenden. Man kann Elemente dieser Menge miteinander in Beziehung setzen, wie zum Beispiel:

1) „x und y sind in der gleichen Übungsgruppe.“

2) „x und y kommen aus denselbem Ort.“

3) „x ist jünger als y.“

4) „x hat eine längere Anreise als y.“

Solche Beziehungen heißen Relationen.

Definition 4.30.

Sei M eine Menge. Eine *Relation* R auf M ist eine Teilmenge des kartesischen Produktes $M \times M$:

$$R \subseteq M \times M.$$

Für zwei Elemente $x, y \in M$ sagt man „x steht in Relation zu y“, falls $(x, y) \in R$ gilt. Man schreibt in diesem Fall xRy, obwohl für Relationen in der Regel andere Symbole benutzt werden:

$$<,\ \leq,\ =,\ \subseteq,\ \sim,\ \ll \text{ usw.}$$

Beispiel 4.31.

1) Wir betrachten $\mathbb{R}$ mit der Relation $<$ „kleiner“. Dann ist $(x, y) \in R$, wenn $x < y$, d.h.

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x < y\}.$$

Aus $(x, y) \in R$ folgt nicht $(y, x) \in R$, da zum Beispiel $2 < 3$ und $(2, 3) \in R$, aber $(3, 2) \notin R$.

2) Die Menge aller Teilmengen einer Grundmenge G mit der Relation $\subseteq$: $A \subseteq B$, wenn A eine Teilmenge von B ist, d.h.

$$R = \{(A, B) \in P(G) \times P(G) : A \subseteq B\}.$$

3) Die Menge aller endlichen Teilmengen von $\mathbb{N}$ mit der Relation $\approx$: $A \approx B$, wenn A und B gleichmächtig sind (die gleiche Anzahl an Elementen haben).

4) Die Menge aller im Hörsaal anwesenden Studierenden mit der folgenden Relation: $x = y$, wenn x und y den gleichen Vornamen haben.

Definition 4.32. Eigenschaften von Relationen

Sei M eine Menge und sei R eine Relation auf M.

1) R heißt *transitiv*, wenn für alle $x, y, z \in M$ gilt: $xRy \wedge yRz \Rightarrow xRz$.

2) R heißt *reflexiv*, wenn für alle $x \in M$ gilt: xRx.

3) R heißt *symmetrisch*, wenn für alle $x, y \in M$ gilt: $xRy \Rightarrow yRx$.

4) R heißt *antisymmetrisch*, wenn für alle $x, y \in M$ gilt: $xRy \wedge yRx \Rightarrow x = y$.

Beispiel 4.33. In den oben betrachteten Beispielen sind 1), 2), 3), 4) transitiv; 2), 3), 4) reflexiv; 1) nicht reflexiv; 3), 4) symmetrisch; 1), 2) nicht symmetrisch; 2) antisymmetrisch; 3), 4) nicht antisymmetrisch. Strikt gesagt ist die Relation im Beispiel 1) antisymmetrisch, der Fall $x < y \wedge y < x$ kommt aber nicht vor.

Definition 4.34.

Eine Relation R auf einer Menge M heißt *Äquivalenzrelation*, wenn R transitiv, reflexiv und symmetrisch ist.

Beispiel 4.35. Die Beispiele 3) und 4) sind Äquivalenzrelationen. Ein weiteres Beispiel für eine Äquivalenzrelation:

5) Sei $M = \mathbb{Z}$ und $x \equiv y$, wenn $x - y$ gerade ist.
Wir zeigen, dass das eine Äquivalenzrelation ist.
Transitivität: Zu zeigen ist $x \equiv y \wedge y \equiv z \Rightarrow x \equiv z$. $x - y$ ist gerade und $y - z$ ist gerade $\Rightarrow x - z = (x - y) + (y - z)$ ist gerade $\Rightarrow x \equiv z$.
Reflexivität: $x \equiv x$, da $x - x = 0$ gerade ist.
Symmetrie: $x \equiv y \Rightarrow x - y$ ist gerade $\Rightarrow y - x = -(x - y)$ ist gerade $\Rightarrow y \equiv x$.

Eine Äquivalenzrelation kann dazu benutzt werden, Elemente einer Menge in Gruppen einzuteilen, zum Beispiel alle Studierenden, die in derselben Übungsgruppe sind.

Definition 4.36.

Seien M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Sei $a \in M$. Die *Äquivalenzklasse* von a ist wie folgt definiert:

$$[a] = \{b \in M : b \sim a\}.$$

Jedes Element $b \in [a]$ heißt *Repräsentant* der Äquivalenzklasse $[a]$. Weitere Bezeichnungen für die Äquivalenzlklasse sind C_a, $\overline{a}$.

Beispiel 4.37. Wir beziehen uns auf Beispiel 3). Hier bestehen die Äquivalenzklassen aus Mengen, die gleich viele Elemente haben, z.B.

$$[\{1\}] = \{\{1\}, \{2\}, \{3\}, \ldots\},$$
$$[\{1,2\}] = \{\{1,2\}, \{1,3\}, \ldots, \{2,3\}, \{2,4\}, \ldots\} \quad \text{usw.}$$

Beim vierten Beispiel bestehen die Äquivalenzklassen aus Studierenden, die den gleichen Vornamen haben.

Lemma 4.38.

Seien M eine Menge und $\sim$ eine Äquivalenzrelation auf M, sowie $a, b \in M$. Dann gilt

$$a \sim b \Rightarrow [a] = [b].$$

Beweis:
Sei $y \in [b]$. Da $y \sim b$ und $b \sim a \Rightarrow y \sim a \Rightarrow y \in [a]$. Wir haben also gezeigt, dass $[b] \subseteq [a]$. Durch Vertauschen von a und b erhalten wir sofort $[a] \subseteq [b]$ und somit insgesamt $[a] = [b]$.

□

Satz 4.39.

Seien M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Zwei Äquivalenzklassen $[a]$ und $[b]$ sind entweder gleich oder elementfremd:

$$[a] \cap [b] \neq \emptyset \Leftrightarrow [a] = [b].$$

Beweis:
Da wir hier eine Äquivalenz zeigen wollen, beginnen wir mit der ersten Implikation.
$\Leftarrow$ Gilt $[a] = [b]$, so ist $[a] \cap [b] = [a] \neq \emptyset$, da diese Klasse wegen $a \in [a]$ nicht leer ist.
$\Rightarrow$ Es gelte nun $[a] \cap [b] \neq \emptyset$. Somit existiert ein $x \in [a] \cap [b]$. Wir haben

$$x \in [a] \Rightarrow x \sim a, \; x \in [b] \Rightarrow x \sim b.$$

Wegen der Symmetrie folgt $x \sim b \Rightarrow b \sim x$ und aufgrund der Transitivität gilt $b \sim x, \; x \sim a \Rightarrow b \sim a$. Nach dem vorherigen Lemma gilt dann $[a] = [b]$.

□

Wir sehen, dass die Äquivalenzklassen eine Partition auf M bilden.

Satz 4.40.

Jede Äquivalenzrelation $\sim$ auf einer Menge M definiert eine Partition von M. Umgekehrt definiert jede Partition $\{U_i\}_{i \in I}$ einer Menge M eine Äquivalenzrelation auf M:

$$x \sim y, \text{ wenn } \exists i \in I : x \in U_i \text{ und } y \in U_i.$$

Beweis:
Da $\forall x \in M : x \in [x]$, ergibt die Vereinigung aller Äquivalenzklassen die Menge M. Die Äquivalenzklassen sind entweder gleich oder elementfremd. Folglich bilden sie eine Partition.

Nun sei $\{U_i\}_{i\in I}$ eine Partition. Wir zeigen, dass die oben definierte Relation eine Äquivalenzrelation ist. Als erstes zeigen wir die Transitivität: $x \sim y$ und $y \sim z$.

$$x \sim y \Rightarrow \ \exists i \in I : x \in U_i \text{ und } y \in U_i.$$
$$y \sim z \Rightarrow \ \exists j \in I : y \in U_j \text{ und } z \in U_j.$$

Also insbesondere $y \in U_i \cap U_j$ und $U_i \cap U_j \neq \emptyset \Rightarrow U_i = U_j \Rightarrow i = j$. Es folgt, dass $z \in U_i \Rightarrow x \sim z$. Die Eigenschaften der Reflexivität $x \sim x$ und der Symmetrie $x \sim y \Rightarrow y \sim x$ sind offensichtlich.

□

Definition 4.41.

Seien M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Die *Quotientenmenge* (die *Faktormenge*) $M/_\sim$ ist die Menge aller Äquivalenzklassen bezüglich $\sim$ (Man liest: „M modulo Tilde“).

4.3.2 Kongruenz modulo m und Restklassen

Definition 4.42.

Sei $m \in \mathbb{N},\ m \geq 2$. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen *kongruent modulo* m , wenn $m|(a-b)$.
Wir schreiben dann: $a \equiv b \mod m,\ a \equiv b(m)$ oder $a \sim_m b$.

Satz 4.43.

Kongruenz modulo m ist eine Äquivalenzrelation.

Beweis:
Transitivität: Es gelte $a \sim_m b,\ b \sim_m c$. Zu zeigen: $a \sim_m c$. Nach Annahme gilt $m|(a-b)$ und $m|(b-c) \Rightarrow m|(a-c)$, da $a - c = (a-b) + (b-c) \Rightarrow a \sim_m c$.
Reflexivität: $a \sim_m a$, da $a - a = 0$ und $m|0$.
Symmetrie: Es gelte $a \sim_m b$. Zu zeigen: $b \sim_m a$. Es gilt $m|(a-b)$ und $b - a = -(a-b) \Rightarrow m|(b-a) \Rightarrow b \sim_m a$.

□

Bemerkung 4.44. $a \equiv b \mod m$ bedeutet, dass a und b bei Division durch m denselben Rest haben. Dies wollen wir noch kurz verifizieren. Sei $a = qm + r$ mit $q \in \mathbb{Z},\ r \in \mathbb{N} \cup \{0\},\ 0 \leq r < m$.

$$m|(a-b) \Rightarrow \ \exists k \in \mathbb{Z} : a - b = mk.$$

Daraus folgt

$$b = a - mk = qm + r - mk = (q-k)m + r,\ q-k \in \mathbb{Z},\ r \in \mathbb{N} \cup \{0\},\ 0 \leq r < m.$$

Die Darstellung bei der Division mit Rest ist eindeutig. Teilen wir also b durch m, erhalten wir denselben Rest r. Ergeben umgekehrt die Zahlen a und b bei der Division durch m denselben Rest r, so gilt

$$a = qm + r,\ b = \ell m + r \text{ mit } q, \ell \in \mathbb{Z} \Rightarrow a - b = (q-\ell)m,\ q - \ell \in \mathbb{Z} \Rightarrow m|(a-b).$$

Beispiel 4.45. $4 \equiv 2 \mod 2,\ 16 \equiv 8 \mod 2,\ 5 \equiv 3 \mod 2,\ 27 \equiv 9 \mod 2,\ 7 \not\equiv 4 \mod 2,$
$15 \equiv 9 \mod 3,\ 16 \equiv 4 \mod 3,\ 17 \equiv 2 \mod 3,\ 7 \not\equiv 2 \mod 3.$

Definition 4.46.

Sei $m \in \mathbb{N},\ m \geq 2$. Die Faktormenge $\mathbb{Z}/_{\sim_m}$ bezeichnet man mit $\mathbb{Z}_m$. Die Äquivalenzklassen heißen *Restklassen modulo m* .

Es gibt genau m Restklassen modulo m: Sie bestehen aus den Zahlen, die beim Teilen durch m den Rest $0, 1, 2, \ldots, m-2$ bzw. $m-1$ ergeben.

Beispiel 4.47.

1) $m = 2$:
$[0]_2 = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = \{2n : n \in \mathbb{Z}\}$.
$[1]_2 = \{\ldots, -3, -1, 1, 3, \ldots\} = \{2n+1 : n \in \mathbb{Z}\}$, also $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$.

2) $m = 3$:
$[0]_3 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} = \{3n : n \in \mathbb{Z}\}$.
$[1]_3 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} = \{3n+1 : n \in \mathbb{Z}\}$.
$[2]_3 = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\} = \{3n+2 : n \in \mathbb{Z}\}$, also $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$.

Bemerkung 4.48. $[0]_m$ besteht aus allen Zahlen, die durch m teilbar sind.

Bemerkung 4.49. Es gilt

$$\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}.$$

Definition 4.50. Rechnen mit Restklassen

Sei $m \in \mathbb{N},\ m \geq 2$. Auf der Menge $\mathbb{Z}_m$ der Restklassen definiert man:

(i) Die *Addition von Restklassen*: $[a]_m + [b]_m = [a+b]_m$.

(ii) Die *Multiplikation von Restklassen*: $[a]_m \cdot [b]_m = [a \cdot b]_m$.

Beispiel 4.51.

1) $[1]_2 + [1]_2 = [2]_2 = [0]_2$ beziehungsweise $1 + 1 \equiv 0 \mod 2$.

2) $[3]_8 + [7]_8 = [10]_8 = [2]_8$ beziehungsweise $3 + 7 \equiv 2 \mod 8$.

3) $[1]_2 \cdot [1]_2 = [1]_2$ beziehungsweise $1 \cdot 1 \equiv 1 \mod 2$.

4) $[3]_8 \cdot [7]_8 = [21]_8 = [5]_8$ beziehungsweise $3 \cdot 7 \equiv 5 \mod 8$.

5) $[2]_8 \cdot [4]_8 = [8]_8 = [0]_8$ beziehungsweise $2 \cdot 4 \equiv 0 \mod 8$.

Bemerkung 4.52. Die Addition und die Multiplikation von Restklassen sind *wohldefiniert*. „Wohldefiniert“ bedeutet, dass die Objekte eindeutig definiert sind. In unserem Fall haben wir die Operationen mithilfe von Repräsentanten definiert. Man muss also zeigen, dass die Operationen von der Wahl des Repräsentanten unabhängig sind.

1) Addition: Seien $a, a' \in [a]_m,\ b, b' \in [b]_m$. Zu zeigen: $[a'+b']_m = [a+b]_m$.

$$\begin{aligned} m|(a'-a) \Rightarrow a'-a &= km,\ k \in \mathbb{Z} \\ \Rightarrow a' &= a+km,\ k \in \mathbb{Z}, \\ m|(b'-b) \Rightarrow b'-b &= \ell m,\ \ell \in \mathbb{Z} \\ \Rightarrow b' &= b+\ell m,\ \ell \in \mathbb{Z}. \end{aligned}$$

Dann aber gilt $a'+b' = a+b+(k+\ell)m \sim_m a+b$. Daraus folgt, dass $[a'+b']_m = [a+b]_m$.

2) Multiplikation: Zu zeigen: $[a' \cdot b']_m = [a \cdot b]_m$.

$$\begin{aligned} a' \cdot b' =& (a + km) \cdot (b + \ell m) \\ =& ab + a\ell m + bkm + k\ell mm \\ =& ab + (a\ell + bk + k\ell m)m \sim_m ab. \end{aligned}$$

Daraus folgt, dass $[a' \cdot b']_m = [a \cdot b]_m$.

Damit ist die Wohldefiniertheit gezeigt.

Bemerkung 4.53. Addition modulo 12 kennen wir alle aus dem täglichen Leben: die Uhr. Auch $\mathbb{Z}_m$ mit $m \neq 12$ kann man als eine Uhr darstellen.

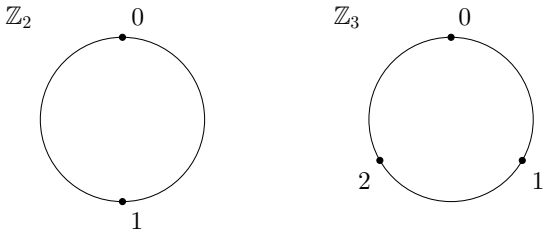

Abbildung 4.1: Exemplarische Darstellung von $\mathbb{Z}_2$ und $\mathbb{Z}_3$.

Kapitel 5

Ungleichungen und Betrag

5.1 Ordnungsrelationen

Definition 5.1.

Eine Relation $\preceq$ auf einer Menge M heißt *Ordnungsrelation*, falls sie

1) transitiv: $x \preceq y \wedge y \preceq z \Rightarrow x \preceq z$,

2) reflexiv: $x \preceq x$ und

3) antisymmetrisch: $x \preceq y \wedge y \preceq x \Rightarrow x = y$

ist. Das Paar $(M, \preceq)$ heißt *geordnete Menge*.

Beispiel 5.2.

1) $(\mathbb{R}, \leq)$.

2) Alle Teilmengen einer Grundmenge G mit der Relation $\subseteq$: $(P(G), \subseteq)$.

3) $(\mathbb{R}^2, \leq)$, wobei $\leq$ folgendermaßen definiert ist:

$$(x, y) \leq (u, v), \text{ wenn } x \leq u \text{ und } y \leq v.$$

4) $(\mathbb{R}^2, \leq_{\text{lex}})$, wobei $\leq_{\text{lex}}$ die lexikographische Ordnung ist:

$$(x, y) \leq_{\text{lex}} (u, v), \text{ wenn } (x \leq u \wedge x \neq u) \text{ oder } (x = u \wedge y \leq v).$$

5) $(\mathbb{N}, |)$ mit der Relation „teilbar“. (Machen Sie sich klar, dass $|$ aud $\mathbb{N}$ tatsächlich eine Ordnungsrelation ist!)

Bemerkung 5.3. Wir schreiben

1) $x \succeq y$, wenn $y \preceq x$,

2) $x \prec y$, wenn $x \preceq y$ und $x \neq y$, sowie

3) $x \succ y$, wenn $y \prec x$.

Definition 5.4.

Gilt für zwei Elemente $a, b \in M$ $a \preceq b$ oder $b \preceq a$, so heißen a und b *vergleichbar* (bezüglich $\preceq$). Andernfalls heißen sie *nicht vergleichbar*.

Definition 5.5.

Eine Ordnungsrelation $\preceq$ heißt *Totalordnung* auf M, wenn zwei beliebige Elemente von M vergleichbar sind. Das Paar $(M, \preceq)$ heißt in diesem Fall *total geordnete Menge*.

Beispiel 5.6.

1) $(\mathbb{R}, \leq)$ ist eine total geordnete Menge.

2) $(P(G), \subseteq)$ ist nicht total geordnet, wenn G aus mehr als einem Element besteht. Sei dazu $G = \{1, 2, 3\}$. Dann sind beispielweise $\{1\}$ und $\{1, 2\}$ vergleichbar: $\{1\} \subseteq \{1, 2\}$, aber $\{1\}$ und $\{2, 3\}$ sind nicht vergleichbar: $\{1\} \not\subseteq \{2, 3\}$ und $\{2, 3\} \not\subseteq \{1\}$.

3) $(\mathbb{R}^2, \leq)$ ist nicht total geordnet, da $(1, 2) \leq (2, 3)$, aber $(1, 2)$ und $(2, 1)$ nicht vergleichbar sind.

4) $(\mathbb{R}^2, \leq_{\text{lex}})$ ist total geordnet.

5) $(\mathbb{N}, |)$ ist nicht total geordnet.

5.2 $\mathbb{R}$ als geordneter Körper

Satz 5.7. *Körperaxiome*

Die Menge $\mathbb{R}$ der reellen Zahlen mit den Operationen $+$ und $\cdot$ erfüllt folgende Eigenschaften:

(K1) $\forall a, b \in \mathbb{R} : a + b = b + a$ (Kommutativität der Addition).

(K2) $\forall a, b, c \in \mathbb{R} : (a + b) + c = a + (b + c)$ (Assoziativität der Addition).

(K3) $\exists 0 \in \mathbb{R} : \forall a \in \mathbb{R} : a + 0 = a$ (Existenz des neutralen Elements bezüglich der Addition — des Nullelements).

(K4) $\forall a \in \mathbb{R} : \exists (-a) \in \mathbb{R} : a + (-a) = 0$ (Existenz des inversen Elements bezüglich der Addition).

(K5) $\forall a, b \in \mathbb{R} : a \cdot b = b \cdot a$ (Kommutativität der Multiplikation).

(K6) $\forall a, b, c \in \mathbb{R} : (ab)c = a(bc)$ (Assoziativität der Multiplikation).

(K7) $\exists 1 \in \mathbb{R} : 1 \neq 0 \wedge \ \forall a \in \mathbb{R} : a \cdot 1 = a$ (Existenz des neutralen Elements bezüglich der Multiplikation — des Einselements).

(K8) $\forall a \in \mathbb{R} \backslash \{0\} : \exists a^{-1} : a \cdot a^{-1} = 1$ (Existenz des inversen Elements bezüglich der Multiplikation).

(K9) $\forall a, b, c \in \mathbb{R} : a(b + c) = ab + ac$ (Distributivität).

Definition 5.8.

Eine nichtleere Menge K mit zwei Verknüpfungen $+, \cdot : K \times K \to K$, für die die Eigenschaften (K1)-(K9) gelten, heißt *Körper*. Die Eigenschaften (K1)-(K9) heißen *Körperaxiome*.

Bemerkung 5.9.

1) Die *Subtraktion* ist definiert als die Addition des inversen Elements bezüglich der Addition: $a - b = a + (-b)$.

2) Die *Division* ist definiert als die Multiplikation mit dem inversen Element bezüglich der Multiplikation: $\frac{a}{b} = a \cdot b^{-1}, \ b \neq 0$.

Alle weiteren Rechenregeln folgen aus Körperaxiomen (K1)-(K9). Im Satz unten beweisen wir eine Auswahl von weiteren Rechenregeln, welche wir insbesondere beim Arbeiten mit Ungleichungen benötigen werden.

Satz 5.10.

1) Die neutralen Elemente bzgl. der Addition und bzgl. der Multiplikation sind eindeutig bestimmt.
2) Die inversen Elemente bzgl. der Addition und bzgl. der Multiplikation sind eindeutig bestimmt.
3) Es gilt $-(-a) = a$ und für $a \neq 0$ gilt $(a^{-1})^{-1} = a$ (doppelte Inversion).
4) Es gilt $-(a+b) = (-a) + (-b)$ und für $a, b \neq 0$ gilt $(ab)^{-1} = a^{-1}b^{-1}$.
5) Es gilt $a \cdot 0 = 0$.
6) Aus $ab = 0$ folgt $a = 0$ oder $b = 0$. Insbesondere gilt für $a, b \neq 0$ auch $ab \neq 0$.
7) Es gilt $-(ab) = (-a)b = a(-b)$ und $(-a)(-b) = ab$.

Beweis:

Die Regeln 1) bis 4) beweisen wir nur für die Addition; die Beweisführung für die Multiplikation ist identisch.

1) Sei $0'$ ein weiteres Nullelement. Dann aber gilt $0' = 0' + 0 = 0$.
2) Sei $\tilde{a}$ ein weiteres inverses Element von a. Dann aber gilt $\tilde{a} = \tilde{a}+0 = \tilde{a}+a+(-a) = 0+(-a) = -a$.
3) Es gilt $a + (-a) = 0$ und $-(-a) + (-a) = 0$. Wegen der Eindeutigkeit des inversen Elements gilt $-(-a) = a$.
4) Es gilt $((-a)+(-b))+(a+b) = (-a)+a+(-b)+b = 0$, und die Formel folgt aus der Eindeutigkeit des inversen Elements.
5) Es gilt $0 = a \cdot 0 + (-(a \cdot 0)) = a \cdot (0+0) + (-(a \cdot 0)) = a \cdot 0 + a \cdot 0 + (-(a \cdot 0)) = a \cdot 0 + 0 = a \cdot 0$.
6) Sei $ab = 0$. Ist $b = 0$, so ist die erste Aussage erfüllt. Ist $b \neq 0$, so hat b ein inverses Element b^{-1} und es gilt $0 = 0 \cdot b^{-1} = abb^{-1} = a \cdot 1 = a$. Die zweite Aussage ist die Kontraposition der ersten.
7) Es gilt $(-a)b + ab = (-a+a)b = 0 \cdot b = 0$, und somit $(-a)b = -(ab)$ wegen der Eindeutigkeit des inversen Elements. Die Formel $a(-b) = -(ab)$ folgt dann durch Vertauschen von a und b. Schließlich haben wir $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.

□

Auf der Menge $\mathbb{R}$ gibt es außerdem die Ordnungsrelation $\leq$. Diese Relation ist folgendermaßen entstanden. Auf $\mathbb{N}$ haben wir $\leq$ durch die Nachfolgeeigenschaft definiert (s. Kapitel „Logik und Beweise“). Man kann dann die Relation $\leq$ auf die natürliche Weise auf $\mathbb{Z}$ erweitern. Für $\mathbb{Q}$ definieren wir $\leq$ wie folgt: $\frac{n_1}{m_1} \leq \frac{n_2}{m_2}$, wenn $n_1 m_2 \leq n_2 m_1$ mit $n_1, n_2 \in \mathbb{Z}$, $m_1, m_2 \in \mathbb{N}$ ist. Schließlich erweitert man $\leq$ auf $\mathbb{R}$ durch die Stetigkeit. Da wir die Konstruktion von $\mathbb{R}$ nicht besprochen haben, verzichten wir hier auf Einzelheiten.

Definition 5.11. Ordnungsaxiome

Ein Körper K mit einer Totalordnung $\leq$ heißt *geordneter Körper*, falls die folgenden *Ordnungsaxiome* gelten:

(O1) $\forall a, b, c \in K : a \leq b \Rightarrow a + c \leq b + c$,

(O2) $\forall a, b \in K : a > 0 \wedge b > 0 \Rightarrow ab > 0$.

Man sagt: Die Ordnungsrelation ist mit den Rechenoperationen *verträglich*.

$(\mathbb{R}, +, \cdot, \leq)$ ist ein geordneter Körper.

Satz 5.12. *Rechenregeln für Ungleichungen in einem geordneten Körper*

Seien $x, y, z \in K$. Dann gilt:

1) $x \leq y \Leftrightarrow y - x \geq 0$.
2) $x < 0 \Leftrightarrow -x > 0$.
3) $y \leq z \wedge x > 0 \Rightarrow xy \leq xz$.
4) $y \leq z \wedge x < 0 \Rightarrow xy \geq xz$.
5) $\forall x \neq 0 : x^2 > 0$. Insbesondere $1 > 0$.
6) $0 < x < y \Rightarrow 0 < y^{-1} < x^{-1}$.

Beweis:

1) Sei $x \leq y$. Dann gilt mit (O1)

$$0 = x + (-x) \leq y + (-x) = y - x \Rightarrow y - x \geq 0.$$

Ist umgekehrt $y - x \geq 0$, so gilt mit (O1)

$$y = y + 0 = y - x + x \geq 0 + x = x.$$

2) Aus 1) mit $y = 0$ folgt:

$$x \leq 0 \Leftrightarrow 0 - x = -x \geq 0.$$

Ist $x \neq 0$, so ist auch $-x \neq 0$, denn sonst wäre x das inverse Element von 0. Aber wegen $(-0) + 0 = 0$ und $0 + 0 = 0$ und der Eindeutigkeit des inversen Elements gilt $-0 = 0$. Also gilt:

$$x < 0 \Leftrightarrow -x > 0.$$

3) 1. Fall: Sei $y = z$. Dann ist $yx = zx$ und die Ungleichung ist erfüllt.
2. Fall: Sei $y < z$. Dann ist $z - y > 0$ und nach Voraussetzung auch $x > 0$. Aus (O2) folgt: $x(z - y) > 0$. Also

$$x(z - y) = xz - xy > 0 \Leftrightarrow xy < xz.$$

4) Aus $x < 0$ folgt $-x > 0$. Aus 3) und 1) folgt, da $y \leq z$, dass $-xy \leq -xz \Leftrightarrow xy - xz \geq 0 \Leftrightarrow xy \geq xz$.

5) Wegen (O2) gilt $x > 0 \Rightarrow x^2 = x \cdot x > 0$. Ist $x < 0$, so ist $-x > 0$ und $x^2 = (-x) \cdot (-x) > 0$. Insbesondere ist $1 = 1^2 > 0$.

6) Ist $x > 0$, so ist auch $x^{-1} \leq 0$. Diese Behauptung beweisen wir mit einem Widerspruchsbeweis: Sei $x > 0$ mit $x^{-1} \leq 0$. Dann ist aber nach 3) $1 = x \cdot x^{-1} \leq 0 \cdot x^{-1} = 0$, Widerspruch zu $1 > 0$. Demnach gilt $x^{-1} > 0$ für $x > 0$. Nun gelte zudem $0 < x < y$, es folgt direkt, dass $x^{-1} > 0,\ y^{-1} > 0$ und nach (O2) $x^{-1} \cdot y^{-1} > 0$. Nach 3) gilt

$$x < y \Rightarrow x(x^{-1}y^{-1}) < y(x^{-1}y^{-1}).$$

Da $x(x^{-1}y^{-1}) = (xx^{-1})y^{-1} = y^{-1}$ und $y(x^{-1}y^{-1}) = x^{-1}(yy^{-1}) = x^{-1}$, folgt $0 < y^{-1} < x^{-1}$.

□

Aus diesen Grundregeln kann man weitere Rechenregeln herleiten, beispielsweise

$$a \leq b \wedge c \leq d \Rightarrow a + c \leq b + d.$$

Beweis: Nach (O1) gilt: $a \leq b \Rightarrow a + c \leq b + c$ und $c \leq d \Rightarrow c + b \leq d + b = b + d$. Daraus folgt $a + c \leq b + c = c + b \leq b + d$.

□

Bemerkung 5.13. Für reelle Zahlen gilt die sog. *Trichotomie*: Für zwei reelle Zahlen a, b trifft genau eine der folgenden drei Möglichkeiten zu:

$$a < b, \quad a = b, \quad a > b.$$

Beweis:

Da $(\mathbb{R}, \leq)$ eine total geordnete Menge ist, gilt für alle $a, b \in \mathbb{R} : a \leq b$ oder $b \leq a$.

1. Fall: $a \leq b$ und $b \leq a \Rightarrow a = b$ wegen der Antisymmetrie der Relation $\leq$.
2. Fall: $a \leq b$ und $b \not\leq a$, insbesondere $b \neq a \Rightarrow a < b$.
3. Fall: $b \leq a$ und $a \not\leq b$, insbesondere $a \neq b \Rightarrow b < a \Rightarrow a > b$.

□

Satz 5.14. *Vorzeichen der Faktoren in einem positiven Produkt*

Seien $a, b \in \mathbb{R}$. Es gilt:

$$ab > 0 \Leftrightarrow ((a > 0 \wedge b > 0) \text{ oder } ((a < 0 \wedge b < 0)).$$

Beweis:

$\Leftarrow$ Wir betrachten zwei Fälle.

1. Fall: Seien $a > 0,\ b > 0$. Dann gilt nach (O2) $ab \geq 0$, und wegen $a \neq 0$, $b \neq 0$ auch $ab \neq 0$, also $ab > 0$.
2. Fall: Seien nun $a < 0,\ b < 0$. Dann sind aber $-a > 0$, $-b > 0$, und $ab = (-a)(-b) > 0$.

$\Rightarrow$ Es gelte $ab > 0$. Für b gibt es drei Möglichkeiten: $b = 0,\ b > 0$, oder $b < 0$.

1. Fall: $b = 0$ tritt nicht auf, da in diesem Fall $ab = 0$ wäre.
2. Fall: $b > 0$. Dann gilt auch $b^{-1} > 0$ und

   $$ab > 0 \Rightarrow a = abb^{-1} > 0 \cdot b^{-1} = 0,$$

   es gilt also auch $a > 0$.
3. Fall: $b < 0$. Dann gilt auch $b^{-1} < 0$ und

   $$ab > 0 \Rightarrow a = abb^{-1} < 0 \cdot b^{-1} = 0,$$

   es gilt also auch $a < 0$.

□

5.3 Betrag

Definition 5.15.

Sei $x \in \mathbb{R}$. Der *Absolutbetrag* (oder *Betrag*) der Zahl x ist definiert durch

$$|x| = \begin{cases} x, & \text{falls } x \geq 0, \\ -x, & \text{falls } x < 0. \end{cases}$$

Widmen wir uns kurz der *graphischen Bedeutung des Betrags*. Es gilt offensichtlich $|x| = |-x|$ und insbesondere $|x-y| = |y-x|$. Für $x, y \in \mathbb{R}$ entspricht $|x-y|$ dem Abstand zwischen x und y auf der Zahlengeraden.

Satz 5.16. *Eigenschaften des Betrags*

Für $x, y \in \mathbb{R}$ gilt:

1) $|x| \geq 0$ und $(|x| = 0 \Leftrightarrow x = 0)$ (positive Definitheit).

2) $|x+y| \leq |x| + |y|$ (Dreiecksungleichung).

3) $|xy| = |x| \cdot |y|$ (Multiplikativität).

Beweis:

1) Die Tatsache, dass $|x| \geq 0$ folgt sofort aus der Definition, ebenso gilt $|0| = 0$ nach der Definition.

$$x \neq 0 \Rightarrow |x| \neq 0 \text{ nach der Definition } \Rightarrow (|x| = 0 \Leftrightarrow x = 0).$$

2) Die zweite Behauptung beweisen wir durch eine Fallunterscheidung.

   1. Fall: $x \geq 0$ und $y \geq 0$. Dann ist auch $x + y \geq 0$, es folgt

   $$|x+y| = x + y = |x| + |y|.$$

   2. Fall: $x < 0$ und $y < 0$, dann ist auch $x + y < 0$, es folgt

   $$|x+y| = -(x+y) = -x - y = |x| + |y|.$$

   3. Fall: $x \geq 0,\ y < 0$ und $x + y \geq 0$.

   $$|x+y| = x + y < x - y = |x| + |y|.$$

   4. Fall: $x \geq 0,\ y < 0$ und $x + y < 0$.

   $$|x+y| = -(x+y) = -x - y < x - y = |x| + |y|.$$

   Der 5. und der 6. Fall mit $y \geq 0$ folgen aus dem 3. bzw. dem 4. Fall durch Vertauschung von x und y.

3) Die Behauptung $|xy| = |x| \cdot |y|$ beweisen wir ebenfalls durch eine Fallunterscheidung.

   1. Fall: $x \geq 0$ und $y \geq 0$, dann ist auch $xy \geq 0$ und folglich

   $$|xy| = xy = |x| \cdot |y|.$$

   2. Fall: $x \geq 0$ und $y < 0$. Dann gilt:

   $$|x| = x,\ |y| = -y,\ xy \leq 0,\ |xy| = -xy \Rightarrow |x| \cdot |y| = -xy = |xy|.$$

3. Fall: $x < 0$ und $y \geq 0$ folgt aus dem 2. Fall durch Vertauschung von x und y.
4. Fall: $x < 0$ und $y < 0$.

$$|x| = -x,\ |y| = -y,\ xy > 0,\ |xy| = xy \Rightarrow |x| \cdot |y| = (-x) \cdot (-y) = xy = |xy|.$$

□

Weitere Rechenregeln folgen daraus, zum Beispiel $\left|\frac{x}{y}\right| = \frac{|x|}{|y|}$ $(y \neq 0)$.

5.4 Lösen von Ungleichungen

In diesem Abschnitt werden einige Methoden zum Lösen von Ungleichungen anhand Beispiele vorgestellt.

Beispiel 5.17.

1) $\dfrac{x+1}{x-2} > 2$

Dann ist $D = \mathbb{R}\backslash\{2\}$ die Definitionsmenge des Terms.

1. Fall: $x - 2 > 0 \Leftrightarrow x > 2$.

$$\begin{aligned}
&\frac{x+1}{x-2} > 2 \quad | \cdot(x-2) > 0 \\
&x + 1 > 2(x-2) \\
&x + 1 > 2x - 4 \quad | -2x - 1 \\
&-x > -5 \quad | \cdot(-1) < 0 \\
&x < 5
\end{aligned}$$

Die Lösungsmenge im 1. Fall ist dann

$$L_1 = \{x \in \mathbb{R} : x > 2 \wedge x < 5\} = (2, 5).$$

2. Fall $x - 2 < 0 \Leftrightarrow x < 2$.

$$\begin{aligned}
&\frac{x+1}{x-2} > 2 \quad | \cdot(x-2) < 0 \\
&x + 1 < 2(x-2) \\
&x + 1 < 2x - 4 \quad | -2x - 1 \\
&-x < -5 \quad | \cdot(-1) < 0 \\
&x > 5
\end{aligned}$$

Die Lösungsmenge im 2. Fall ist dann

$$L_2 = \{x \in \mathbb{R} : x < 2 \wedge x > 5\} = \emptyset.$$

Die Gesamtlösungsmenge entspricht der Vereinigung der Lösungsmengen der einzelnen Fälle, also

$$L = L_1 \cup L_2 = (2, 5) \cup \emptyset = (2, 5).$$

2) $|x - 10| \leq \dfrac{1}{2}x$

Für die linke Seite gilt

$$|x - 10| = \begin{cases} x - 10, & \text{falls } x - 10 \geq 0 \Leftrightarrow x \geq 10, \\ -(x - 10), & \text{falls } x - 10 < 0 \Leftrightarrow x < 10. \end{cases}$$

1. Fall: $x \geq 10$.

$$\begin{aligned} x - 10 &\leq \frac{1}{2}x \quad | -\frac{1}{2}x + 10 \\ \frac{1}{2}x &\leq 10 \quad | \cdot 2 > 0 \\ x &\leq 20 \end{aligned}$$

Die Lösungsmenge im ersten Fall ist dann

$$L_1 = \{x \in \mathbb{R} : x \geq 10 \wedge x \leq 20\} = [10, 20].$$

2. Fall: $x < 10$.

$$\begin{aligned} -x + 10 &\leq \frac{1}{2}x \quad | +x \\ 10 &\leq \frac{3}{2}x \quad | \cdot \frac{2}{3} \\ \frac{20}{3} &\leq x \end{aligned}$$

Somit lautet die Lösungsmenge im zweiten Fall

$$L_2 = \left\{x \in \mathbb{R} : x < 10 \wedge x \geq \frac{20}{3}\right\} = \left[\frac{20}{3}, 10\right).$$

Insgesamt erhalten wir dann als Gesamtlösungsmenge

$$L = L_1 \cup L_2 = [10, 20] \cup \left[\frac{20}{3}, 10\right) = \left[\frac{20}{3}, 20\right].$$

3) Als letztes Beispiel betrachten wir die Ungleichung $|x + 3| \leq |2x - 1| + 3$.
Dabei sind

$$|x+3| = \begin{cases} x+3, & \text{falls } x+3 \geq 0 \Leftrightarrow x \geq -3, \\ -(x+3), & \text{falls } x+3 < 0 \Leftrightarrow x < -3, \end{cases}$$

$$|2x-1| = \begin{cases} 2x-1, & \text{falls } 2x-1 \geq 0 \Leftrightarrow x \geq \frac{1}{2}, \\ -(2x-1), & \text{falls} 2x-1 < 0 \Leftrightarrow x < \frac{1}{2}. \end{cases}$$

Die Punkte $x = -3$ und $x = \frac{1}{2}$ teilen die Zahlengerade in drei Intervalle. Wir betrachten also drei Fälle.

1. Fall: $x < -3$. Wir haben

$$|x + 3| = -(x + 3) = -x - 3 \text{ und } |2x - 1| = -(2x - 1) = -2x + 1,$$

damit folgt

$$\begin{aligned} -x - 3 &\leq -2x + 1 + 3 \\ -x - 3 &\leq -2x + 4 \quad | +2x + 3 \\ x &\leq 7 \end{aligned}$$

und somit als erste Lösungsmenge

$$L_1 = \{x \in \mathbb{R} : x < -3 \wedge x \leq 7\} = (-\infty, -3).$$

2. Fall: $-3 \leq x < \frac{1}{2}$. Es gilt

$$|x+3| = x+3 \text{ und } |2x-1| = -(2x-1) - 2x + 1,$$

damit folgt

$$\begin{aligned} & x+3 \leq -2x+1+3 \\ & x+3 \leq -2x+4 \quad | +2x-3 \\ & 3x \leq 1 \quad \left| \cdot \frac{1}{3} > 0 \right. \\ & x \leq \frac{1}{3} \end{aligned}$$

und somit als zweite Lösungsmenge

$$L_2 = \left\{ x \in \mathbb{R} : -3 \leq x < \frac{1}{2} \wedge x \leq \frac{1}{3} \right\} = \left[-3, \frac{1}{3} \right].$$

3. Fall: $x \geq \frac{1}{2}$. Dann ist

$$|x+3| = x+3 \text{ und } |2x-1| = 2x-1,$$

damit folgt

$$\begin{aligned} & x+3 \leq 2x-1+3 \\ & x+3 \leq 2x+2 \quad | -2x-3 \\ & -x \leq -1 \quad | \cdot(-1) < 0 \\ & x \geq 1 \end{aligned}$$

und somit als dritte Lösungsmenge

$$L_3 = \left\{ x \in \mathbb{R} : x \geq \frac{1}{2} \wedge x \geq 1 \right\} = [1, \infty)$$

und als Gesamtlösungsmenge

$$L = L_1 \cup L_2 \cup L_3 = (-\infty, -3) \cup \left[-3, \frac{1}{3} \right] \cup [1, \infty) = \left(-\infty, \frac{1}{3} \right] \cup \left[1, \infty \right).$$

Index