Unterlagen zur Vorlesung

Diskrete Mathematik

Wintersemester 2017/18

Erhard Aichinger
Institut für Algebra
Johannes Kepler Universität Linz

Version 15. Jänner 2018

Adresse:

Erhard Aichinger
Institut für Algebra, Johannes Kepler Universität Linz
4040 Linz, Österreich
e-mail: erhard.aichinger@jku.at

Version 15.1.2018

Druck: Kopierstelle, Abteilung Service, Universität Linz

Inhaltsverzeichnis

Teil 1

Logik und Mengenlehre

KAPITEL 1

Aussagenlogik

1. Aussagen

Wir bezeichnen als eine *Aussage* eine „Behauptung“, von der man sinnvollerweise fragen kann, ob sie wahr oder falsch ist. Beispiele:

(1) $5 > 2$.
Das ist eine Aussage, und sie ist wahr.
(2) $5 < 2$.
Das ist eine Aussage, und sie ist falsch.
(3) $5 + 2$.
Es hat keinen Sinn, zu fragen, ob $5 + 2$ wahr oder falsch ist. $5 + 2$ ist daher keine Aussage, sondern ein Ausdruck oder *Term*.
(4) Es gibt eine gerade Zahl, deren Quadrat ungerade ist.
Das ist eine Aussage, und sie ist falsch.
(5) Es gibt ein $n \in \mathbb{N}$, sodass n gerade und n^2 ungerade ist.
Das ist eine Aussage, und sie ist falsch. (Wir bezeichnen mit $\mathbb{N} := \{1, 2, 3, \ldots\}$ die natürlichen Zahlen, $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.)
(6) Für alle $n \in \mathbb{N}$ gilt: wenn n gerade ist, so ist n^2 gerade.
Das ist eine Aussage, und sie ist wahr.
(7) n ist gerade oder durch 3 teilbar.
Das ist keine Aussage, weil eine Variable, n, vorkommt. Wir bezeichnen eine solche Behauptung, die noch von Variablen abhängt, als *Aussageform*. Obige Aussageform stimmt für manche n, zum Beispiel für $n = 8$ und $n = 9$, und für andere nicht, zum Beispiel für $n = 7$.
(8) n ist gerade oder $n + 1$ ist gerade.
Das stimmt zwar für alle natürlichen Zahlen, ist aber keine Aussage, da n vorkommt.
(9) Für alle $n \in \mathbb{N}$ ist n gerade oder $n + 1$ gerade.
Das ist eine Aussage, und sie ist wahr. Hier kommt zwar n noch vor, aber es ist durch „für alle“ gebunden.
(10) Jede gerade natürliche Zahl n mit $n \geq 4$ lässt sich als Summe zweier Primzahlen schreiben.
Das ist eine Aussage. Man weiß nicht, ob sie wahr ist. Der Mathematiker Christian Goldbach hat 1742 in einem Brief an Leonhard Euler (1707-1783) vermutet, dass diese Aussage wahr ist. Euler hielt sie für „ein ganz

gewisses theorema, ungeachtet ich dasselbe nicht demonstriren kann“. Diese Aussage heißt *Goldbachsche Vermutung*.

(11) Jede gerade Zahl ist Summe von höchstens 6 Primzahlen.
Das ist eine Aussage. Seit 1995 weiß man, dass sie wahr ist.

Wir werden nun genauer untersuchen, wie Aussagen aufgebaut sein können.

2. Die Junktoren „und“, „oder“ und „nicht“

Atomare Aussagen sind Aussagen folgender Form: $5 > 2$, $3 = 4$, $2 + 5 > 6$.

Diese Aussagen können nun mit logischen Junktoren zu neuen Aussagen verbunden werden.

2.1. Logisches „und“.

- $5 > 2$ und $3 = 4$.
  Diese Aussage ist falsch.
- $5 > 2$ und $3 < 4$.
  Diese Aussage ist wahr.
- $5 < 2$ und $3 < 4$.
  Diese Aussage ist falsch.
- $5 < 2$ und $3 = 4$.
  Diese Aussage ist falsch,

Definition 1.1. Wenn A und B Aussagen sind, dann betrachten (definieren) wir die neue Aussage

$$A \text{ und } B$$

dann als wahr, wenn A und B beide wahr sind.

Diese Festlegung präzisiert die Bedeutung von „und“ in der Mathematik, schränkt aber gleichzeitig ein. Wenn wir im Alltag sagen: „Sie ging zum Arzt und wurde krank“, oder wenn wir sagen: „Sie wurde krank und ging zum Arzt“, so schwingt im ersten Satz, neben einer zeitlichen Abfolge, auch „der Arztbesuch war Schuld“ mit, im zweiten „weil sie krank war, ging sie zum Arzt“. Wenn wir mathematische Zusammenhänge in der Sprache der Prädikatenlogik ausdrücken, verzichten wir bewusst auf mitschwingende Nebenbedeutungen.

Für die Aussage „A und B“ schreiben wir auch $A \wedge B$ und bezeichnen sie als die *Konjunktion* von A und B.

Definition 1.2. Wir bezeichnen den *Wahrheitswert* einer Aussage A mit w oder 1, wenn die Aussage wahr ist, und mit f oder 0, wenn die Aussage falsch ist. Wir kürzen den Wahrheitswert von A auch mit $W(A)$ ab.

Sei $\sqcap$ die Funktion von $\{0,1\}^2 \to \{0,1\}$, die durch $0 \sqcap 0 = 0 \sqcap 1 = 1 \sqcap 0 = 0$ und $1 \sqcap 1 = 1$ definiert ist. Dann ist der Wahrheitswert von $A \wedge B$ durch

$$W(A \wedge B) = W(A) \sqcap W(B)$$

gegeben. Wir halten insbesondere fest, dass der Wahrheitswert von $A \wedge B$ nur von den Wahrheitswerten von A und B abhängt.

2.2. Logisches „oder“.

- $5 > 2$ oder $3 = 4$.
  Diese Aussage ist wahr.
- $5 > 2$ oder $3 < 4$.
  Diese Aussage ist wahr.
- $5 < 2$ oder $3 < 4$.
  Diese Aussage ist wahr.
- $5 < 2$ oder $3 = 4$.
  Diese Aussage ist falsch.

Definition 1.3. Seien A und B Aussagen, und sei C die Aussage

$$A \text{ oder } B.$$

Dann ist C genau dann wahr, wenn zumindest eine der beiden Aussagen A und B wahr ist. Wir schreiben für „A oder B“ auch $A \vee B$, und bezeichnen C als die *Disjunktion* von A und B.

Wir normieren hier den Gebrauch des Wortes „oder“.

Wenn etwa eine Mutter ihrem Kind verspricht: „Du bekommst ein Eis oder eine Torte“, so ist das Versprechen auch dann erfüllt, wenn das Kind Eis und Torte bekommt. Es ist aber vorstellbar, dass die Mutter gemeint hat: „Du bekommst ein Eis oder eine Torte, aber nicht beides“. Für den mathematischen Gebrauch normieren wir, dass $A \vee B$ auch dann wahr ist, wenn beide Aussagen A und B wahr sind.

Definition 1.4. Sei $\sqcup$ die Funktion von $\{0,1\}^2 \to \{0,1\}$, die durch $0 \sqcup 0 = 0$ und $0 \sqcup 1 = 1 \sqcup 0 = 1 \sqcup 1 = 1$ definiert ist. Dann ist der Wahrheitswert von $A \vee B$ durch

$$W(A \vee B) = W(A) \sqcup W(B)$$

gegeben.

Der Wahrheitswert von $A \vee B$ hängt also nur von den Wahrheitswerten von A und B ab.

2.3. Verneinung.

- 5 ist nicht größer als 7.
  Da $5 > 7$ falsch ist, ist diese Aussage wahr.
- Nicht alle Primzahlen sind ungerade.
  Die Aussage „alle Primzahlen sind ungerade“ ist falsch, da 2 gerade und eine Primzahl ist. Also ist die Aussage „nicht alle Primzahlen sind ungerade“ wahr.
- 5 ist nicht größer als 3.
  Diese Aussage ist falsch, weil 5 größer als 3 ist.

DEFINITION 1.5. Sei A eine Aussage, und sei C die Aussage

$$\text{nicht } A.$$

Dann ist C dann wahr, wenn A falsch ist, und C ist dann falsch, wenn A wahr ist. Wir schreiben für „nicht A“ auch $\neg A$.

DEFINITION 1.6. Sei $\sim$ die Funktion von $\{0,1\} \to \{0,1\}$, die durch $\sim(0) = 1$ und $\sim(1) = 0$ definiert ist. Dann ist der Wahrheitswert von $\neg A$ durch

$$W(\neg A) = \sim(W(A))$$

gegeben.

Die Bedeutung von „nicht“ in der Mathematik weicht also nicht vom üblichen Gebrauch ab. Verneinungen können aber manchmal durchaus schwierig zu durchblicken sein. Die Behauptung

> „nicht alle natürlichen Zahlen sind nicht ungerade“

lässt sich etwa viel einfacher als

> „nicht alle natürlichen Zahlen sind gerade“

oder

> „es gibt ungerade natürliche Zahlen“

ausdrücken. Wir werden in Kürze sehen, wie wir solche Vereinfachungen fast mechanisch durchführen können.

Mehrfache Verneinungen sind logische Stolperfallen: in „Emilia Galotti“ von G.E. Lessing warnt eine Mutter ihre Tochter:

> „Wie wild er [der Vater] schon war, als er nur hörte, daß der Prinz dich jüngst nicht ohne Missfallen gesehen!“.

Die Tragödie beruht aber dann darauf, dass der Prinz die Tochter vielmehr ganz ohne Missfallen gesehen hat.

3. Rechengesetze für Junktoren

DEFINITION 1.7. Seien A und B Aussagen. Wir bezeichnen A und B als *äquivalent*, wenn A und B beide wahr, oder beide falsch sind. Wir schreiben dafür $A \equiv B$.

SATZ 1.8. *Seien A, B Aussagen. Dann gilt:*

(1) $\neg(\neg A) \equiv A$.
(2) $\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$ *(De Morgansches Gesetz[1])*
(3) $\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)$ *(De Morgansches Gesetz)*

Beweis I: (1) Wir betrachten zuerst den Fall, dass A wahr ist. Dann ist $\neg A$ falsch, also ist $\neg(\neg A)$ wahr. Nun betrachten wir den Fall, dass A falsch ist. Dann ist $\neg A$ wahr, also ist $\neg(\neg A)$ falsch. In jedem Fall haben A und $\neg(\neg A)$ also den gleichen Wahrheitswert.

(2) Wir nehmen zuerst an, dass $\neg(A \wedge B)$ wahr ist. Dann ist $A \wedge B$ falsch. Das bedeutet, dass A und B nicht beide wahr sein können; eine der beiden Aussagen ist also falsch. Wenn A falsch ist, so ist $\neg A$ wahr, und somit erst recht $(\neg A)\vee(\neg B)$. Wenn B falsch ist, so ist $\neg B$ wahr. Auch dann ist $(\neg A) \vee (\neg B)$ wahr.

Nehmen wir nun an, dass $\neg(A \wedge B)$ falsch ist. Dann ist $A \wedge B$ wahr, also sind sind beide Aussagen A und B wahr. Folglich sind beide Aussagen $\neg A$ und $\neg B$ falsch; dann ist auch $(\neg A) \vee (\neg B)$ falsch.

Den Beweis von (3) lassen wir hier aus. □

ÜBUNGSAUFGABEN 1.9.

(1) Zeigen Sie $\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)$. Verwenden Sie dazu ähnliche Formulierungen wie im Beweis von Satz 1.8 (2).

Wir geben nun eine zweite Variante des Beweises von Satz 1.8 (2) an.

Beweis II: Sei a der Wahrheitswert von A, und sei b der Wahrheitswert von B. Dann gilt

$$\begin{aligned} W(\neg(A \wedge B)) &= \sim(W(A \wedge B)) \\ &= \sim(W(A) \sqcap W(B)) \\ &= \sim(a \sqcap b). \end{aligned}$$

Ebenso gilt

$$\begin{aligned} W((\neg A) \vee (\neg B)) &= W(\neg A) \sqcup W(\neg B) \\ &= (\sim(W(A))) \sqcup (\sim(W(B))) \\ &= (\sim a) \sqcup (\sim b). \end{aligned}$$

[1]Augustus De Morgan, 1806-1871, englischer Mathematiker.

Nun bleibt zu zeigen, dass für alle 4 Belegungen von a und b gilt, dass $\sim(a \sqcap b) = (\sim a) \sqcup (\sim b)$. Wir machen dazu folgende Tabelle; eine solche Tabelle heißt auch *Wahrheitstafel*.

a	b	$a \sqcap b$	$\sim(a \sqcap b)$	$\sim a$	$\sim b$	$(\sim a) \sqcup (\sim b)$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

Da die 4. und die 7. Spalte dieser Tabelle gleich sind, gilt für alle $(a, b) \in \{0, 1\}^2$, dass $\sim(a \sqcap b) = (\sim a) \sqcup (\sim b)$. Somit gilt insgesamt $W(\neg(A \wedge B)) = W(\neg(A) \vee \neg(B))$, und somit sind $\neg(A \wedge B))$ und $(\neg A) \vee (\neg B)$ äquivalent.

SATZ 1.10. *Seien A, B, C Aussagen. Dann gilt:*

(1) $(A \wedge B) \vee C \equiv (A \vee C) \wedge (B \vee C)$ *(Distributivgesetz).*
(2) $(A \vee B) \wedge C \equiv (A \wedge C) \vee (B \wedge C)$ *(Distributivgesetz).*
(3) $A \wedge A \equiv A$ *(Idempotenz von $\wedge$).*
(4) $A \vee A \equiv A$ *(Idempotenz von $\vee$).*
(5) $A \wedge (A \vee B) \equiv A$ *(Verschmelzungs- oder Absorptionsgesetz).*
(6) $A \vee (A \wedge B) \equiv A$ *(Verschmelzungs- oder Absorptionsgesetz).*
(7) $A \wedge B \equiv B \wedge A$ *(Kommutativität von $\wedge$).*
(8) $A \vee B \equiv B \vee A$ *(Kommutativität von $\vee$).*
(9) $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$ *(Assoziativität von $\wedge$).*
(10) $(A \vee B) \vee C \equiv A \vee (B \vee C)$ *(Assoziativität von $\vee$).*

Beweis: Wir beweisen diese Eigenschaften jeweils mit vollkommen verschiedenen Strategien.

(1) Wir nehmen zuerst an, dass $(A \wedge B) \vee C$ wahr ist und zeigen, dass dann auch $(A \vee C) \wedge (B \vee C)$ wahr ist. Da $(A \wedge B) \vee C$ wahr ist, ist entweder $A \wedge B$ wahr, oder C ist wahr. Wir betrachten zuerst den Fall, dass $A \wedge B$ wahr ist. Dann sind A und B beide wahr, also sind auch $A \vee C$ und $B \vee C$ beide wahr. Somit ist auch $(A \vee C) \wedge (B \vee C)$ wahr. Wir betrachten nun den Fall, dass C wahr ist. Dann sind $A \vee C$ und $B \vee C$ beide wahr, und somit ist $(A \vee C) \wedge (B \vee C)$ wahr.

Nun nehmen wir an, dass $(A \wedge B) \vee C$ falsch ist und zeigen, dass dann auch $(A \vee C) \wedge (B \vee C)$ falsch ist. Wenn $(A \wedge B) \vee C$ falsch ist, dann ist sowohl $(A \wedge B)$ als auch C falsch. Da $A \wedge B$ falsch ist, muss zumindest eine der beiden Aussagen A und B falsch sein. Wir betrachten zuerst den Fall, dass A falsch ist. Da dann A und C beide falsch sind, ist $A \vee C$ falsch; damit ist aber $(A \vee C) \wedge (B \vee C)$ auch falsch. Wir betrachten nun den Fall, dass B falsch ist. Da dann B und C beide falsch sind, ist $B \vee C$ falsch; damit ist aber $(A \vee C) \wedge (B \vee C)$ auch falsch.

(2)

$$\begin{array}{rcll}(A \vee B) \wedge C & \equiv & \neg\big(\neg((A \vee B) \wedge C)\big) & \text{wegen Satz 1.8 (1)} \\ & \equiv & \neg\big((\neg(A \vee B)) \vee (\neg C)\big) & \text{wegen Satz 1.8 (2)} \\ & \equiv & \neg\big((\neg(A) \wedge \neg(B)) \vee (\neg C)\big) & \text{wegen Satz 1.8 (3).}\end{array}$$

Nun verwenden wir (1) (für $A' := \neg A$, $B' := \neg B$, $C' := \neg C$) und erhalten, dass der letzte Ausdruck gleich $\neg\big(((\neg A) \vee (\neg C)) \wedge ((\neg B) \vee (\neg C))\big)$ ist. Wir verwenden nun wieder die De Morganschen Gesetze und erhalten

$$\begin{array}{rcl}\neg\big(((\neg A) \vee (\neg C)) \wedge ((\neg B) \vee (\neg C))\big) & \equiv & \neg\big((\neg A) \vee (\neg C)\big) \vee \neg\big((\neg B) \vee (\neg C)\big) \\ & \equiv & \big((\neg(\neg A)) \wedge (\neg(\neg C))\big) \vee \big((\neg(\neg B)) \wedge (\neg(\neg C))\big) \\ & \equiv & (A \wedge C) \vee (B \wedge C).\end{array}$$

(3) Wenn der Wahrheitswert von A gleich a ist, so ist der Wahrheitswert von $A \wedge A$ gleich $a \sqcap a$. Da $0 \sqcap 0 = 0$ und $1 \sqcap 1 = 1$, gilt also für alle $a \in \{0, 1\}$, dass $a \sqcap a = a$. Somit sind die Wahrheitswerte von $A \wedge A$ und A gleich.

(5) Wir zeigen folgendes:

(1) Wenn $A \wedge (A \vee B)$ wahr ist, so ist A wahr.
(2) Wenn A wahr ist, so ist $A \wedge (A \vee B)$ wahr.

Wir überlegen uns, warum das ausreicht. Wir sollten ja eigentlich zeigen, dass $A \wedge (A \vee B)$ und A den gleichen Wahrheitswert haben. Wenn sie verschiedenen Wahrheitswert haben, dann ist entweder $A \wedge (A \vee B)$ wahr und A falsch, oder es ist $A \wedge (A \vee B)$ falsch und A wahr. Die erste Alternative wird aber von der Überlegung (1) ausgeschlossen, die zweite von der Überlegung (2).

Wir nehmen also an, dass $A \wedge (A \vee B)$ wahr ist. Dann sind A und $A \vee B$ beide wahr. Insbesondere ist also A wahr.

Nun nehmen wir an, dass A wahr ist. Dann ist $A \vee B$ (erst recht) wahr, also sind A und $A \vee B$ beide wahr. Folglich ist $A \wedge (A \vee B)$ war.

ÜBUNGSAUFGABEN 1.11.

(1) Wir haben im Beweis von Satz 1.10 die Eigenschaft (2) aus (1) und den De Morganschen Gesetzen hergeleitet. Geben Sie einen Beweis von (2), der so aufgebaut ist, wie der Beweis von (1); starten Sie also damit, dass Sie annehmen, dass $(A \vee B) \wedge C$ wahr ist, ...
(2) Geben Sie einen Beweis von Satz 1.10 (1) durch Wahrheitstafeln.
(3) Finden Sie zwei Ausdrücke p, q der Form $A \wedge B$, $(\neg A) \vee B$, ..., sodass folgendes gilt: wenn p wahr ist, ist auch q wahr, aber wenn q wahr ist, muss deshalb p nicht notwendigerweise wahr sein.
(4) Zeigen Sie Satz 1.10 (6), indem Sie die Funktionen $f(a, b) = a \sqcap (a \sqcup b) = a$ und $g(a, b) = a$ tabellieren.
(5) Zeigen Sie Satz 1.10 (6), indem Sie so vorgehen wie im angegebenen Beweis von Satz 1.10 (5).
(6) Zeigen Sie, dass für alle Aussagen A, B gilt: $A \vee B \equiv B \vee A$ und $A \wedge B = B \wedge A$ (*Kommutativgesetz*).
(7) Zeigen Sie, dass für alle Aussagen A, B, C gilt: $(A \vee B) \vee C \equiv A \vee (B \vee C)$ und $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$ (*Assoziativgesetz*).

Wir kürzen nun die wahre Aussage $0 = 0$ mit $\mathbf{T}$, und die falsche Aussage $0 \neq 0$ mit $\mathbf{F}$ ab.

Satz 1.12. *Sei A eine Aussage. Dann gilt:*

(1) $A \wedge \mathbf{T} \equiv A$,
(2) $A \vee \mathbf{T} \equiv \mathbf{T}$,
(3) $A \wedge \mathbf{F} \equiv \mathbf{F}$,
(4) $A \vee \mathbf{F} \equiv A$.

Beweis: (1) Wir nehmen an, dass $A \wedge \mathbf{T}$ wahr ist. Dann ist A wahr und $\mathbf{T}$ wahr. Somit ist A wahr. Nun nehmen wir an, dass A wahr ist. Da dann A und $\mathbf{T}$ beide wahr sind, ist auch $A \wedge \mathbf{T}$ wahr.

(2) Sei a der Wahrheitswert von A. Dann ist der Wahrheitswert von $A \vee \mathbf{T}$ gleich $a \sqcup 1$. Nun sehen wir, dass $0 \sqcup 1 = 1 \sqcup 1 = 1$, also ist der Wahrheitswert von $a \sqcup 1$ gleich 1. Der Wahrheitswert von $\mathbf{T}$ ist ebenfalls 1. Somit haben $A \vee \mathbf{T}$ und $\mathbf{T}$ den gleichen Wahrheitswert, und somit äquivalent.

(3) Wir verwenden De Morgan und erhalten $A \wedge \mathbf{F} \equiv \neg(\neg(A \wedge \mathbf{F})) \equiv \neg((\neg A) \vee (\neg\mathbf{F})) \equiv \neg((\neg A) \vee \mathbf{T}) \equiv (\neg\mathbf{T}) = \mathbf{F}$. (Warum gilt jedes der vier $\equiv$?)

(4) wird ausgelassen. □

Übungsaufgaben 1.13.

(1) Geben Sie einen Beweis für Satz 1.12 (4) in jener Form an, in der wir Satz 1.12 (1) bewiesen haben.
(2) Geben Sie einen Beweis für Satz 1.12 (4) in jener Form an, in der wir Satz 1.12 (2) bewiesen haben.
(3) Geben Sie einen Beweis für Satz 1.12 (4), indem Sie die De Morganschen Gesetze und $\neg(\neg X) \equiv X$ ausnützen und damit (4) auf eine der bereits bewiesenen Äquivalenzen zurückführen.

4. Die Implikation

In diesem Abschnitt normieren wir den Gebrauch von „wenn . . . , dann“. Betrachten wir dazu folgendes Beispiel (cf. [**BT09**, S. 49]). Anton sagt zu Berta:

> „Wenn du mir das Buch morgen zurückbringst, zahle ich dir einen Kaffee“.

In welchen der möglichen vier Fälle hat Anton seine Zusage gehalten?

(1) Berta bringt das Buch zurück, und Anton zahlt ihr einen Kaffee: Zusage gehalten.
(2) Berta bringt das Buch zurück, und Anton zahlt ihr keinen Kaffee: Zusage nicht gehalten.
(3) Berta bringt das Buch nicht zurück, und Anton zahlt ihr keinen Kaffee: Auch hier kann sich Berta nicht beschweren: für diesen Fall hatte ihr Anton nichts versprochen. Zusage gehalten.
(4) Berta bringt das Buch nicht zurück, und Anton zahlt ihr einen Kaffee: Das ist sehr nett von Anton, und verletzt die Abmachung sicher nicht: darüber, was Anton tut, wenn Berta das Buch nicht zurückbringt, hat er nichts zugesagt. Insgesamt: Zusage gehalten.

Die einzige Möglichkeit, dass eine Aussage „wenn A, dann B“ falsch ist, ist also die, dass die Prämisse A eintritt, die Konklusion B aber nicht.

DEFINITION 1.14. Seien A und B Aussagen, und sei C die Aussage

wenn A, dann B.

Dann ist C genau dann falsch, wenn A wahr und B falsch ist. Sonst ist C wahr. Wir kürzen die Aussage „wenn A, dann B“ auch mit $A \Rightarrow B$ ab und bezeichnen C als eine *Implikation*.

Sei $\to$ die Funktion von $\{0,1\}^2$ nach $\{0,1\}$, die durch folgende Tabelle erklärt ist:

a	b	$a \to b$
0	0	1
0	1	1
1	0	0
1	1	1

SATZ 1.15. *Seien A und B Aussagen, sei a der Wahrheitswert von A, und sei b der Wahrheitswert von B. Dann ist der Wahrheitswert von $A \Rightarrow B$ gleich $a \to b$.*

Beweis: Wir betrachten als erstes den Fall, dass $A \Rightarrow B$ falsch ist. Das bedeutet, dass A wahr und B falsch ist. Dann ist $a = 1$ und $b = 0$. Wegen $1 \to 0 = 0$ gilt dann $a \to b = 0$.

Nun betrachten wir den Fall, dass $A \Rightarrow B$ wahr ist. Nehmen wir, im Widerspruch zur Behauptung, an dass $a \to b = 0$. Dann gilt $a = 1$ und $b = 0$ und somit ist A wahr und B falsch. Dann ist ist $A \Rightarrow B$ falsch, im Widerspruch zur Fallannahme. Somit kann $a \to b = 0$ nicht gelten. Also gilt $a \to b = 1$. □

Ähnlich wie bei „oder“ gibt die Normierung nur eine der normalsprachlichen Bedeutungen von „wenn, dann“ wieder. Wir betrachten folgende Beispiele:

(1) $(5 > 2) \Rightarrow (10 > 4)$.
$(5 > 2)$ und $(10 > 4)$ sind beide wahr. Also ist $(5 > 2) \Rightarrow (10 > 4)$ wahr.

Im Satz „wenn 5 größer als 2 ist, dann ist auch 10 größer als 4“ schwingt aber auch mit “klar, denn ich brauche $5 > 2$ nur zu verdoppeln. Der Wahrheitswert von $A \Rightarrow B$ sagt aber nichts über einen kausalen Zusammenhang von A und B aus, sondern nur, dass es nicht so ist, dass A wahr und B falsch ist.

(2) $(5 > 2) \Rightarrow$ (6 ist eine gerade Zahl).
Beide Teilaussagen sind wahr, also ist die Implikation wahr.

Dass die beiden Aussagen inhaltlich keine Verbindung haben, stört nicht. Der Wahrheitswert der Implikation hängt nur von den Wahrheitswerten der Teilaussagen ab.

(3) $(5 < 4) \Rightarrow (5 < 11)$.
Hier ist $A = (5 < 4)$ falsch und $B = (5 < 11)$ wahr. Ingesamt ist $A \Rightarrow B$ also wahr.
(4) $(3 < 2) \Rightarrow (103 < 102)$.
Da $3 < 2$ und $103 < 102$ beide falsch sind, ist die Implikation wahr.
(5) $(5 > 3) \Rightarrow (-5 > -3)$.
Da $5 > 3$ wahr ist, und $-5 > -3$ falsch, ist die Implikation falsch.
(6) Wenn Paris in Ungarn liegt, so ist Schnee schwarz.
Die Implikation ist wahr.

In der mathematischen „Umgangssprache“ kommt es manchmal vor, dass „wenn, dann“ auch ein heimliches „für alle“ enthält. Wir betrachten die Aussage:

> Wenn n gerade ist, so ist n^2 durch 4 teilbar.

Wir können das so sehen: $G(n)$ ist die *Aussageform* „n ist gerade“, $V(n)$ ist die Aussageform „n ist Vielfaches von 4“. Dann meint obige Behauptung vermutlich:

> Für alle n gilt: wenn $G(n)$, dann $V(n^2)$,

was man auch als

$$\text{für alle } n \in \mathbb{N} : (G(n) \Rightarrow V(n^2))$$

schreiben kann. Diese Aussage ist wahr: wenn n gerade ist, so gibt es ein $k \in \mathbb{N}$ mit $n = 2k$. Also gilt $n^2 = 4k^2$, und das ist ein Vielfaches von 4. Wir betrachten nun die Aussage:

> Wenn n gerade ist, so ist n durch 3 teilbar.

Wenn wir $t \mid n$ für „t teilt n“ schreiben, so wäre

$$2 \mid n \Rightarrow 3 \mid n.$$

eine Formalisierung. Die Aussageform $I(n) := (2 \mid n \Rightarrow 3 \mid n)$ ist für manche n wahr (etwa für $n = 5$, $n = 6$, $n = 3$), für andere n falsch (etwa $n = 2$). Es könnte aber auch sein, dass

$$\text{für alle } n \in \mathbb{N} : (2 \mid n \Rightarrow 3 \mid n)$$

gemeint ist. Das könnte man so ausdrücken:

> Für alle natürlichen Zahlen $n \in \mathbb{N}$ gilt: wenn n gerade ist, so ist n durch 3 teilbar.

Diese Aussage ist falsch, da die Aussageform $I(n)$ für $n = 2$ nicht gilt.

Wir werden die Formulierung

> Für alle $n \in \mathbb{N}$ gilt: wenn n gerade ist, so ist n^2 durch 4 teilbar

gegenüber

> Wenn n gerade ist, so ist n^2 durch 4 teilbar.

bevorzugen.

Übungsaufgaben 1.16.

(1) Schreiben Sie folgende Sätze so um, dass sie die Form „für alle $x \ldots \in \ldots$ gilt : $A(x) \Rightarrow B(x)$“ haben.
   (a) Wenn x eine reelle Zahl ist, so ist $x^2 \geq 0$.
   (b) Wenn n kein Vielfaches von 3 ist, so hat n^2 bei Division durch 3 Rest 1. *Hinweis:* $B(x)$ ist dann „x hat bei Division durch 3 Rest 1“.
(2) Schreiben Sie folgende Sätze so um, dass sie die Form „für alle $x \ldots \in \ldots$ gilt : $A(x) \Rightarrow B(x)$“ haben.
   (a) Die Wurzel einer natürlichen Zahl ist eine natürliche Zahl oder irrational. (Für eine reelle Zahl x sei $A(x)$ die Eigenschaft, dass x Wurzel einer natürlichen Zahl ist, $N(x)$ die Eigenschaft, dass x natürlich und $R(x)$ die Eigenschaft, dass x rational ist.)
   (b) Ein Quadrat ist auch ein Rechteck.

Die meisten mathematischen Zusammenhänge lassen sich erst darstellen, wenn man *Aussageformen* (also „Aussagen über Variablen“) und die *Quantoren* „für alle ... gilt:“ und „es gibt ein ..., sodass“ verwendet. Die *Prädikatenlogik* ist jenes Teilgebiet der Mathematik, dass sich mit Ausdrücken, die aus Aussagen, Aussageformen, Junktoren und Quantoren gebildet werden, beschäftigt. Die *Aussagenlogik* beschäftigt sich den Ausdrücken, die aus Aussagen und Junktoren gebildet werden.

Die Implikation lässt sich auch durch Konjunktion, Disjunktion und Negation ausdrücken.

Satz 1.17. *Seien A, B Aussagen. Dann gilt:*

(1) $A \Rightarrow B \equiv (\neg A) \vee B$.
(2) $A \Rightarrow B \equiv \neg(A \wedge (\neg B))$.
(3) $A \Rightarrow B \equiv ((\neg B) \Rightarrow (\neg A))$ *(*Kontrapositionsregel*).*

Beweis: Wahrheitstafeln.

Wir halten nun noch einige sprachliche Möglichkeiten, die Tatsache, dass $A \Rightarrow B$ wahr ist, auszudrücken, fest:

(1) A impliziert B.
(2) Wenn A, dann B.
(3) A gilt nur dann, wenn B gilt.
(4) B gilt, wenn A gilt.
(5) Wenn B nicht gilt, so gilt auch A nicht.

5. Weitere Junktoren

Definition 1.18. Seien A und B Aussagen. Dann definieren wir:

(1) $A \Leftarrow B$ steht für $B \Rightarrow A$.
(2) $A \Leftrightarrow B$ ist genau dann wahr, wenn $(A \Rightarrow B) \wedge (B \Rightarrow A)$ wahr ist.

Wir bezeichnen $A \Leftrightarrow B$ als die *Äquivalenz von A und B.*

SATZ 1.19. *Seien A und B Aussagen. Dann ist $A \Leftrightarrow B$ genau dann wahr, wenn A und B beide wahr oder beide falsch sind.*

Dass die Äquivalenz $A \Leftrightarrow B$ wahr ist, kann auch durch folgende Formulierungen ausgedrückt werden.

(1) A genau dann, wenn B.
(2) A gilt dann, und nur dann, wenn B gilt.
(3) (englisch) A if and only if B.
(4) (englisch + P. Halmos[2]) A iff B.
(5) A und B sind äquivalent.

ÜBUNGSAUFGABEN 1.20.
Überprüfen Sie jeweils, ob die die Aussagen p und q für alle Aussagen A und B äquivalent sind. Geben Sie dafür (im Fall der Äquivalenz) einen Beweis an, und finden Sie im Fall, dass die Aussagen nicht äquivalent sind, Belegungen für die Wahrheitswerte von A und B, sodass eine Seite wahr und die andere falsch ist.

(1) $p = \neg(A \Rightarrow B)$, $q = A \wedge (\neg B)$.
(2) $p = (A \Rightarrow B) \Rightarrow C$, $q = A \Rightarrow (B \Rightarrow C)$.
(3) $p = A \Leftrightarrow B$, $q = (A \vee (\neg B)) \wedge ((\neg A) \vee B)$.
(4) $p = A \Rightarrow (B \Rightarrow C)$, $q = (A \wedge B) \Rightarrow C$.
(5) $p = A \Rightarrow (B \Rightarrow C)$, $q = B \Rightarrow (A \Rightarrow C)$.
(6) $p = A \Rightarrow (B \Rightarrow B)$, $q = B \Rightarrow (A \Rightarrow A)$.
(7) $p = (A \Rightarrow B) \Rightarrow A$, $q = A$.

DEFINITION 1.21. Seien A und B Aussagen. Dann ist $A \dot{\vee} B$ definiert als $(A \wedge (\neg B)) \vee ((\neg A) \wedge B)$.

$A \dot{\vee} B$ ist das „ausschließende oder“: eines von beiden, und nicht beide.

SATZ 1.22. *Seien A, B Aussagen. Dann gilt $A \dot{\vee} B \equiv \neg(A \Leftrightarrow B) \equiv (A \vee B) \wedge (\neg(A \wedge B))$.*

Die dazu gehörige Boole'sche Funktion bezeichnet man mit $\oplus$. Sie ist durch $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$ definiert.

DEFINITION 1.23. Die Sheffer-Funktion[3] ist definiert durch

$$x|y := \sim(x \sqcap y).$$

Die Shefferfunktion verdankt ihre Popularität der Tatsache, dass sie imstande ist, alle anderen logischen Junktoren auszudrücken: $\sim x = x|x$, $x \sqcap y = (x|y)|(x|y)$, $x \sqcup y = (x|x)|(y|y)$, $x \oplus y = (x|(x|y))|(y|(x|y))$ für alle $x, y \in \{0, 1\}$. Das kann außer der Shefferfunktion keine der Funktionen $\sqcup, \sqcap, \sim, \oplus$ allein. Allerdings reichen zum Beispiel auch $\sqcap$ und $\sim$ gemeinsam aus, um alle anderen Junktoren auszudrücken.

ÜBUNGSAUFGABEN 1.24.

[2]Paul Halmos, 1916-2006
[3]Henry Sheffer, 1882-1964

(1) Finden Sie für jede der 16 möglichen Funktionen von $\{0,1\}^2$ nach $\{0,1\}$ einen möglichst einfachen Ausdruck, der 0, 1, $\sqcup, \sqcap, \oplus, \sim$ verwendet und die entsprechende Funktion beschreibt.

a	b	?	$a \sqcap b$	?	?	?	?	?	?	?	?	?	?	?	?	?
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

(2) Finden Sie jeweils einen Ausdruck, der nur $0, x, y$ und den Junktor $\rightarrow$ verwendet, und der folgende Funktionen beschreibt:
   (a) $\sim x$.
   (b) $x \sqcup y$.
   (c) $x \sqcap y$.

KAPITEL 2

Prädikatenlogik

1. Aussageformen

Kapitel 3 vorwegnehmend verwenden wir in der Folge einige Mengen:

$$\begin{aligned} \mathbb{N} &= \{1, 2, 3, 4, \ldots\} \\ \mathbb{N}_0 &= \{0, 1, 2, 3, 4, \ldots\} \\ \mathbb{R} &= \text{ die Menge der reellen Zahlen} \end{aligned}$$

Es gilt $4 \in \mathbb{N}$, $\pi \notin \mathbb{N}$, $\mathbb{N} \notin \mathbb{N}_0$. Als *Aussageform* bezeichnen wir eine Aussage über Variablen, etwa

(1) x ist gerade,
(2) $x \geq 2 + y$,
(3) $3x - 2y = 8$,
(4) x und y haben denselben Rest bei der Division durch 5.

Wenn wir für alle Variablen Werte einsetzen, dann erhalten wir Aussagen, die wahr oder falsch sein können. Wenn etwa $A(x)$ die Aussageform „x ist gerade“ ist, so ist $A(3)$ die Aussage „3 ist gerade“ und $A(4)$ die Aussage „4 ist gerade“. Bei der Definition einer Aussageform ist es sinnvoll, anzugeben, welche Werte x annehmen darf, etwa in folgender Form:

Für $x \in \mathbb{N}$ definieren wir

$$A(x) :\Leftrightarrow x \text{ ist gerade.}$$

Damit ist klar, dass $A(\pi)$ nicht definiert wurde.

Wir können aus Aussageformen mithilfe der logischen Junktoren neue Aussageformen bauen. Die Aussageform $A(n)$ über den natürlichen Zahlen, die durch

$$A(n) :\Leftrightarrow n \text{ ist gerade oder } n \text{ ist durch 3 teilbar}$$

gegeben ist, gilt nicht für alle $n \in \mathbb{N}$, da 5 weder gerade noch durch 3 teilbar ist, aber doch für manche, zum Beispiel für $n = 2$ und $n = 18$.

Definition 2.1. Seien $A(x_1, \ldots, x_n)$ und $B(x_1, \ldots, x_n)$ Aussageformen, die für alle $x_1, \ldots, x_n \in X$ definiert sind.

(1) $A(x_1, \ldots, x_n)$ und $B(x_1, \ldots, x_n)$ sind *äquivalent*, wenn für alle $a_1, \ldots, a_n \in X$ die Aussagen $A(a_1, \ldots, a_n)$ und $B(a_1, \ldots, a_n)$ den gleichen Wahrheitswert haben. Wir schreiben dafür $A(x_1, \ldots, x_n) \equiv B(x_1, \ldots, x_n)$.

(2) $A(x_1, \ldots, x_n)$ ist *hinreichend für* $B(x_1, \ldots, x_n)$, wenn für alle $a_1, \ldots, a_n \in X$, für die $A(a_1, \ldots, a_n)$ wahr ist, auch $B(a_1, \ldots, a_n)$ wahr ist.
(3) $B(x_1, \ldots, x_n)$ ist *notwendig für* $A(x_1, \ldots, x_n)$, wenn $A(x_1, \ldots, x_n)$ hinreichend für $B(x_1, \ldots, x_n)$ ist.

So ist sind etwa über den reellen Zahlen die Aussageformen $x+y = 3$ und $x = 3-y$ äquivalent. Daher kommt der Begriff „Äquivalenzumformung“. Man formt eine Aussageform in eine äquivalente Aussageform um.

2. Quantoren

Wir betrachten die Aussageform $A(x, y)$ über den natürlichen Zahlen, die durch

$$A(x, y) :\Leftrightarrow x = 2y - 1$$

geben ist. Aus dieser Aussageform bilden wir eine Aussageform $B(x)$, die durch

$$B(x) :\Leftrightarrow \text{es gibt ein } y \in \mathbb{N}, \text{ sodass } A(x, y) \text{ gilt.}$$

definiert ist. $B(x)$ gilt also genau dann, wenn es ein y in den natürlichen Zahlen gibt, sodass $x = 2y - 1$. Die Aussageform $A(x, y)$ ist für folgende Paare (x, y) wahr: $(1, 1), (3, 2), (5, 3), (7, 4), (9, 5), \ldots$. Die Aussageform $B(x)$ ist genau dann wahr, wenn x eine ungerade natürliche Zahl ist.

Wir betrachten als nächstes folgende Aussageform $C(x, y)$ über den reellen Zahlen:

$$C(x, y) :\Leftrightarrow x^2 = y.$$

Wir bilden eine neue Aussageform $D(y)$ durch

$$D(y) :\Leftrightarrow \text{es gibt ein } x \in \mathbb{R}, \text{ sodass } C(x, y) \text{ gilt.}$$

Wir fragen uns nun, ob $D(2)$ gilt. Es gibt zwei x, die die Eigenschaft $C(x, 2)$ erfüllen, da $(\sqrt{2})^2 = 2$ und $(-\sqrt{2})^2 = 2$. Wir normieren die Bedeutung von „es gibt ein“ dahingehend, dass wir damit immer „es gibt mindestens ein“ meinen, und nicht „es gibt genau ein“. Somit ist $D(y)$ genau für die $y \in \mathbb{R}$ erfüllt, die $y \geq 0$ erfüllen. Die Aussageform $D(y)$ ist also äquivalent zu $y \geq 0$.

Definition 2.2. Sei $A(x, y_1, \ldots, y_n)$ eine Aussageform, die für alle $x, y_1, \ldots, y_n \in X$ definiert ist. Wir definieren eine neue Aussageform

$$B(y_1, \ldots, y_n) :\Leftrightarrow \text{es gibt ein } x \in X, \text{ sodass } A(x, y_1, \ldots, y_n).$$

Seien $b_1, b_2, \ldots, b_n \in X$. Dann ist $B(b_1, \ldots, b_n)$ genau dann wahr, wenn es mindestens ein $a \in X$ gibt, sodass $A(a, b_1, \ldots, b_n)$ wahr ist.

Für die neue Aussage $B(y_1, \ldots, y_n)$ schreiben wir auch

$$\exists x \in X : A(x, y_1, \ldots, y_n),$$

$(\exists x \in X)\,(A(x, y_1, \ldots, y_n))$, oder $(\exists x \in X)\, A(x, y_1, \ldots, y_n)$. Lies:

- Es gibt ein $x \in X$, sodass $A(x, y_1, \ldots, y_n)$.
- Es existiert ein $x \in X$, sodass $A(x, y_1, \ldots, y_n)$.
- Es gibt ein $x \in X$ mit $A(x, y_1, \ldots, y_n)$.
- Es existiert ein $x \in X$ mit $A(x, y_1, \ldots, y_n)$.

Wir nennen $\exists$ den *Existenzquantor*. Wenn wir aus einer Aussageform $A(x, y)$ die Aussageform $B(y) = (\exists x \in X)(A(x, y))$ machen, so wird die Variable x „verschluckt“; der Fachausdruck dafür ist, dass x durch den Quantor *gebunden* wird. Wenn eine Variable nicht durch einen Quantor gebunden wird, so heißt sie *frei*.

Wir betrachten nun folgende Aussageform über den reellen Zahlen:

$$E(x, y) :\Leftrightarrow x^2 \geq y.$$

Wir bilden nun eine neue Aussageform $F(y)$ durch

$$F(y) :\Leftrightarrow \text{für alle } x \in \mathbb{R} \text{ gilt } E(x, y).$$

$F(y)$ ist also genau dann wahr, wenn für alle $x \in \mathbb{R}$ gilt, dass $x^2 \geq y$. $F(y)$ ist äquivalent zu $y \leq 0$.

Definition 2.3. Sei $A(x, y_1, \ldots, y_n)$ eine Aussageform, die für alle $x, y_1, \ldots, y_n \in X$ definiert ist. Wir definieren eine neue Aussageform

$$B(y_1, \ldots, y_n) :\Leftrightarrow \text{für alle } x \in X \text{ gilt } A(x, y_1, \ldots, y_n).$$

Seien $b_1, b_2, \ldots, b_n \in X$. Dann ist $B(b_1, \ldots, b_n)$ genau dann wahr, wenn $A(a, b_1, \ldots, b_n)$ für alle $a \in X$ wahr ist.

Für die neue Aussage $B(y_1, \ldots, y_n)$ schreiben wir auch

$$\forall x \in X : A(x, y_1, \ldots, y_n),$$

$(\forall x \in X)\,(A(x, y_1, \ldots, y_n))$ oder $(\forall x \in X)\,A(x, y_1, \ldots, y_n)$ Lies:

$$\text{Für alle } x \in X \text{ gilt } A(x, y_1, \ldots, y_n).$$

Wir nennen $\forall$ den *Allquantor*.

Wir formulieren nun ein paar Zusammenhänge mithilfe dieser Quantoren. Wir betrachten folgende Aussage:

Es gibt eine gerade Zahl, die durch 3 und durch 5 teilbar ist.

Wir könnten das so schreiben: sei $G := \{2, 4, 6, \ldots\} = \{x \in \mathbb{N} \mid \exists k \in \mathbb{N} : x = 2k\}$ die Menge der positiven geraden Zahlen. Dann können wir die Aussage so schreiben:

$$\exists x \in G : (3|x) \wedge (5|x)$$

oder so:

$$\exists x \in \mathbb{N} : (x \in G) \wedge (3|x) \wedge (5|x).$$

Diese Aussage ist wahr. Das wird zum Beispiel von $x = 60$ belegt. Die Aussage „das Quadrat einer geraden Zahl ist ein Vielfaches von 4“ können wir so ausdrücken:

$$\forall x \in G : x^2 \text{ ist ein Vielfaches von } 4.$$

Oder, anders:

$$\forall x \in \mathbb{N} : (x \in G) \Rightarrow (4 \mid x^2).$$
$$\forall x \in \mathbb{N} : ((x \in G) \Rightarrow (\exists y \in \mathbb{N} : x^2 = 4y)).$$

Die letzte Zeile liest man etwa so

> Für alle x aus den natürlichen Zahlen gilt: wenn x ein Element von G ist, so gibt es ein y aus den natürlichen Zahlen, sodass x Quadrat gleich 4 mal y ist.

oder so:

> Für alle x aus $\mathbb{N}$ mit $x \in G$ gibt es ein y aus $\mathbb{N}$, sodass $x^2 = 4y$.

Interessant ist, dass die Formalisierung von

$$\text{Es gibt ein } x \in \mathbb{N} \text{ mit } A(x), \text{ sodass } B(x)$$

durch die logische Formel

$$\exists x \in \mathbb{N} : (A(x) \wedge B(x))$$

gegeben ist, die Formalisierung von

$$\text{Für alle } x \in \mathbb{N} \text{ mit } A(x) \text{ gilt } B(x)$$

aber durch

$$\forall x \in \mathbb{N} : A(x) \Rightarrow B(x).$$

Mithilfe mehrerer Quantoren kann man kompliziertere Aussageformen zusammenbauen. Betrachten wir etwa folgende Aussageformen über den reellen Zahlen:

$$\text{Für alle } x \in \mathbb{R} \text{ gibt es ein } y \in \mathbb{R}, \text{ sodass } ay = x.$$

Die Aussageform $ay = x$ ist eine Aussage über a, x, y. Somit ist

$$\forall x \in \mathbb{R} : (\exists y \in \mathbb{R} : ay = x)$$

eine Aussage über a. Die Variablen x und y sind durch Quantoren gebunden. Sie ist äquivalent zur Aussageform $a \neq 0$. Um das zu beweisen, nehmen wir zunächst an, dass $a \neq 0$ ist. Sei nun $x \in \mathbb{R}$. Es ist zu zeigen, dass es $y \in \mathbb{R}$ gibt, sodass $ay = x$. Wir wählen $y := \frac{x}{a}$. Dann gilt $ay = \frac{ax}{a} = x$. Somit belegt $y := \frac{x}{a}$ die Gültigkeit von $\exists y \in \mathbb{R} : ay = x$.

Nehmen wir nun an, dass $a \neq 0$ falsch ist, dass also $a = 0$. Dann gibt es für $x = 2$ kein y mit $0y = 2$. Somit widerlegt $x := 2$ die Gültigkeit von $\forall x \in \mathbb{R} : (\exists y \in \mathbb{R} : ay = x)$. Also ist dann $\forall x \in \mathbb{R} : (\exists y \in \mathbb{R} : ay = x)$ falsch.

Somit sind die beiden Aussagen äquivalent.

In anderer Schreibweise könnten wir für diese Aussageform

$$\forall x \in \mathbb{R} : (\exists y \in R : ay = x)$$

schreiben. Man lässt die Klammern auch oft weg und schreibt

$$\forall x \in \mathbb{R}\, \exists y \in \mathbb{R} \, : \, ay = x$$

oder

$$(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})\, (ay = x).$$

Die Reihenfolge der Quantoren darf man nicht einfach umdrehen. Wir betrachten dazu

$$\exists y \in \mathbb{R}\ \forall x \in \mathbb{R} \, : \, ay = x. \tag{2.1}$$

Diese Aussageform ist für alle $a \in \mathbb{R}$ falsch: Nehmen wir an, $a \in \mathbb{R}$ ist so, dass $\exists y \in \mathbb{R} \forall x \in \mathbb{R} \, : \, ay = x$ gilt. Dann gibt es ein $y \in \mathbb{R}$, sodass für alle $x \in \mathbb{R}$ gilt, dass $ay = x$. Damit gilt aber auch für $x = ay + 1$, dass $ay = ay + 1$. Das ist falsch. Dieser Widerspruch zeigt, dass die Annahme, dass es ein a gibt, für das (2.1) gilt, falsch ist. Somit ist (2.1) für jedes $a \in \mathbb{R}$ falsch.

Wir betrachten nun

$$\forall x \in \mathbb{R}\ \forall y \in \mathbb{R} \, : \, ay = x.$$

Das ist für alle $a \in \mathbb{R}$ falsch, da $x = 1$ und $y = 0$ die Gleichung $ay = x$ nicht erfüllen.

Die Aussageform

$$\exists x \in \mathbb{R}\ \forall y \in \mathbb{R} \, : \, ay = x$$

ist für $a = 0$ wahr, und sonst falsch. Wenn $a = 0$, so belegt $x = 0$, dass $\exists x \in \mathbb{R}, \forall y \in \mathbb{R} \, : \, ay = x$ wahr ist. Dann gilt nämlich für jedes $y \in \mathbb{R}$, dass $ay = 0y = 0 = x$. Wenn $a \neq 0$, so ist die Aussage falsch. Nehmen wir an, $x \in \mathbb{R}$ ist so, dass $\forall y \in \mathbb{R} \, : \, ay = x$ wahr ist. Dann gilt $a = a \cdot 1 = x = a \cdot 0 = 0$, im Widerspruch zur Annahme, dass $a = 0$. Also gibt es kein $x \in \mathbb{R}$ mit $\forall y \in \mathbb{R} \, : \, ay = x$.

Die Aussageform

$$\forall y \in \mathbb{R}\ \exists x \in \mathbb{R} \, : \, ay = x$$

ist für alle $a \in \mathbb{R}$ wahr. Sei dazu $a \in \mathbb{R}$ und $y \in \mathbb{R}$. Wir finden das gesuchte x als $x := ay$. Die Aussage

$$\forall a \in \mathbb{R}\ \forall y \in \mathbb{R}\ \exists x \in \mathbb{R} \, : \, ay = x$$

ist also wahr.

Die Aussageform

$$\exists y \in \mathbb{R}\ \exists x \in \mathbb{R} \, : \, ay = x$$

ist für alle $a \in \mathbb{R}$ wahr. Die Werte $y = a$ und $x = a^2$ belegen, dass $\exists y \in \mathbb{R}\ \exists x \in \mathbb{R} \, : \, ay = x$ wahr ist.

Mithilfe des Allquantors können wir auch die Begriffe *äquivalent*, *hinreichend* und *notwendig* besser beschreiben.

SATZ 2.4. *Seien $A(x_1, \ldots, x_n)$ und $B(x_1, \ldots, x_n)$ Aussageformen, die für alle $x_1, \ldots, x_n \in X$ definiert sind.*

(1) *$A(x_1, \ldots, x_n)$ und $B(x_1, \ldots, x_n)$ sind genau dann* äquivalent*, wenn die Aussage*

$$(\forall x_1 \in X)(\forall x_2 \in X) \ldots (\forall x_n \in X)\ (A(x_1, \ldots, x_n) \Leftrightarrow B(x_1, \ldots, x_n))$$

wahr ist.

(2) *$A(x_1, \ldots, x_n)$ ist genau dann* hinreichend *für $B(x_1, \ldots, x_n)$, wenn die Aussage*

$$(\forall x_1 \in X)(\forall x_2 \in X) \ldots (\forall x_n \in X)\ (A(x_1, \ldots, x_n) \Rightarrow B(x_1, \ldots, x_n))$$

wahr ist. Genau dann ist auch $B(x_1, \ldots, x_n)$ notwendig *für $A(x_1, \ldots, x_n)$.*

3. Rechenregeln für Quantoren

Die Rechenregeln für Quantoren sind schwieriger als die Rechenregeln für die Aussagenlogik. Wir halten nur einige Äquivalenzen fest.

SATZ 2.5 (Umbenennung von Variablen). *Seien $x, y_1, \ldots, y_n, z$ voneinander paarweise verschiedene Variablen, und sei $A(x, y_1, \ldots, y_n)$ eine Aussageform, die für alle Belegungen von $x, y_1, \ldots, y_n$ mit Werten aus X definiert ist. Dann gilt*

$$(\exists x \in X)\, A(x, y_1, \ldots, y_n) \equiv (\exists z \in X)\, A(z, y_1, \ldots, y_n)$$

und

$$(\forall x \in X)\, A(x, y_1, \ldots, y_n) \equiv (\forall z \in X)\, A(z, y_1, \ldots, y_n).$$

Beweisskizze: Seien $b_1, \ldots, b_n \in X$ so, dass $(\exists x \in X)\, A(x, b_1, \ldots, b_n)$ gilt. Dann gibt es ein $a \in X$, sodass $A(a, b_1, \ldots, b_n)$ gilt. Also belegt $z := a$, dass auch $(\exists z \in X)\, A(z, b_1, \ldots, b_n)$ gilt. Die umgekehrte Implikation und die Aussage über den Allquantor werden ganz ähnlich bewiesen. □

SATZ 2.6 (Vertauschung gleicher Quantoren). *Sei $A(x, y)$ eine Aussageform, die für alle $x \in X$ und $y \in Y$ definiert ist. Dann gilt:*

(1) $(\exists x \in X)(\exists y \in Y)\, A(x, y) \equiv (\exists y \in Y)(\exists x \in X)\, A(x, y)$.
(2) $(\forall x \in X)(\forall y \in Y)\, A(x, y) \equiv (\forall y \in Y)(\forall x \in X)\, A(x, y)$.

Der nächste Satz sagt, dass „nicht alle Schafe sind weiß“ äquivalent zu „es gibt ein Schaf, das nicht weiß ist“ ist.

SATZ 2.7 (Regel von De Morgan für Quantoren). *Sei $A(x)$ eine Aussageform, die für alle $x \in X$ definiert ist. Dann gilt:*

(1) $\neg((\exists x \in X)\, A(x)) \equiv (\forall x \in X)(\neg A(x))$.
(2) $\neg((\forall x \in X)\, A(x)) \equiv (\exists x \in X)(\neg A(x))$.

Beweis: (1): Wir nehmen zunächst an, dass $\neg((\exists x \in X)\, A(x))$ wahr ist. Wir wollen zeigen, dass $(\forall x \in X)(\neg A(x))$ gilt. Sei dazu $y \in X$. Wir wollen zeigen, dass $\neg A(y)$ wahr ist. Wenn $A(y)$ wahr ist, so gilt belegt dieses y, dass $(\exists x \in X)A(x)$ wahr ist, im Widerspruch zur Annahme. Also ist $A(y)$ falsch, und somit $\neg A(y)$ wahr. Insgesamt gilt also $(\forall x \in X)\,(\neg A(x))$.

Nehmen wir nun an, dass $(\forall x \in X)(\neg A(x))$ wahr ist. Wir wollen zeigen, dass $\neg((\exists x \in X)\, A(x))$ wahr ist. Dazu zeigen wir, dass $(\exists x \in X)\, A(x)$ falsch ist. Nehmen wir, im Widerspruch zur Behauptung, an, dass $(\exists x \in X)\, A(x)$ wahr ist. Sei $y \in X$ ein Element aus X, das das belegt, also so, dass $A(y)$ gilt. Dann ist $\neg A(y)$ falsch, im Widerspruch zur Annahme, dass $(\forall x \in X)\neg A(x)$ wahr ist. Somit ist die $(\exists x \in X)\, A(x)$ falsch.

(2): Vorlesung. □

Wir geben von weiteren Regeln über Quantoren nur eine Auswahl.

Satz 2.8 (Vorziehen des Quantors). *Seien $A(x)$ und $B(x, y)$ Aussageformen, die für alle $x \in X$ und $y \in Y$ definiert sind. Dann gilt:*

(1) $A(x) \wedge (\exists y \in Y)\, B(x, y) \equiv (\exists y \in Y)\, (A(x) \wedge B(x, y))$
(2) $A(x) \vee (\forall y \in Y)\, B(x, y) \equiv (\forall y \in Y)\, (A(x) \vee B(x, y))$.

Beweis: (1) Nehmen wir an, dass $a \in X$ so ist, dass $A(a) \wedge (\exists y \in Y)B(a, y)$ gilt. Dann gibt es ein $b \in Y$, sodass $B(a, b)$ gilt. Nun belegt dieses b, dass $(\exists y \in Y)\, (A(a) \wedge B(a, y))$ gilt.

Sei umgekehrt $a \in X$ so, dass $(\exists y \in Y)\, (A(a) \wedge B(a, y))$ gilt. Sei $b \in Y$ so, dass $A(a) \wedge B(a, b)$ gilt. Dann gilt $A(a)$, und b belegt, dass $(\exists y \in Y)B(a, y)$ gilt. Somit gilt $A(a) \wedge (\exists y \in Y)B(a, y)$.

Die beiden Aussageformen gelten also für die gleichen $a \in X$, und sind somit äquivalent.

(2) Vorlesung. □

Entscheidend ist hier, dass im Ausdruck $A(x)$ die Variable y nicht vorkommen darf.

Satz 2.9 (Vorziehen des Quantors). *Seien $A(x)$ und $B(x, y)$ Aussageformen, die für alle $x \in X$ und $y \in Y$ definiert sind. Wenn die Menge Y nicht leer ist, so gilt:*

(1) $A(x) \vee (\exists y \in Y)B(x, y) \equiv (\exists y \in Y)\, (A(x) \vee B(x, y))$.
(2) $A(x) \wedge (\forall y \in Y)B(x, y) \equiv (\forall y \in Y)\, (A(x) \wedge B(x, y))$.

Satz 2.10. *Sei $A(x, y)$ eine Aussageform, die für alle $x \in X$ und $y \in Y$ definiert ist. Wenn $(\exists x \in X)(\forall y \in Y)\, A(x, y)$ gilt, so auch $(\forall y \in X)(\exists x \in X)\, A(x, y)$.*

Wir schließen diesen Abschnitt mit einer auf den ersten Blick überraschenden Tautologie. Als *Tautologie* bezeichnet man eine Eigenschaft von Aussageformen, die für alle Aussageformen gilt, wie etwa $(\forall x \in X)\,(A(x) \vee (\neg A(x))$.

Satz 2.11. *Sei X eine nichtleere Menge, und sei $A(x)$ eine Aussageform, die für alle $x \in X$ definiert ist. Dann sind die folgenden Aussagen wahr:*

(1) $(\exists x \in X)\,\Big(A(x) \Rightarrow \big((\forall y \in X)\,A(y)\big)\Big)$.
(2) $(\exists x \in X)(\forall y \in X)\,\big((\neg A(x)) \vee A(y)\big)$.

Beweis: (1) Wir müssen ein $x \in X$ finden, sodass $A(x) \Rightarrow ((\forall y \in X)\,A(y))$ gilt. Wir betrachten dazu zwei Fälle.

- 1.Fall: $(\forall y \in X)\,A(y)$ *gilt*: Wir benutzen, dass X nicht leer ist und somit ein Element a besitzt. Wir setzen $x := a$. Es gilt dann $A(a) \Rightarrow ((\forall y \in X)\,A(y))$, da wegen der Fallannahme die Konklusion dieser Implikation wahr ist.
- 2.Fall: $(\forall y \in X)\,A(y)$ *gilt nicht*: Dann gilt $\neg((\forall y \in X)\,A(y))$, also $(\exists y \in X)(\neg A(y))$. Sei $a \in X$ so, dass $\neg A(a)$ gilt. Dann gilt $A(a) \Rightarrow ((\forall y \in X)\,A(y))$, da die Prämisse der Implikation falsch ist.

(2) Übung.

Übungsaufgaben 2.12.

(1) Zeigen Sie: Wenn Y nichtleer ist und $(\forall y \in Y)\,(C(y))$ gilt, so gilt auch $(\exists y \in Y)\,(C(y))$.
Zeigen Sie in den folgenden Beispielen jeweils, dass die Aussagen p und q nicht äquivalent sein müssen, indem Sie konkrete Aussageformen finden, sodass p und q nicht äquivalent sind.
(2) $p = (\forall x \in \mathbb{R})(\exists y \in \mathbb{R})\,A(x,y)$, $q = (\exists y \in \mathbb{R})(\forall x \in \mathbb{R})\,A(x,y)$. *Hinweis*: Versuchen Sie für $A(x,y)$ eine Gleichung in x und y.
(3) $p = (\forall x \in \mathbb{R})(\exists y \in \mathbb{R})\,A(x,y)$, $q = (\exists x \in \mathbb{R})(\forall y \in \mathbb{R})\,A(x,y)$.
(4) $p = (\exists x \in \mathbb{R})\,(A(x) \Rightarrow B)$, $q = ((\exists x \in \mathbb{R})\,A(x)) \Rightarrow B$.
Bestimmen Sie in den folgenden Beispielen, ob p und q für alle Aussageformen äquivalent sind.
(5) $p = \exists x \in \mathbb{R} : A(x) \wedge B(x)$, $q = (\exists x \in \mathbb{R} : A(x)) \wedge (\exists x \in \mathbb{R} : B(x))$.
(6) $p = \exists x \in \mathbb{R} : A(x) \vee B(x)$, $q = (\exists x \in \mathbb{R} : A(x)) \vee (\exists x \in \mathbb{R} : B(x))$.
(7) $p = \forall x \in \mathbb{R} : A(x) \vee B(x)$, $q = (\forall x \in \mathbb{R} : A(x)) \vee (\forall x \in \mathbb{R} : B(x))$.
(8) Seien A, B Aussageformen, sodass $(\forall x \in \mathbb{R})\,(A(x) \Rightarrow B(x))$ und $(\exists x \in \mathbb{R})\,A(x)$ beide gelten. Zeigen Sie, dass $(\exists x \in \mathbb{R})\,(A(x) \wedge B(x))$ gilt.
(9) Ist folgende Aussage für alle Aussageformen wahr? $(\exists x \in \mathbb{R})\,(\forall y \in \mathbb{R})\;(A(y) \Rightarrow A(x))$.
(10) Zeigen Sie Satz 2.11 (2).

Die Aussage von Satz 2.11 wird manchmal so formuliert:

> Es gibt immer einen, sodass, wenn der einen Hut trägt, alle einen Hut tragen.

Die Aussage $A(x)$ ist dann „x trägt einen Hut“. Abgesehen davon, dass diese Formulierung die Bedingung übergeht, dass die Menge X nicht leer sein soll, könnte sie in folgender Weise missverstanden werden:

> Es gibt ein $x \in X$, sodass für alle Aussageformen A gilt: wenn $A(x)$ gilt, so gilt für alle $y \in X$, dass $A(y)$.

In dieser Weise missverstanden heißt der obige Satz:

> Es gibt einen in unserer Gruppe, wir nennen ihn Franz, sodass folgendes gilt: wann immer Franz einen Hut auf hat, haben alle einen Hut auf.

Es ist aber offensichtlich, dass es so einen Franz nicht geben kann. Es ist nämlich möglich, dass Franz einen Hut trägt, aber sonst niemand. Der Satz mit dem Hut sollte also so verstanden werden:

> Für alle Aussageformen A gibt es ein $x \in X$ mit folgender Eigenschaft: wenn $A(x)$ gilt, so gilt für alle $y \in X$, dass $A(y)$.

Das ist jetzt genau die Aussage von Satz 2.11 , und wir können dieses x schnell finden. Übertragen auf die Formulierung mit dem Hut ist dieser eine jemand, der keinen Hut trägt, falls es so jemanden gibt, und irgendjemand sonst.

4. Weitere Quantoren

Manchmal verwendet man auch andere Quantoren, etwa in

$$\text{es gibt genau ein } x \in \mathbb{R}, \text{ sodass } x > 0 \text{ und } x^2 = 4.$$

Eine Schreibweise dafür ist

$$\exists!\, x \in \mathbb{R} : (x > 0 \wedge x^2 = 4).$$

Das kann man auch ohne den neuen Quantor $\exists!$ ausdrücken, etwa durch

$$\exists x \in \mathbb{R} : \Big((x > 0 \wedge x^2 = 4) \wedge \big(\forall y \in \mathbb{R} : ((y > 0 \wedge y^2 = 4) \Rightarrow y = x)\big)\Big).$$

Meistens ist es nützlich, die Aussage in eine Konjunktion von „es gibt mindestens ein“ und „es gibt höchstens ein“ zu verwandeln. Die Formalisierung ist dann

$$\big(\exists x \in \mathbb{R} : (x > 0 \wedge x^2 = 4)\big) \wedge \big(\forall y \in \mathbb{R}\ \forall z \in \mathbb{R}\ :\ (y > 0 \wedge y^2 = 4 \wedge z > 0 \wedge z^2 = 4) \Rightarrow y = z\big).$$

Satz 2.13. *Sei $A(x)$ eine Aussageform, die für alle $x \in X$ definiert ist. Dann sind folgende beiden Aussagen äquivalent.*

(1) $(\exists!\, x \in X)\, A(x)$.
(2) $\Big((\exists x \in X)\, A(x)\Big) \wedge \Big((\forall y \in X)(\forall z \in X)\, \big((A(y) \wedge (A(z))) \Rightarrow y = z\big)\Big)$

Auch andere Formulierungen, wie „es gibt kein“, „es gibt mindestens zwei“, „es gibt höchstens zwei“, ..., lassen sich mit $\exists, \forall, \neg$ und $=$ gut ausdrücken. Der Sinn davon ist, dass die gebräuchlichen Regeln unseres logischen Schließens genau zu

den Quantoren $\exists$ und $\forall$ passen. Einen Beweis von „es gibt genau ein“ führt man etwa oft dadurch, dass man zeigt, dass es mindestens ein Element gibt, und dass zwei Elemente, die beide die geforderte Bedingung erfüllen, gleich sein müssen. Man benützt also Satz 2.13.

Übungsaufgaben 2.14.

(1) Geben Sie Formulierungen von „es gibt kein $x \in X$ mit $A(x)$“, von „es gibt mindestens zwei $x \in X$ mit $A(x)$“, von „es gibt höchstens zwei $x \in X$ mit $A(x)$“ und von „es gibt genau zwei $x \in X$ mit $A(x)$“ an, in denen Sie nur die Quantoren $\exists$ und $\forall$ benützen.

KAPITEL 3

Mengen

1. Eigenschaften von Mengen

Unter einer *Menge* stellen wir uns eine Zusammenfassung von Objekten zu einem Ganzen vor. Wenn das Objekt a zur Menge M gehört, schreiben wir

$$a \in M,$$

und sagen, dass *a ein Element von M ist*. Zwei Mengen A, B sehen wir als gleich an, wenn sie dieselben Elemente enthalten. Diese Eigenschaft nennt man das *Extensionalitätsaxiom* oder *Axiom der Umfangsbestimmtheit*.

Wir geben zunächst in Form von Beispielen drei wichtige Arten an, in denen man eine Menge angeben kann. Die Menge $A = \{2, 3, 4\}$ ist die Menge, die genau die drei Zahlen 2,3 und 4 als Elemente besitzt. Als nächstes geben wir eine Menge B durch

$$B := \{x \in \mathbb{Z} \mid \exists y \in \mathbb{Z} : y^2 = x\}$$

an. Wir lesen das als „B ist die Menge der x in $\mathbb{Z}$, für die es ein y in $\mathbb{Z}$ gibt, sodass x gleich y zum Quadrat ist“. Die Menge B enthält also die Zahlen 1, 4, 9, 16, 25,.... Schließlich geben wir eine Menge C durch

$$C := \{x^2 \mid x \in \mathbb{Z}, x \leq -5\}$$

an. Wir lesen das als „C ist die Menge aller x^2, wobei x Element von $\mathbb{Z}$ ist, und $x \leq -5$ gilt“. C enthält also alle Quadratzahlen ab 25. Man kann diese Art, C anzugeben, auch als Kurzschreibweise für $C := \{y \mid \exists x : (y = x^2 \text{ und } x \in \mathbb{Z} \text{ und } x \leq -5)\}$ sehen.

Der Begriff *Menge* wird nicht präzise mathematisch definiert. Vielmehr gibt man einige Eigenschaften an, die Mengen unserer Vorstellung nach erfüllen sollen. Als Grundlage fast aller Teilgebiete der Mathematik haben sich jene Eigenschaften bewährt, die Ernst Zermelo (1871-1953), Abraham Fraenkel (1891-1965) und Thoralf Skolem (1887-1963) von 1907 bis 1929 von Mengen gefordert haben. Diese Eigenschaften sind die *Axiome der Zermelo-Fraenkel-Mengenlehre*. Die Zermelo-Fraenkel-Mengenlehre hat sich als ausgezeichnet geeignet herausgestellt, fast alle Resultate der Mathematik klar darzustellen und zu vermitteln. Zum anderen sind die Axiome auch theoretisch – in der Logik und der Mengenlehre – gut untersucht worden, ohne dass man bis heute einen Widerspruch in ihnen gefunden hätte. Wir

werden nicht alle Axiome diskutieren, aber zumindest das Extensionalitätsaxiom explizit angeben.

AXIOM 3.1 (Extensionalitätsaxiom). *Seien A, B Mengen. Dann gilt $A = B$ genau dann, wenn für alle $x \in A$ auch $x \in B$ gilt, und für alle $x \in B$ auch $x \in A$ gilt.*

Insbesondere gilt $\{1, 2\} = \{2, 1\} = \{2, 1, 1, 2, 2\} = \{x \in \mathbb{N} \mid x \leq 2\} = \{n \in \mathbb{N} \mid \exists a, b, c \in \mathbb{N} : a^n + b^n = c^n\}$, da diese Mengen alle genau dieselben Elemente enthalten. Dass auch die letzte Menge genau $\{1, 2\}$ ist, war allerdings 358 Jahre lang ein offenes Problem (Fermats letzter Satz), bevor es Andrew Wiles[1] im Jahr 1995 gelöst hat.

DEFINITION 3.2 (Teilmenge). Seien A, B Mengen. Dann gilt $A \subseteq B$ genau dann, wenn für alle $a \in A$ auch $a \in B$ gilt.

Wir können nun das Extensionalitätsaxiom so umformulieren:

> Seien A, B Mengen. Dann gilt $A = B$ genau dann, wenn $A \subseteq B$ und $B \subseteq A$.

Anstelle von $A \subseteq B$ schreiben wir auch manchmal $B \supseteq A$.

2. Operationen auf Mengen

Wir werden nun einige Operationen definieren, mithilfe derer wir aus gegebenen neue Mengen bilden können.

DEFINITION 3.3 (Durchschnitt und Vereinigung). Seien A, B Mengen. Dann definieren wir:

$$\begin{aligned} A \cap B &:= \{x \mid x \in A \text{ und } x \in B\}, \\ A \cup B &:= \{x \mid x \in A \text{ oder } x \in B\}. \end{aligned}$$

$A \cap B$ ist der *Durchschnitt* von A und B. $A \cup B$ ist die *Vereinigung* von A und B.

SATZ 3.4. *Seien A, B, C Mengen. Dann gilt:*

(1) $A \cap B = B \cap A$,
(2) $A \cup B = B \cup A$,
(3) $A \cup (B \cup C) = (A \cup B) \cup C$,
(4) $A \cap (B \cap C) = (A \cap B) \cap C$,
(5) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$,
(6) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

Wir zeigen zwei mögliche Arten, diese Gleichungen zu beweisen, und illustrieren diese Arten am Beispiel (5).

[1] Andrew Wiles, *1953

Beweis I von Satz 3.4 (5)*:* Es gilt

$$\begin{aligned}(A \cap B) \cup C &= \{x \mid x \in A \cap B \text{ oder } x \in C\} \\ &= \{x \mid (x \in A \wedge x \in B) \vee x \in C\}.\end{aligned}$$

Außerdem gilt

$$\begin{aligned}(A \cup C) \cap (B \cup C) &= \{x \mid x \in A \cup C \wedge x \in B \cup C\} \\ &= \{x \mid (x \in A \vee x \in C) \wedge (x \in B \vee x \in C)\}.\end{aligned}$$

Wir müssen also nachweisen, dass für alle x die Eigenschaft $(x \in A \wedge x \in B) \vee x \in C$ genau dann gilt, wenn $(x \in A \vee x \in C) \wedge (x \in B \vee x \in C)$. Sei dazu x fixiert. Wir beobachten, dass beide Aussagen aus den gleichen drei Aussagen $a := (x \in A)$, $b := (x \in B)$, und $c := (x \in C)$ zusammengebaut sind. Wir brauchen also nur 8 Fälle zu untersuchen, je nach dem ob a, b, c jeweils wahr oder falsch sind.

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

Wir sehen, dass $(a \vee c) \wedge (b \vee c)$ und $(a \wedge b) \vee c$ für alle Belegungen von a, b, c mit w und f den gleichen Wert annehmen. Somit gilt $(x \in A \wedge x \in B) \vee x \in C$ genau dann, wenn $(x \in A \vee x \in C) \wedge (x \in B \vee x \in C)$. Also gilt $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$. □

In diesem Beweis haben wir die Mengengleichheit $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ also auf die Äquivalenz der Aussagen $(a \wedge b) \vee c$ und $(a \vee c) \wedge (b \vee c)$ zurückgeführt. Kürzer könnte man diesen Beweis so formulieren: Es gilt

$$\begin{aligned}x \in (A \cup C) \cap (B \cup C) &\Leftrightarrow (x \in A \cup C) \wedge (x \in B \cup C) \\ &\Leftrightarrow ((x \in A) \vee (x \in C)) \wedge ((x \in B) \vee (x \in C)) \\ &\Leftrightarrow ((x \in A) \wedge (x \in B)) \vee (x \in C) \\ &\Leftrightarrow (x \in A \cap B) \vee (x \in C) \\ &\Leftrightarrow x \in (A \cap B) \cup C.\end{aligned}$$

Im zweiten Beweis benutzen wir jetzt eine Technik, die man oft zum Beweisen der Gleichheit zweier Mengen X und Y verwendet. Um $X = Y$ zu zeigen, beweisen wir $X \subseteq Y$ und $Y \subseteq X$. Das Extensionalitätsaxiom sagt dann, dass X und Y gleich sind.

Beweis II von Satz 3.4: Um zu zeigen, dass

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C), \tag{3.1}$$

zeigen wir, dass $(A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C)$ und dass $(A \cap B) \cup C \supseteq (A \cup C) \cap (B \cup C)$. „$\subseteq$“: Sei $x \in (A \cap B) \cup C$. Wir wollen zeigen, dass $x \in (A \cup C) \cap (B \cup C)$.

Dazu zeigen wir zuerst, dass $x \in A \cup C$. Da $x \in (A \cap B) \cup C$, wissen wir, dass $x \in A \cap B$ oder $x \in C$.

- *1.Fall:* $x \in A \cap B$*:* Da dann $x \in A \cap B$, gilt $x \in A$, und somit $x \in A \cup C$.
- *2.Fall:* $x \in C$*:* Dann liegt x in $A \cup C$.

Somit liegt x also in $A \cup C$.

Nun zeigen wir, dass $x \in B \cup C$. Da $x \in (A \cap B) \cup C$, wissen wir, dass x in $A \cap B$ oder in C liegt.

- *1.Fall:* $x \in A \cap B$*:* Dann gilt $x \in B$, und somit $x \in B \cup C$.
- *2.Fall:* $x \in C$*:* Dann liegt x in $B \cup C$.

Somit liegt x also in $B \cup C$.

Daher liegt x also sowohl in $A \cup C$ als auch in $B \cup C$, und somit gilt $x \in (A \cup C) \cap (B \cup C)$.

„$\supseteq$“: Sei $x \in (A \cup C) \cap (B \cup C)$. Wir wollen zeigen, dass $x \in (A \cap B) \cup C$. Wir betrachten dazu zwei Fälle.

- *1. Fall:* $x \in C$*:* Dann liegt x auch in $(A \cap B) \cup C$.
- *2. Fall:* $x \notin C$*:* Da x in $(A \cup C) \cap (B \cup C)$ liegt, gilt $x \in A \cup C$. Da $x \notin C$, gilt also $x \in A$. Da x in $(A \cup C) \cap (B \cup C)$ liegt, gilt auch $x \in B \cup C$. Da $x \notin C$, gilt also $x \in B$. Insgesamt gilt also $x \in A \cap B$, und somit $x \in (A \cap B) \cup C$.

□

Übungsaufgaben 3.5.

(1) Zeigen Sie die übrigen Aussagen von Satz 3.4. Versuchen Sie, Beweise in beiden der illustrierten Arten (also einmal durch Verwendung von Gleichheiten der Aussagenlogik, und einmal durch Beweisen von zwei Inklusionen) anzugeben.

Definition 3.6. Seien A, B Mengen. Dann ist $B \setminus A$ definiert durch

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

Dabei steht $x \notin A$ für (nicht $x \in A$).

Wenn man nur Mengen betrachtet, die Teilmengen einer Menge U, des *Universums*, sind, so schreibt man auch $\complement_U B$ für $U \setminus B$. Es gelten etwa folgende Zusammenhänge:

SATZ 3.7. *Seien A, B, C, U Mengen, sodass A, B, C Teilmengen von U sind. Dann gilt:*

(1) $B \setminus A = B \cap (\complement_U A)$,
(2) $C \setminus (B \setminus A) = (A \cap C) \cup (C \setminus B)$,
(3) *(De Morgansche Regeln)* $\complement_U(A \cap B) = \complement_U(A) \cup \complement_U(B)$ *und* $\complement_U(A \cup B) = \complement_U(A) \cap \complement_U(B)$.

Beweis von (2)*:* Es gilt

$$\begin{aligned} x \in (C \setminus (B \setminus A)) &\Leftrightarrow x \in C \wedge (x \notin B \setminus A) \\ &\Leftrightarrow x \in C \wedge \neg(x \in B \wedge x \notin A) \\ &\Leftrightarrow x \in C \wedge (x \notin B \vee x \in A) \\ &\Leftrightarrow (x \in C \wedge x \notin B) \vee (x \in C \wedge x \in A) \\ &\Leftrightarrow (x \in C \setminus B) \vee (x \in C \cap A) \\ &\Leftrightarrow x \in (C \setminus B) \cup (C \cap A). \end{aligned}$$

ÜBUNGSAUFGABEN 3.8.

(1) Zeigen Sie die übrigen Aussagen von Satz 3.7.
(2) Seien A, B, C Mengen mit $A \cap C = \varnothing$ und $A \cup C = B$. Zeigen Sie, dass $C = B \setminus A$.
(3) Gilt für alle Mengen A, B, C, dass $A \setminus (B \setminus C) = (A \cap C) \cup (A \setminus B)$?
(4) Gilt für alle Mengen A, B, C, dass $(A \setminus C) \setminus (C \setminus B) = A \cup B$?

Mit $\varnothing$ bezeichnen wir die leere Menge, die kein Element enthält. Für jede Menge A gilt $\varnothing \subseteq A$ und $A \setminus A = \varnothing$.

DEFINITION 3.9. Seien A, B Mengen. Mit $A\Delta B$ bezeichnen wir die Menge

$$A\Delta B := (A \setminus B) \cup (B \setminus A).$$

$A\Delta B$ heißt die *symmetrische Differenz* von A und B. Ein Element x liegt also in $A\Delta B$, wenn es in genau einer der Mengen A und B enthalten ist, wenn also $(x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)$ gilt. Wir werden im folgenden auch brauchen, wann ein Element *nicht* in $A\Delta B$ liegt. Es gilt

$$x \notin A\Delta B \Leftrightarrow (x \in A \wedge x \in B) \vee (x \notin A \wedge x \notin B).$$

SATZ 3.10. *Seien A, B, C Mengen. Es gilt:*

(1) $A\Delta B = (A \cup B) \setminus (A \cap B)$.
(2) $(A\Delta B)\Delta C = A\Delta(B\Delta C)$.
(3) $A\Delta B = B\Delta A$.
(4) $A\Delta\varnothing = A$.
(5) $A\Delta A = \varnothing$.
(6) $(A\Delta B) \cap C = (A \cap C)\Delta(B \cap C)$.

Beweis: Wir zeigen (2). Dazu beobachten wir, dass für jedes x gilt:

$$\begin{aligned} x \in (A\Delta B)\Delta C &\Leftrightarrow (x \in (A\Delta B) \setminus C) \vee (x \in C \setminus (A\Delta B)) \\ &\Leftrightarrow (x \in (A\Delta B) \wedge x \notin C) \vee (x \in C \wedge x \notin (A\Delta B)) \\ &\Leftrightarrow (((x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)) \wedge x \notin C) \\ &\quad \vee (x \in C \wedge ((x \in A \wedge x \in B) \vee (x \notin A \wedge x \notin B))) \\ &\Leftrightarrow (x \in A \wedge x \notin B \wedge x \notin C) \vee (x \notin A \wedge x \in B \wedge x \notin C) \\ &\quad \vee (x \in A \wedge x \in B \wedge x \in C) \vee (x \notin A \wedge x \notin B \wedge x \in C). \end{aligned}$$

Ähnliche Berechnung zeigen, dass $x \in A\Delta(B\Delta C)$ ebenfalls genau dann gilt, wenn $(x \in A \wedge x \notin B \wedge x \notin C) \vee (x \notin A \wedge x \in B \wedge x \notin C) \vee (x \in A \wedge x \in B \wedge x \in C) \vee (x \notin A \wedge x \notin B \wedge x \in C)$. Das beweist (2)

Wir beweisen nun (6), indem wir beide Inklusionen zeigen. Sei dazu $x \in (A\Delta B) \cap C$. Da $x \in A\Delta B$ liegt, gilt $x \in A \wedge x \notin B$ oder $x \notin A$ und $x \in B$.

- 1.Fall: $x \in A \wedge x \notin B$: Da $x \in C$, gilt $x \in (A \cap C)$. Es gilt $x \notin (B \cap C)$. Insgesamt gilt also $x \in ((A \cap C)\Delta(B \cap C))$.
- 2.Fall: $x \notin A \wedge x \in B$: Da $x \in C$, gilt $x \in (B \cap C)$. Es gilt $x \notin (A \cap C)$. Insgesamt gilt also $x \in ((A \cap C)\Delta(B \cap C))$.

Somit ist die Inklusion $\subseteq$ gezeigt.

Für $\supseteq$ wählen wir $x \in (A \cap C)\Delta(B \cap C)$. Da $x \in (A \cap C)\Delta(B \cap C)$ liegt, gilt $x \in (A \cap C) \wedge x \notin (B \cap C)$ oder $x \notin (A \cap C) \wedge x \in (B \cap C)$.

- 1. Fall: $x \in (A \cap C) \wedge x \notin (B \cap C)$: Da $x \in A \cap C$ gilt $x \in C$ und $x \in A$. Da $x \in C$ und $x \notin B \cap C$, gilt $x \notin B$. Somit gilt $x \in (A\Delta B)$ und $x \in C$, also $x \in (A\Delta B) \cap C$.
- 2. Fall: $x \notin (A \cap C) \wedge x \in (B \cap C)$: Da $x \in B \cap C$ gilt $x \in C$ und $x \in B$. Da $x \in C$ und $x \notin A \cap C$, gilt $x \notin A$. Somit gilt $x \in (A\Delta B)$ und $x \in C$, also $x \in (A\Delta B) \cap C$.

□

Übungsaufgaben 3.11.

(1) Sei $n \in \mathbb{N}$, und seien $A_1, \ldots, A_n$ Mengen. Zeigen Sie, dass $x \in ((\ldots((A_1\Delta A_2)\Delta A_3)\Delta \ldots)\Delta A_{n-1})\Delta A_n$ genau dann gilt, wenn x in einer ungeraden Anzahl der Mengen $A_1, \ldots, A_n$ enthalten ist. *Hinweis:* Induktion nach n.

Definition 3.12. Sei A eine Menge. Dann ist die Menge $\mathcal{P}(A)$, die *Potenzmenge* von A, definiert durch

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

Es gilt etwa $\mathcal{P}(\{1,2\}) = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$.

Satz 3.13. *Sei $n \in \mathbb{N}$, und sei $A = \{1, 2, \ldots, n\}$. Dann hat $\mathcal{P}(A)$ genau 2^n Elemente.*

Beweis: Wir beweisen diesen Satz mit Induktion. Sei $n = 1$. Dann gilt $A = \{1\}$ und $\mathcal{P}(A) = \{\varnothing, \{1\}\}$. Die Menge $\mathcal{P}(A)$ hat also genau 2 Elemente. Wir nehmen nun an, dass $n \in \mathbb{N}$, und dass $\mathcal{P}(\{1, \ldots, n\})$ genau 2^n Elemente hat. Wir berechnen nun $\mathcal{P}(\{1, \ldots, n+1\})$. Es gilt

$$\begin{aligned}\mathcal{P}(\{1, \ldots, n, n+1\}) &= \{B \mid B \subseteq \{1, \ldots, n+1\} \wedge n+1 \in B\} \\ &\quad \cup \{B \mid B \subseteq \{1, \ldots, n+1\} \wedge n+1 \notin B\} \\ &= \{C \cup \{n+1\} \mid C \subseteq \{1, \ldots, n\}\} \\ &\quad \cup \{C \mid C \subseteq \{1, \ldots, n\}\}.\end{aligned}$$

Die Menge $\{C \mid C \subseteq \{1, \ldots, n\}\}$ ist die Menge $\mathcal{P}(\{1, \ldots, n\})$. Nach der Induktionsannahme hat diese Menge 2^n Elemente. Da verschiedene Teilmengen von $\{1, \ldots, n\}$ durch Hinzufügen von $n+1$ verschieden bleiben, hat auch $\{C \cup \{n+1\} \mid C \subseteq \{1, \ldots, n\}\}$ genau 2^n Elemente. Schließlich haben $\{C \cup \{n+1\} \mid C \subseteq \{1, \ldots, n\}\}$ und $\{C \mid C \subseteq \{1, \ldots, n\}\}$ keine Elemente gemeinsam, es gilt daher

$$\{C \cup \{n+1\} \mid C \subseteq \{1, \ldots, n\}\} \cap \{C \mid C \subseteq \{1, \ldots, n\}\} = \varnothing.$$

Also hat ihre Vereinigung $2^n + 2^n = 2^{n+1}$ Elemente. Insgesamt haben wir gezeigt, dass $\mathcal{P}(\{1, \ldots, n+1\})$ genau 2^{n+1} Elemente hat; damit ist auch der Induktionsschritt gelungen. □

Übungsaufgaben 3.14.

(1) Gilt für alle Mengen A, B, dass $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$?
(2) Gilt für alle Mengen A, B, dass $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$?

Wenn eine Menge A genau n verschiedene Elemente hat (mit $n \in \mathbb{N}_0$), so schreiben wir $|A| = n$ (oder $\#A = n$). Eine solche Menge nennen wir auch n-elementig, und wir sagen, n ist die *Kardinalität* oder *Mächtigkeit* der Menge. Eine Menge, für die es kein solches $n \in \mathbb{N}_0$ gibt, bezeichnen wir als *unendlich*. Manchmal schreibt man $|A| = \infty$. Eine genauere Unterscheidung zwischen „verschieden großen“ unendlichen Mengen werden wir in Kapitel **??** vornehmen.

Wir halten nun die Kardinalität einiger endlichen Mengen fest.

Satz 3.15. *Seien $A, B, A_1, \ldots, A_n$ endliche Mengen. Dann gilt:*

(1) *Wenn $A \cap B = \varnothing$, so gilt $|A \cup B| = |A| + |B|$.*
(2) *Wenn für alle $i, j \in \{1, \ldots, n\}$ mit $i \neq j$ gilt, dass $A_i \cap A_j = \varnothing$, so gilt: $|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$.*
(3) *Es gilt $|A \cup B| = |A| + |B| - |A \cap B|$.*

Beweis: Wir beweisen hier nur die Eigenschaft (3). Da $A \setminus B$ und B disjunkt sind, und $A \cup B = (A \setminus B) \cup B$, gilt

$$|A \cup B| = |A \setminus B| + |B|. \tag{3.2}$$

Nun gilt $(A \cap B) \cup (A \setminus B) = A$ und $(A \cap B) \cap (A \setminus B) = \varnothing$. Folglich gilt $|A \cap B| + |A \setminus B| = |A|$. Wenn man nun in Gleichung (3.2) $|A \setminus B|$ durch $|A| - |A \cap B|$ ersetzt, so erhält man $|A \cup B| = |A| + |B| - |A \cap B|$. □

Satz 3.16. *Sei A eine Menge mit n Elementen, und sei $i \in \{0, \ldots, n\}$. Dann hat A genau $\binom{n}{i} = \frac{n!}{i!(n-i)!}$ Teilmengen mit i Elementen.*

Beweis: Zunächst zeigen wir, dass für $n \in \mathbb{N}$ und $i \in \{1, \ldots, n-1\}$ gilt:

$$\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}. \tag{3.3}$$

Es gilt $\binom{n-1}{i} + \binom{n-1}{i-1} = \frac{(n-1)!}{(n-1-i)!\,i!} + \frac{(n-1)!}{(n-i)!\,(i-1)!} = \frac{(n-1)! \cdot (n-i) + (n-1)! \cdot i}{(n-i)!\,i!} = \frac{(n-1)! \cdot n}{(n-i)!\,i!} = \frac{n!}{(n-i)!\,i!} = \binom{n}{i}$. Das beweist (3.3). Nun zeigen wir den Satz mit Induktion nach n. Für $n = 1$ sehen wir, dass eine einelementige Menge genau eine nullelementige und eine einelementige Teilmenge hat. Sei nun $n \geq 2$. Für $i = 0$ sehen wir, dass A genau eine nullelementige Teilmenge, nämlich $\varnothing$, hat. Für $i = n$ hat A genau eine n-elementige Teilmenge, nämlich A. Sei nun $i \in \{1, \ldots, n-1\}$. Wir wählen ein Element a aus A. Es gilt

$$\begin{aligned}\{B \mid B \subseteq A, |B| = i\} &= \{B \mid B \subseteq A, |B| = i, a \notin B\} \cup \{B \mid B \subseteq A, |B| = i, a \in B\} \\ &= \{B \mid B \subseteq A \setminus \{a\}, |B| = i\} \\ &\quad \cup \{B \cup \{a\} \mid B \subseteq A \setminus \{a\}, |B| = i - 1\}.\end{aligned}$$

Nun hat die erste dieser Mengen $\binom{n-1}{i}$ und die zweite $\binom{n-1}{i-1}$ Elemente. Somit gilt $|\{B : B \subseteq A, |B| = i\}| = \binom{n-1}{i} + \binom{n-1}{i-1} = \binom{n}{i}$. □

Es gibt Mengen, deren Elemente wiederum allesamt Mengen sind. Wir geben jetzt der Vereinigung aller Elemente einer Menge und dem Durchschnitt aller Elemente einer Menge eine Abkürzung.

Definition 3.17. Sei $\mathcal{A}$ eine Menge, deren Elemente alle Mengen sind. Mit $\bigcup \mathcal{A}$ oder $\bigcup_{A \in \mathcal{A}} A$ bezeichnen wir die Menge, die durch

$$\bigcup \mathcal{A} = \{x \mid \exists A \in \mathcal{A} : x \in A\}$$

definiert ist.

Beispiele:

- $\bigcup \{\{1, 2\}, \{2, 5\}, \{1, 5, 0\}\} = \{0, 1, 2, 5\}$.
- $\bigcup_{n \in \mathbb{N}}]n, n+1[= \{x \in \mathbb{R}^+ \mid x \geq 1\} \setminus \mathbb{N}$.
- $\bigcup \varnothing = \varnothing$.

DEFINITION 3.18. Sei $\mathcal{A}$ eine nichtleere Menge, deren Elemente alle Mengen sind. Mit $\bigcap \mathcal{A}$ oder $\bigcap_{A\in\mathcal{A}} A$ bezeichnen wir die Menge, die durch

$$\bigcap \mathcal{A} = \{x \mid \forall A \in \mathcal{A} : x \in A\}$$

definiert ist.

Beispiel: $\bigcap\{\{1,2\},\{2,5\},\{2,6\}\} = \{2\}$, $\bigcap\{]n, n+1[\mid n \in \mathbb{N}\} = \bigcap_{n\in\mathbb{N}}]n, n+1[= \varnothing$.

ÜBUNGSAUFGABEN 3.19.

(1) Geben Sie die Menge
$$A = \bigcup_{i\in\mathbb{N}} \{(a, a+i) \mid a \in \mathbb{N}\}$$
in der Form $A = \{(c,d) \in \mathbb{N}\times\mathbb{N} \mid \ldots\ldots\}$ an.
(2) Bestimmen Sie die Menge
$$B = \bigcap_{i\in\mathbb{N}} \{(a, a+i) \mid a \in \mathbb{N}\}.$$
Begründen Sie Ihre Antwort.

3. Geordnete Paare

DEFINITION 3.20. Für beliebige a, b definieren wir das *geordnete Paar* (a, b) durch

$$(a, b) := \{\{a\}, \{a, b\}\}.$$

SATZ 3.21. *Für alle a, b, c, d gilt $(a, b) = (c, d)$ genau dann, wenn $a = c$ und $b = d$.*

Beweis: Wenn $a = c$ und $b = d$, so gilt $(a, b) = \{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} = (c, d)$.

Wir zeigen nun, dass aus $(a, b) = (c, d)$ folgt, dass $a = c$ und $b = d$. Seien dazu a, b, c, d so, dass $(a, b) = (c, d)$. Wir wissen also, dass $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$.

- *1.Fall: $a \neq b$:* Wir wissen, dass $\{c\} \in \{\{a\}, \{a, b\}\}$. Da $\{a, b\}$ nicht einelementig ist, kann nur $\{c\} = \{a\}$ gelten. Dann gilt $a = c$. Somit gilt also $\{\{a\}, \{a, b\}\} = \{\{a\}, \{a, d\}\}$. Da $\{a, b\} \neq \{a\}$, muss $\{a, b\} = \{a, d\}$ gelten. Somit gilt $b \in \{a, d\}$, und folglich $b = d$.
- *2.Fall: $a = b$:* Dann gilt $\{\{a\}\} = \{\{c\}, \{c, d\}\}$. Also gilt $\{c, d\} = \{a\}$, und somit $c = d = a$. Also gilt $a = c$ und $d = b$.

DEFINITION 3.22. Seien A, B Mengen. Wir definieren $A \times B$, das *kartesische Produkt von A und B*, durch

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

SATZ 3.23. *Seien A, B, X, Y Mengen. Dann gilt*

(1) $(A \cup B) \times X = (A \times X) \cup (B \times X)$,
(2) $(A \cap B) \times (X \cap Y) = (A \times X) \cap (B \times Y)$,
(3) $\varnothing \times B = \varnothing$.
(4) *Wenn* $A \times B = \varnothing$, *so gilt* $A = \varnothing$ *oder* $B = \varnothing$.

Beweis: Wir geben nur die Beweise von (1) und (4) an. (1): Es gilt $(x, y) \in (A \cup B) \times X \Leftrightarrow (x \in A \vee x \in B) \wedge y \in X \Leftrightarrow (x \in A \wedge y \in X) \vee (x \in B \wedge y \in X) \Leftrightarrow (x, y) \in (A \times X) \cup (B \times X)$. (4): Nehmen wir an $A \neq \varnothing$ und $B \neq \varnothing$. Dann gibt es $a \in A$ und $b \in B$. Somit gilt $(a, b) \in A \times B$, und folglich gilt $A \times B \neq \varnothing$. $\square$

Teil 2

Die natürlichen Zahlen

KAPITEL 4

Die natürlichen Zahlen

1. Der Aufbau der natürlichen Zahlen

In diesem Kapitel geht es darum, die Menge

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

näher zu bestimmen. Man verwendet allgemein die natürlichen Zahlen und ihre Arithmetik, etwa $7 \cdot 8 = 56$ oder $\forall x, y \in \mathbb{N} : x \cdot y = y \cdot x$ mit großer Selbstverständlichkeit. Wenn man aber versucht, etwa $\forall x, y \in \mathbb{N} : x \cdot y = y \cdot x$ zu *beweisen*, fehlen eine Definition der natürlichen Zahlen und der Rechenoperationen. Giuseppe Peano[1] hat die Eigenschaften der natürlichen Zahlen, die man man für die Entwicklung ihrer Theorie braucht, als *Axiome* zusammengestellt. Peano schreibt[2]:

> „Die Aussagen, die durch die Operationen der Logik von anderen abgeleitet werden, sind *Sätze*; die, die in Wahrheit nicht [abgeleitet werden], habe ich *Axiome* genannt. Axiome gibt es hier neun, und sie drücken die grundlegenden Eigenschaften der Zeichen, die keine Definition besitzen, aus."

Wir passen die Peano-Axiome an unsere Schreibweise an. Außerdem lassen wir die Axiome aus, die die Bedeutung des Gleichheitszeichens erklären.

Axiome 4.1 (Peano-Axiome, [**Pea89**]). $\mathbb{N}$ *bedeutet die Menge der positiven ganzen Zahlen,* $a + 1$ *ist der Nachfolger von* a*.*

(1) $1 \in \mathbb{N}$*.*
(6) *Für alle* $a \in \mathbb{N}$ *gilt* $a + 1 \in \mathbb{N}$*.*
(7) *Für alle* $a, b \in \mathbb{N}$ *gilt:* $a = b \Leftrightarrow a + 1 = b + 1$*.*
(8) *Für alle* $a \in \mathbb{N}$ *gilt* $a + 1 \neq 1$*.*
(9) *Für alle Mengen* k*, die folgende Eigenschaft erfüllen:*

$$1 \in k \text{ und } \forall x \in k : x + 1 \in k$$

gilt $\mathbb{N} \subseteq k$*.*

[1] Giuseppe Peano, 1858–1932
[2] Übersetzung und Anpassung an unsere Sprechweise vom Autor des Skriptums

Wir schreiben nun den Nachfolger von a als a^+. Peano definiert dann die Addition rekursiv durch $a+1 = a^+$ und $a+(b^+) = (a+b)^+$. Das erlaubt, etwa $2+3$ wirklich zu berechnen: $2+3 = 1^+ + 1^{++} = (1^+ + 1^+)^+ = (1^+ + 1)^{++} = (1^{++})^{++} = 1^{++++} = 5$. Das ist ineffizient, hat aber den Nutzen, dass wir jetzt Eigenschaften, wie etwa $\forall x, y \in \mathbb{N} : x + y = y + x$ *beweisen* können. Die Existenz der natürlichen Zahlen wird so aber nicht erklärt, sondern einfach postuliert.

Heute baut man die Mathematik lieber aus der Mengenlehre auf, da sich die Mengenlehre als sehr gut geeignet herausgestellt hat, die Ergebnisse der verschiedensten Gebiete der Mathematik auszudrücken. Man braucht auch dann Axiome: das sind heute üblicherweise die Axiome der Zermelo-Fraenkelschen Mengenlehre. Wenn man nun bereits Mengen zur Verfügung hat, kann man eine Menge und eine Nachfolgerfunktion definieren, die die Eigenschaften der Peano-Axiome erfüllen. Damit verlieren die Peano-Axiome ihren Status als Axiome, und sind nur mehr Sätze. Die folgende Konstruktion der natürlichen Zahlen stammt von John von Neumann[3] aus dem Jahr 1923. Sie scheint zunächst umständlich und beweist ihre ganze Kraft tatsächlich erst bei der Beschreibung von unendlichen Mengen, die, in gewissem Sinn, größer als die Menge der natürlichen Zahlen sind. Als erstes definiert man für jede Menge x eine Menge x^+ durch

$$x^+ := x \cup \{x\}$$

und nennt sie den *Nachfolger* von x. Nun definiert man

$$0 := \varnothing,\ 1 := 0^+ = \varnothing^+ = \varnothing \cup \{\varnothing\} = \{\varnothing\}, \tag{4.1}$$
$$2 := 1^+ = \{\varnothing, \{\varnothing\}\},\ 3 := 2^+ = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \ldots$$

Man fordert dann, als Axiom (*Unendlichkeitsaxiom*), dass es eine Menge U gibt, die 0 enthält, und mit jedem x auch seinen Nachfolger x^+. Eine solche Menge enthält zumindest $0, 0^+, (0^+)^+, \ldots$. Schließlich definiert man $\mathbb{N}_0$ als Durchschnitt aller Teilmengen von U, die 0 enthalten, und mit jedem Element auch dessen Nachfolger. Das hat folgende Nachteile:

(1) Die Elemente sind sehr unhandlich, so ist etwa $3 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$. Die Darstellung braucht also viel mehr Platz als das heute verwendete Stellenwertsystem, das vermutlich bereits vor 500 n.Chr. erfunden worden ist. In dieser Darstellung braucht man für die Darstellung der Zahl n insgesamt $2^{n+1} - 1$ Symbole. Selbst die Vereinfachung $3 = 0^{+++}$ braucht für die Zahl n immer noch $n+1$ Symbole. Das Stellenwertsystem kommt mit $\lfloor \log_{10}(n) \rfloor + 1$ Symbolen aus.
(2) Es ergeben sich ungewöhnliche Gleichheiten, etwa $\{0\} = 1$, $2 = 1 \cup (\varnothing, \varnothing)$, die man außerhalb der Mengenlehre als falsch ansehen würde.

[3] John von Neumann, 1903–1957

(3) Das Unendlichkeitsaxiom und die anderen Axiome der Mengenlehre sind nicht unmittelbar als unverrückbar wahr einsichtig. Dagegen formalisieren die Peano-Axiome Tatsachen, die unmittelbar unserer Vorstellung vom Zählen entsprechen.

Vorteile sind:

(1) Man braucht keine neuen Objekte, sondern kann die in der Mengenlehre bereits vorhandenen Objekte, wie etwa $\varnothing, \{\varnothing\}, \ldots$ verwenden.
(2) Man braucht keine neuen unbewiesenen Behauptungen, wie etwa die Peano-Axiome, hinzuzunehmen, sondern findet mit den Axiomen der Mengenlehre das Auslangen. Man reduziert daher die Gefahr, dass die Axiome einander widersprechen.
(3) Die Anordnung der natürlichen Zahlen lässt sich leicht beschreiben: Es gilt $x \leq y$ genau dann, wenn $x \subseteq y$.
(4) Von Neumanns Konstruktion lässt sich auf „größere“ Mengen verallgemeinern. Dafür hat er sie auch erfunden.

In dieser Betrachtungsweise erhält man Peanos Axiome dann als Satz.

Satz 4.2 (Peano-Axiome in der Sichtweise der Mengenlehre). *Es gilt:*

(1) $0 \in \mathbb{N}_0$.
(2) *Für alle* $n \in \mathbb{N}_0$ *gilt* $n^+ \in \mathbb{N}_0$.
(3) *Es gibt kein* $n \in \mathbb{N}_0$ *mit* $n^+ = 0$.
(4) *Für alle* $n, m \in \mathbb{N}_0$ *mit* $n^+ = m^+$ *gilt auch* $n = m$.
(5) *Für alle Teilmengen* S *von* $\mathbb{N}_0$ *gilt: Wenn*

$$0 \in S \text{ und } \forall n \in S : n^+ \in S \tag{4.2}$$

gelten, so gilt $S = \mathbb{N}_0$.

Beweis: Die Eigenschaften (1) und (2) ergeben sich daraus, dass $\mathbb{N}_0$ als Durchschnitt von lauter solchen Mengen definiert wurde, die (1) und (2) erfüllen. Wenn wir lauter Mengen schneiden, die 0 als Element enthalten, enthält deren Durchschnitt wieder 0. Ebenso bleibt der Durchschnitt abgeschlossen unter $^+$. Für die Eigenschaft (3) nehmen wir an, dass $n^+ = 0$. Dann gilt $n \cup \{n\} = \varnothing$, also $n \in \varnothing$. Das ist eine falsche Aussage, weil die leere Menge kein Element hat. Wir zeigen nun (5). Sei S eine Teilmenge von $\mathbb{N}_0$, die die Eigenschaft (4.2) erfüllt. Dann ist S eine jener Mengen, als deren Durchschnitt $\mathbb{N}_0$ definiert wurde. Somit gilt $\mathbb{N}_0 \subseteq S$. Also gilt insgesamt $S \subseteq \mathbb{N}_0$ und $\mathbb{N}_0 \subseteq S$, und somit $\mathbb{N}_0 = S$. Den Beweis von (4) machen wir in zwei Schritten: wir zeigen zuerst:

$$\forall i \in \mathbb{N}_0 \, \forall x \in \mathbb{N}_0 \, : \, x \in i \Rightarrow x \subseteq i. \tag{4.3}$$

Für den Beweis von (4.3) zeigen wir, dass die Menge

$$S := \{i \in \mathbb{N}_0 \mid \forall x \in \mathbb{N}_0 : x \in i \Rightarrow x \subseteq i\}$$

die Eigenschaft (4.2) erfüllt. Dann gilt wegen Eigenschaft (5), dass $S = \mathbb{N}_0$. Dazu untersuchen wir als erstes, ob $0 \in S$. Dazu muss gelten:

$$\forall x \in \mathbb{N}_0 : x \in \varnothing \Rightarrow x \subseteq \varnothing. \tag{4.4}$$

Sei nun $x \in \mathbb{N}_0$. Die Voraussetzung $x \in \varnothing$ ist falsch, also gilt die Implikation. Das beweist (4.4), und somit gilt $0 \in S$.

Sei nun $i \in S$. Wir zeigen, dass dann auch $i^+ \in S$ gilt. Dazu muss gelten:

$$\forall x \in \mathbb{N}_0 : x \in i^+ \Rightarrow x \subseteq i^+. \tag{4.5}$$

Sei dazu $x \in \mathbb{N}_0$. Wir nehmen an, dass $x \in i^+$. Also gilt $x \in i \cup \{i\}$. Wenn $x \in i$, dann gilt wegen $i \in S$ auch $x \subseteq i$. Wegen $i \subseteq i \cup \{i\} = i^+$ gilt daher auch $x \subseteq i^+$. Wenn $x = i$, so gilt $x \subseteq i$, und somit ebenfalls $x \subseteq i^+$. Somit erfüllt i^+ die Eigenschaft (4.5), und damit gilt $i^+ \in S$. Damit erfüllt S also die Eigenschaft (4.2), 0 zu enthalten und mit jedem Element seinen Nachfolger. Somit gilt wegen (5), dass $S = \mathbb{N}_0$. Damit gilt aber (4.3).

Wir zeigen nun (4). Seien $n, m \in \mathbb{N}_0$ so, dass $n^+ = m^+$. Wir nehmen an, dass $n \neq m$. Da $n \in n \cup \{n\}$, gilt $n \in n^+$. Also gilt $n \in m^+$, und somit $n \in m \cup \{m\}$. Da $n \neq m$, muss also $n \in m$ gelten. Somit gilt nach (4.3) auch $n \subseteq m$. Da auch $m \in m^+ = n^+ = n \cup \{n\}$, gilt wegen $m \neq n$, dass $m \in n$. Also gilt wegen (4.3) auch $m \subseteq n$. Somit gilt insgesamt $n = m$, im Widerspruch zur Annahme. Also gilt $n = m$. □

Wir haben jetzt also die Menge $\mathbb{N}_0$ und ihre Teilmenge $\mathbb{N} := \mathbb{N}_0 \setminus \{0\}$ zur Verfügung, aber erst eine Rechenoperation: die Operation, die zu jeder Zahl ihren Nachfolger bildet. Den Nachfolger n^+ von n schreiben wir auch als $n + 1$. Einen Vorgänger können wir ebenfalls bestimmen; wir erfinden also die Operation $n \mapsto n - 1$:

Satz 4.3. *Sei $n \in \mathbb{N}$. Dann gibt es genau ein $x \in \mathbb{N}_0$, sodass $x^+ = n$.*

Beweis: Wir zeigen zunächst die Existenz eines solchen x: Wir definieren die Menge

$$S := \{n \in \mathbb{N}_0 \mid n = 0 \text{ oder } \exists x \in \mathbb{N}_0 : x^+ = n\}.$$

Wir zeigen, dass S die Eigenschaft (4.2) aus Satz 4.2 erfüllt. Klarerweise gilt $0 \in S$. Wir zeigen nun $\forall n \in S : n^+ \in S$. Sei dazu $n \in S$. Um zu zeigen, dass $n^+ \in S$ ist, müssen wir zeigen:

$$n^+ = 0 \text{ oder } \exists x \in \mathbb{N}_0 : x^+ = n^+.$$

Der zweite Teil dieser Disjunktion ist wahr: die Wahl $x := n$ belegt, dass $\exists x \in \mathbb{N}_0 : x^+ = n^+$ wahr ist. Also sind die Eigenschaften (4.2) aus Satz 4.2 erfüllt. Satz 4.2 (5) liefert nun $S = \mathbb{N}_0$. Folglich gilt für alle $n \in \mathbb{N}_0$ mit $n \neq 0$, dass es ein $x \in \mathbb{N}_0$ mit $x^+ = n$ gibt.

Wir zeigen nun die Eindeutigkeit. Seien dazu $x, y \in \mathbb{N}_0$ so, dass $x^+ = n$ und $y^+ = n$. Dann gilt $x^+ = y^+$. Satz 4.2 (4) liefert nun $x = y$. □

Für $n \in \mathbb{N}$ definieren wir nun $n-1$ als jenes $x \in \mathbb{N}_0$ mit $x^+ = n$. Es gilt dann $(n-1)+1 = x+1 = x^+ = n$, und $(n+1)-1 = (n^+)-1 = n$.

Wir haben bereits zweimal eine neue Beweismethode verwendet, um zu zeigen, dass $\forall n \in \mathbb{N}_0 : A(n)$ gilt. Wir haben nachgewiesen, dass die Menge $S := \{n \in \mathbb{N}_0 \mid A(n)\}$ die Eigenschaften $0 \in S$ und $\forall s \in S : s^+ \in S$ erfüllt, und dann aus Satz 4.2 (5) geschlossen, dass $S = \mathbb{N}_0$ ist. Also gilt $A(n)$ für alle $n \in \mathbb{N}_0$. Das ist so wichtig, dass wir die Menge S von nun an verstecken werden, und diese Beweismethode explizit formulieren:

Satz 4.4 (Beweismethode „vollständige Induktion“). *Sei $A(n)$ eine Aussageform, die für alle $n \in \mathbb{N}_0$ definiert ist. Wir nehmen an, dass $A(0)$ gilt, und dass $\forall n \in \mathbb{N}_0 : \big(A(n) \Rightarrow A(n+1)\big)$ gilt. Dann gilt auch $\forall n \in \mathbb{N}_0 : A(n)$.*

Beweisskizze: Die Menge $S := \{n \in \mathbb{N}_0 \mid A(n)\}$ erfüllt die Eigenschaft (4.2) aus Satz 4.2 (5). Also gilt $S = \mathbb{N}_0$. □

Das erlaubt uns also, im Induktionsschritt, in dem wir $A(n+1)$ zeigen wollen, $A(n)$ zu verwenden. Eine Variante davon erlaubt, nicht nur $A(n)$, sondern gleich alle $A(0), \dots, A(n)$ zu verwenden.

Satz 4.5 (Variante der Beweismethode „vollständige Induktion“). *Sei $A(n)$ eine Aussageform, die für alle $n \in \mathbb{N}_0$ definiert ist. Wir nehmen an, dass $A(0)$ gilt, und dass*

$$\forall n \in \mathbb{N}_0 : \Big(\big(\forall k \in \{0, 1, \dots, n\} : A(k)\big) \Rightarrow A(n+1)\Big)$$

gilt. Dann gilt auch $\forall n \in \mathbb{N}_0 : A(n)$.

Beweis: Sei $B(n) :\Leftrightarrow \forall k \in \{0, 1, \dots, n\} : A(k)$. Wir zeigen mithilfe von Satz 4.4, dass $\forall n \in \mathbb{N}_0 : B(n)$ gilt. Dazu zeigen wir

$$B(0) \wedge \big(\forall n \in \mathbb{N}_0 : B(n) \Rightarrow B(n+1)\big).$$

Wir zeigen als erstes $B(0)$. Da $A(0)$ laut Voraussetzung wahr ist, ist auch $B(0)$ wahr. Wir zeigen nun $\forall n \in \mathbb{N}_0 : B(n) \Rightarrow B(n+1)$. Sei dazu $n \in \mathbb{N}_0$. Wir nehmen an, dass $B(n)$ gilt, und zeigen $B(n+1)$. Da $B(n)$ gilt, gilt $\forall k \in \{0, 1, \dots, n\} : A(k)$. Nach Voraussetzung gilt daher $A(n+1)$. Also gilt $\forall k \in \{0, 1, \dots, n+1\} : A(k)$. Somit gilt $B(n+1)$. Wir verwenden nun Satz 4.4 und erhalten, dass $\forall n \in \mathbb{N}_0 : B(n)$ gilt. Wir zeigen, dass dann auch $\forall n \in \mathbb{N}_0 : A(n)$ gilt. Sei dazu $n \in \mathbb{N}$. Dann gilt $B(n)$, also $\forall k \in \{0, 1, \dots, n\} : A(k)$. Damit gilt insbesondere (setze $k := n$) auch $A(n)$. □

Wir brauchen noch eine weitere Eigenschaft der natürlichen Zahlen: man kann Funktionen rekursiv definieren. Wir kennen das etwa in folgenden Definitionen:

(1) $0\,! := 1$ und $(n+1)\,! := (n+1) \cdot (n\,!)$ für $n \in \mathbb{N}_0$.
(2) Die Fibonaccizahlen F_n sind definiert durch $F_0 = 0$, $F_1 = 1$ und $F_n = F_{n-1} + F_{n-2}$ für $n \in \mathbb{N}$ mit $n \geq 2$.

Dass durch die erste Definition tatsächlich eine Funktion definiert wird, begründet folgender Satz, der in der Mengenlehre *Rekursionstheorem* genannt wird.

Satz 4.6 (Definitionsmethode „Rekursion“, cf. [**Hal76**]). *Sei X eine Menge, sei $a \in X$, und sei f eine Funktion von X nach X. Dann gibt es genau eine Funktion u von $\mathbb{N}_0$ nach X mit $u(0) = a$ und $u(n+1) = f(u(n))$.*

Man benutzt diesen Satz etwa so: Wir definieren $\psi : \mathbb{N}_0 \to \mathbb{N}_0$ rekursiv durch $\psi(0) = 1$ und $\psi(n+1) = 2 \cdot \psi(n)$ für $n \in \mathbb{N}_0$. Dann gilt $\psi(1) = 2\psi(0) = 2$, $\psi(2) = 2\psi(1) = 4, \ldots$. Rekursionen, die auf die Funktionswerte mehrerer kleinerer Werte zurückgreifen oder die in der Definition von $f(n+1)$ nicht nur $f(n)$, sondern auch n verwenden, rechtfertigt man mit Varianten dieses Satzes.

2. Der Aufbau der Arithmetik

Die Arithmetik hat Peano bereits 1889 so aufgebaut:

Definition 4.7 (Addition). Für jedes $m \in \mathbb{N}_0$ definieren wir eine Funktion $a_m : \mathbb{N}_0 \to \mathbb{N}_0$ rekursiv durch $a_m(0) := m$ und $a_m(x^+) := (a_m(x))^+$. Darauf aufbauend definieren wir $x + y := a_x(y)$ für $x, y \in \mathbb{N}_0$ und nennen $x + y$ die *Summe* von x und y.

Mit dieser Definition gilt offensichtlich für alle $x \in \mathbb{N}_0$, dass $x+0 = x$, da $x+0 = a_x(0) = x$, und es gilt $x + 1 = x^+$, da $x + 1 = a_x(1) = a_x(0^+) = (a_x(0))^+ = x^+$. Schon die einfache Eigenschaft $0 + x = x$ ist nicht offensichtlich; wir werden sie im Verlauf des Beweises des nächsten Satzes begründen.

Satz 4.8. *Seien $x, y \in \mathbb{N}_0$. Dann gilt $x + y = y + x$.*

Wir beweisen dazu als erstes:

$$\forall u \in \mathbb{N}_0 : 0 + u = u. \tag{4.6}$$

Wir verwenden dazu vollständige Induktion nach u.

Induktionsanfang: Sei $u := 0$. Zu zeigen ist

$$0 + 0 = 0. \tag{4.7}$$

Die Definition von $+$ liefert $0+0 = a_0(0)$. Die Definition von a_0 liefert $a_0(0) = 0$. Somit gilt (4.7). Damit ist der Induktionsanfang gelungen.

Induktionsschritt: Wir zeigen

$$\forall u \in \mathbb{N}_0 : 0 + u = u \Rightarrow 0 + u^+ = u^+.$$

Sei dazu $u \in \mathbb{N}_0$. Wir nehmen an, dass $0+u = u$ gilt. (Diese Annahme nennen wir die *Induktionsannahme* oder *Induktionsvoraussetzung*). Wir zeigen, dass dann

$$0 + u^+ = u^+ \tag{4.8}$$

gilt. (Diese Konklusion nennen wir die *Induktionsbehauptung.*) Es gilt

$$\begin{aligned} 0 + u^+ &= a_0(u^+) \\ &= (a_0(u))^+ \\ &= (0+u)^+. \end{aligned}$$

Nun verwenden wir die Induktionsannahme $0 + u = u$ und erhalten daraus

$$(0+u)^+ = u^+.$$

Somit gilt die Induktionsbehauptung (4.8). Der Induktionsschritt ist damit gelungen. Es gilt also (4.6).

Als nächstes zeigen wir:

$$\forall u \in \mathbb{N}_0 : \big(\forall v \in \mathbb{N}_0 : (v+u)^+ = v^+ + u\big). \tag{4.9}$$

Wir verwenden dazu vollständige Induktion nach u.

Induktionsanfang: Sei $u := 0$. Zu zeigen ist

$$\forall v \in \mathbb{N}_0 : (v+0)^+ = v^+ + 0. \tag{4.10}$$

Sei dazu $v \in \mathbb{N}_0$. Es gilt $(v+0)^+ = (a_v(0))^+ = v^+$ und $v^+ + 0 = a_{v^+}(0) = v^+$. Somit gilt (4.10). Damit ist der Induktionsanfang gelungen.

Induktionsschritt: Wir zeigen

$$\forall u \in \mathbb{N}_0 : \Big(\big(\forall v \in \mathbb{N}_0 : (v+u)^+ = v^+ + u\big) \Rightarrow \big(\forall v \in \mathbb{N}_0 : (v+u^+)^+ = v^+ + u^+\big)\Big).$$

Sei dazu $u \in \mathbb{N}_0$. Wir nehmen an, dass $\forall v \in \mathbb{N}_0 : (v+u)^+ = v^+ + u$ gilt. (Das ist die *Induktionsannahme*). Wir zeigen, dass dann

$$\forall v \in \mathbb{N}_0 : (v+u^+)^+ = v^+ + u^+ \tag{4.11}$$

gilt. (Das ist die *Induktionsbehauptung.*) Sei dazu $v \in \mathbb{N}_0$. Es gilt

$$\begin{aligned} (v+u^+)^+ &= \big(a_v(u^+)\big)^+ \\ &= \big((a_v(u))^+\big)^+ \\ &= \big((v+u)^+\big)^+. \end{aligned}$$

Nun verwenden wir die Induktionsannahme und erhalten

$$\begin{aligned} \big((v+u)^+\big)^+ &= \big(v^+ + u\big)^+ \\ &= (a_{v^+}(u))^+ \\ &= a_{v^+}(u^+) \\ &= v^+ + u^+. \end{aligned}$$

Somit gilt die Induktionsbehauptung (4.11). Der Induktionsschritt ist damit gelungen. Es gilt also (4.9).

Wir beweisen nun

$$\forall y \in \mathbb{N}_0 : (\forall x \in \mathbb{N}_0 : x + y = y + x) \tag{4.12}$$

durch vollständige Induktion nach y.

Induktionsanfang: Sei $x \in \mathbb{N}_0$. Es gilt $x + 0 = a_x(0)$. Nach der Definition von a_x gilt $a_x(0) = x$. Nun berechnen wir $0 + x$. Nach (4.6) gilt $0 + x = x$. Also gilt $x + 0 = 0 + x$.

Induktionsschritt: Sei $y \in \mathbb{N}_0$. Wir nehmen an, dass

$$\forall x \in \mathbb{N}_0 : x + y = y + x$$

gilt und zeigen, dass dann

$$\forall x \in \mathbb{N}_0 : x + y^+ = y^+ + x \tag{4.13}$$

gilt. Um (4.13) zu zeigen, wählen wir $x \in \mathbb{N}_0$. Es gilt dann

$$\begin{aligned} x + y^+ &= a_x(y^+) \\ &= (a_x(y))^+ \\ &= (x + y)^+. \end{aligned}$$

Wir verwenden die Induktionssannahme und erhalten

$$(x + y)^+ = (y + x)^+.$$

Wegen (4.9) gilt

$$(y + x)^+ = y^+ + x.$$

Insgesamt gilt also (4.13). Somit ist der Induktionsschritt gelungen. Es gilt also (4.12), und somit die Aussage des Satzes. □

Wir werden jetzt Peanos Aufbau nicht weiter im Detail durchgehen. Er definiert als nächstes $x - y$ (falls $x \geq y$), $x \cdot y$ und beweist dafür etliche Rechengesetze. Um $x - y$ auch für $y > x$ zu definieren, erweitert man die natürlichen Zahlen zu den ganzen Zahlen

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\},$$

und erweitert dann auch $+$ und $\cdot$ von $\mathbb{N}_0$ auf $\mathbb{Z}$. Schließlich gelangt man zu den drei Grundrechungsarten $+, -, \cdot$ für die ganzen Zahlen. Wir verwenden dabei $-$ sowohl einstellig (in „-3“) und zweistellig (in „$x - y$“).

Satz 4.9 (Rechengesetze in $\mathbb{Z}$). *Seien $x, y, z \in \mathbb{Z}$. Dann gilt:*

(1) $(x + y) + z = x + (y + z)$ *($+$ ist assoziativ).*
(2) $x + 0 = 0 + x = x$ *(0 ist beidseitig neutrales Element bezüglich $+$).*
(3) $x + (-x) = (-x) + x = 0$ *($-x$ ist zu das zu x additiv inverse Element).*
(4) $x + y = y + x$ *($+$ ist kommutativ).*
(5) $x - y = x + (-y)$ *(Zusammenhang zwischen einstelligem und zweistelligem $-$).*
(6) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ *($\cdot$ ist assoziativ).*

(7) $x \cdot (y + z) = x \cdot y + x \cdot z$ *(Linksdistributivgesetz).*
(8) $(x + y) \cdot z = x \cdot z + y \cdot z$ *(Rechtsdistributivgesetz).*
(9) $x \cdot y = y \cdot x$ *($\cdot$ ist kommutativ).*
(10) $1 \cdot x = x \cdot 1 = x$ *(1 ist beidseitig neutrales Element bezüglich $\cdot$).*
(11) $0 \cdot x = x \cdot 0 = 0$ *(0 ist absorbierendes Element bezüglich $\cdot$).*
(12) $(-x) \cdot y = -(x \cdot y) = x \cdot (-y)$ *(Aufteilung von $-$ auf ein Produkt).*
(13) $-(-x) = x$.

Oft hat man es in der Mathematik auch mit anderen Mengen als $\mathbb{Z}$ zu tun, die aber ebenfalls Operationen $+, -, \cdot$ und Elemente $0, 1$ besitzen, die diese Rechengesetze erfüllen. Beispiele sind $\mathbb{R}$, die Menge $\mathbb{R}[x]$ der Polynome über $\mathbb{R}$, die komplexen Zahlen $\mathbb{C}$, die Gaußschen ganzen Zahlen der Form $a + b\,i$ mit $a, b \in \mathbb{Z}$. Eine solche Struktur, die aus einer nicht leeren Menge und drei darauf definierten Operationen besteht, die alle Rechengesetze (1)-(13) erfüllen, heißt *kommutativer Ring mit Eins.* In der abstrakten Algebra beschreibt man auch Strukturen, die nur manche dieser Rechengesetze erfüllen. Je nachdem, welche Rechengesetze sie erfüllen, haben diese Strukturen besondere Namen bekommen.

Tabelle 1. Algebraische Strukturen mit $+, -, \cdot$

	A+ (1)	**0** (2)	**-** (3)	**K+** (4)	**A∗** (6)	**LD** (7)	**RD** (8)	**K∗** (9)	typisches Beispiel
Kommutativer Ring	•	•	•	•	•	•	•	•	$(\mathbb{Z}, +, -, \cdot)$
Ring	•	•	•	•	•	•	•		Matrixring $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$
Distributiver Fastring	•	•	•		•	•	•		
Fastring, Rechtsfastring	•	•	•		•		•		Polynome $(\mathbb{R}[x], +, \circ)$ $p(x) \circ q(x) := p(q(x))$

Manchmal müssen auch nicht alle drei Grundrechnungsarten existieren, sondern nur einige davon. Wir vereinbaren, dass Rechenoperationen, die in keinem geforderten Rechengesetz erwähnt werden, auch nicht vorkommen.

TABELLE 2. Einige weitere Algebraische Strukturen

	A+ (1)	**0** (2)	**-** (3)	**K+** (4)	**A∗** (6)	**LD** (7)	**RD** (8)	**K∗** (9)	**1** (10)	typisches Beispiel
Halbgruppe, additiv geschrieben	•									
Halbgruppe, multiplikativ geschrieben					•					Worthalbgruppe $\{a,b\}^* = \{a, b, aa, ab, \ldots\}$, $abaa * bbb = abaabbb$
kommutative Halbgruppe, multiplikativ geschrieben					•			•		Worthalbgruppe $\{a\}^* = \{a, aa, aaa, \ldots\}$, $aaaa * aaa = aaaaaaa$
Monoid, multiplikativ geschrieben					•				•	Transformationenmonoid $(\{f : \mathbb{N} \to \mathbb{N}\}, \circ, \mathrm{id}_{\mathbb{N}})$
kommutatives Monoid, additiv geschrieben	•	•		•						$(\mathbb{N}_0, +, 0)$
Gruppe, additiv geschrieben	•	•	•							
abelsche Gruppe, additiv geschrieben	•	•	•	•						$(\mathbb{Z}, +, -, 0)$
Halbring	•	•		•	•	•	•			$(\mathbb{N}_0, \max, +)$

3. Division und Teilbarkeit

DEFINITION 4.10 (Teilbarkeit). Für $x, y \in \mathbb{Z}$ definieren wir, dass

$$x \textit{ teilt } y$$

genau dann gilt, wenn es ein $z \in \mathbb{Z}$ gibt, sodass $x \cdot z = y$ ist.

Wir schreiben dann auch $x \mid y$; die Zahl y ist dann ein *Vielfaches* von x.

ÜBUNGSAUFGABEN 4.11.
In den folgenden Beispielen beweisen wir einige grundlegende Eigenschaften der Teilbarkeitsrelation. Zeigen Sie in den folgenden Beispielen jeweils, dass die angeführte Implikation für alle $x, y, z \in \mathbb{Z}$ gilt.

(1) $(x \mid y \text{ und } x \mid z) \Rightarrow x \mid (y + z)$.
(2) $x \mid y \Rightarrow x \mid zy$.
(3) $(x \mid y \text{ und } y \mid z) \Rightarrow x \mid z$.

(4) $(x \mid y \text{ und } y \mid x) \Rightarrow (x = y \text{ oder } x = -y)$.
(5) $(x \mid y \text{ und } z \mid x \text{ und } z \mid y \text{ und } z \neq 0) \Rightarrow \frac{x}{z} \mid \frac{y}{z}$.
(6) $x \mid y \Rightarrow zx \mid zy$.

Der folgende Satz liefert Quotienten und Rest einer Division in $\mathbb{Z}$.

SATZ 4.12. *Seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}$. Dann gibt es genau ein Paar von Zahlen $(q, r) \in \mathbb{Z} \times \mathbb{N}_0$, sodass $a = q \cdot n + r$ und $r \in \{0, \ldots, n-1\}$.*

Beweis: Wir zeigen als erstes die Existenz eines Paares (q, r). Sei $n \in \mathbb{N}$. Wir zeigen zunächst durch Induktion nach a, dass es für alle $a \in \mathbb{N}_0$ ein solches Paar (q, r) gibt.

Induktionsanfang: Sei $a = 0$. Dann ist $a = 0n + 0$ die gewünschte Darstellung.

Induktionsschritt: Wir nehmen an, dass $a \in \mathbb{N}$ so ist, dass sich alle $b \in \mathbb{N}_0$ mit $b < a$ als $qn + r$ mit $r \in \{0, \ldots, n-1\}$ darstellen lassen.

1. Fall: $a < n$: Dann ist $a = 0n + a$ bereits die passende Darstellung.

2. Fall: $a \geq n$: Dann gilt $a - n \in \mathbb{N}_0$ und und $a - n < a$. Somit gibt es nach Induktionsvoraussetzung $(q_1, r_1) \in \mathbb{Z} \times \{0, \ldots, n-1\}$ mit $a - n = q_1 n + r_1$. Dann gilt $a = (q_1 + 1)n + r_1$. Somit leistet $(q, r) := (q_1 + 1, r_1)$ das Gewünschte. Das beendet den Induktionsbeweis; jedes $a \in \mathbb{N}_0$ lässt sich also als $qn + r$ mit $0 \leq r < n$ schreiben.

Wenn $a < 0$, so gibt es q, r mit $0 \leq r \leq n - 1$ und $-a = qn + r$. Im Fall $r = 0$ gilt dann $a = (-q)n + r$. Wenn $r > 0$, so gilt $a = (-q - 1)n + (n - r)$, und $0 < n - r \leq n - 1$. Somit leisten $(q', r') := (-(q + 1), n - r)$ das Gewünschte.

Wir zeigen nun die Eindeutigkeit: Sei $a = q_1 n + r_1$ und $a = q_2 n + r_2$. Dann gilt $(q_1 - q_2)n + (r_1 - r_2) = 0$, also $r_1 - r_2 = (q_2 - q_1)n$. Da r_1, r_2 Elemente von $\{0, \ldots, n-1\}$ sind, gilt $-(n-1) \leq r_1 - r_2 \leq n - 1$. Das einzige Vielfache von n zwischen $-(n-1)$ und $n - 1$ ist 0. Also gilt $r_1 - r_2 = 0$, und somit $q_1 n = q_2 n$. Wegen $n \neq 0$ gilt dann auch $q_1 = q_2$, und somit $(q_1, r_1) = (q_2, r_2)$. □

Mit $a \bmod n$ kürzen wir den Rest von a bei der Division durch n ab.

DEFINITION 4.13 (Größter gemeinsamer Teiler). Für zwei Zahlen $a, b \in \mathbb{Z}$ (nicht beide 0) ist $\mathrm{ggT}(a, b)$ die größte Zahl $z \in \mathbb{N}$ mit $z \mid a$ und $z \mid b$.

SATZ 4.14. *Seien $a, b \in \mathbb{Z}$, nicht beide 0, und sei $z \in \mathbb{Z}$. Dann gilt:*

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(a + z \cdot b, b).$$

So gilt zum Beispiel $\mathrm{ggT}(25, 15) = \mathrm{ggT}(40, 15)$.

Beweis: Wir zeigen, dass nicht nur der ggT, sondern sogar die Mengen der gemeinsamen Teiler der beiden Zahlenpaare gleich sind. Wir zeigen also

$$\{t \in \mathbb{Z} : t \mid a \text{ und } t \mid b\} = \{t \in \mathbb{Z} : t \mid a + zb \text{ und } t \mid b\}.$$

"$\subseteq$": Falls t sowohl a als auch b teilt, dann auch $a + zb$ und b. "$\supseteq$": Falls t sowohl $a + zb$, als auch b teilt, dann auch $a + zb - zb$ und b, also auch a und b. □

Das nützen wir jetzt möglichst geschickt aus, um $\mathrm{ggT}(147, 33)$ zu berechnen:

$$\begin{aligned}\mathrm{ggT}\,(147, 33) &= \mathrm{ggT}\,(147 - 4 \cdot 33, 33)\\ &= \mathrm{ggT}\,(15, 33)\\ &= \mathrm{ggT}\,(15, 33 - 2 \cdot 15)\\ &= \mathrm{ggT}\,(15, 3)\\ &= \mathrm{ggT}\,(0, 3)\\ &= 3.\end{aligned}$$

Günstig ist es also, z so zu wählen, dass $a + zb$ der Rest von a bei der Division durch b wird.

Mithilfe des *erweiterten Euklidischen Algorithmus* findet man nicht nur den ggT von a und b, sondern auch $u, v \in \mathbb{Z}$, sodass $\mathrm{ggT}\,(a, b) = u \cdot a + v \cdot b$.

Beispiel: Wir berechnen $\mathrm{ggT}(147, 33)$, und schreiben das so:

	147	33	
147	1	0	$(147 = 1 \cdot 147 + 0 \cdot 33)$
33	0	1	$(33 = 0 \cdot 147 + 1 \cdot 33)$
15	1	-4	$(15 = 1 \cdot 147 - 4 \cdot 33)$
3	-2	9	$(3 = -2 \cdot 147 + 9 \cdot 33)$
0			

Berechnet man $\mathrm{ggT}(a, b)$ mithilfe dieses Algorithmus, sieht man, dass sich die auftretenden Zahlen immer als Linearkombination von a und b schreiben lassen. Als Konsequenz davon erhalten wir folgenden Satz:

Satz 4.15. *Seien $a, b \in \mathbb{Z}$ (nicht beide 0). Dann gibt es $u, v \in \mathbb{Z}$, sodass*

$$\mathrm{ggT}\,(a, b) = u \cdot a + v \cdot b.$$

Beweis: Wir zeigen als erstes:

$$\begin{aligned}(4.14)\quad \forall n \in \mathbb{N}_0 : \big(\forall (a, b) \in (\mathbb{N}_0 \times \mathbb{N}_0) \setminus \{(0, 0)\} : (a \leq n \vee b \leq n) \Rightarrow \\ (\exists u, v \in \mathbb{Z} : \mathrm{ggT}(a, b) = ua + vb)\big)\end{aligned}$$

durch Induktion.

Induktionsanfang: Wir nehmen an, dass $n = 0$. Seien $a, b \in \mathbb{N}_0$, nicht beide 0. Wenn $a = 0$, so gilt $\mathrm{ggT}(a, b) = b = 0a + 1b$. Also leistet $(u, v) = (0, 1)$ das Gewünschte. Wenn $b = 0$, so gilt $\mathrm{ggT}(a, b) = a = 1a + 0b$.

Induktionsschritt: Sei $n \in \mathbb{N}_0$. Wir nehmen an, dass

$$\forall (a, b) \in (\mathbb{N}_0 \times \mathbb{N}_0) \setminus \{(0, 0)\} : (a \leq n \vee b \leq n) \Rightarrow (\exists u, v \in \mathbb{Z} : \mathrm{ggT}(a, b) = ua + vb)$$

gilt, und zeigen

$$\forall (a,b) \in (\mathbb{N}_0 \times \mathbb{N}_0) \setminus \{(0,0)\} : (a \leq n+1 \vee b \leq n+1) \Rightarrow \\ (\exists u, v \in \mathbb{Z} : \mathrm{ggT}(a,b) = ua + vb).$$

Seien dazu $a, b \in \mathbb{N}_0$, nicht beide 0. Wir nehmen an, dass $a \leq n+1$ oder $b \leq n+1$.

1.Fall: $a = 0$ oder $b = 0$: Wenn $a = 0$, so gilt $\mathrm{ggT}(a,b) = b = 0a + 1b$, und wenn $b = 0$, dann gilt $\mathrm{ggT}(a,b) = 1a + 0b$. Wir nehmen also an, dass $a > 0$ und $b > 0$.

2.Fall: $a > 0$ und $b > 0$:

Fall 2.1: $a \leq n+1$: Durch Division erhalten wir $q, r \in \mathbb{N}_0$ mit $b = qa + r$ und $r \leq n$. Da $r \leq n$, können wir die Induktionsannahme verwenden, und erhalten $u_1, v_1 \in \mathbb{Z}$, sodass

$$\mathrm{ggT}(a,r) = u_1 a + v_1 r.$$

Da $r = b - qa$, gilt $\mathrm{ggT}(a,b) = \mathrm{ggT}(a, b-qa) = \mathrm{ggT}(a,r) = u_1 a + v_1 r = u_1 a + v_1(b - qa) = (u_1 - q)a + v_1 b$. Somit leistet $(u,v) := (u_1 - q, v_1)$ das Gewünschte.

Fall 2.2: $b \leq n+1$: Durch Division erhalten wir $q, r \in \mathbb{N}_0$ mit $a = qb + r$ und $r \leq n$. Da $r \leq n$, können wir die Induktionsannahme verwenden, und erhalten $u_1, v_1 \in \mathbb{Z}$, sodass

$$\mathrm{ggT}(r,b) = u_1 r + v_1 b.$$

Da $r = a - qb$, gilt $\mathrm{ggT}(r,b) = \mathrm{ggT}(a - qb, b) = \mathrm{ggT}(r,b) = u_1 r + v_1 b = u_1(a - qb) + v_1 b = u_1 a + (v_1 - q)b$. Somit leistet $(u,v) := (u_1, v_1 - q)$ das Gewünschte. Damit ist (4.14) bewiesen. Folglich gibt es für alle $a, b \in \mathbb{N}_0$, die nicht beide 0 sind, eine Darstellung des ggT als Linearkombination.

Wir zeigen nun, dass es eine solche Linearkombination für alle $(a,b) \in (\mathbb{Z} \times \mathbb{Z}) \setminus \{(0,0)\}$ gibt. Wenn $a = 0$ oder $b = 0$, finden wir (u,v) als $(0,1)$, $(0,-1)$, $(1,0)$ oder $(-1,0)$. Also nehmen wir nun an, dass $a \neq 0$ und $b \neq 0$. Wir finden dann $u_1, v_1 \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = \mathrm{ggT}(|a|,|b|) = u_1|a| + v_1|b| = \frac{u_1|a|}{a}a + \frac{v_1|b|}{b}b$. Somit leisten $(u,v) = (\frac{u_1|a|}{a}, \frac{v_1|b|}{b})$ das Gewünschte. □

Eine Folgerung davon ist:

Satz 4.16. *Seien $a, b \in \mathbb{Z}$, nicht beide 0, und sei $t \in \mathbb{Z}$ so, dass $t \mid a$ und $t \mid b$. Dann gilt auch $t \mid \mathrm{ggT}(a,b)$.*

Beweis: Seien $u, v \in \mathbb{Z}$ so, dass $\mathrm{ggT}(a,b) = ua + vb$. Da t die Zahl a teilt, ist auch ua ein Vielfaches von t. Ebenso ist vb ein Vielfaches von t. Somit ist auch die Summe $ua + vb$ ein Vielfaches von t. Die Zahl t ist also ein Teiler von $\mathrm{ggT}(a,b)$.

Wenn a und b größten gemeinsamen Teiler 1 haben, so heißen sie *teilerfremd* oder *relativ prim*.

Satz 4.17. *Seien $a, b, c \in \mathbb{Z}$, und sei zumindest eine der Zahlen a und b nicht 0. Wir nehmen an, dass a die Zahl $b \cdot c$ teilt, und dass $\mathrm{ggT}(a,b) = 1$ gilt. Dann gilt: a teilt c.*

Beweis: Es gibt $u, v \in \mathbb{Z}$, sodass $1 = u \cdot a + v \cdot b$. Da $a \mid uac$ gilt, und da wegen $a \mid bc$ auch $a \mid vbc$ gilt, gilt auch

$$a \mid (ua + vb)c$$

und folglich $a \mid c$. □

Sind $a, b \in \mathbb{Z}$, so nennt man jede Zahl $c \in \mathbb{Z}$, die von a und b geteilt wird, ein gemeinsames Vielfaches von a und b. Unter allen gemeinsamen Vielfachen zeichnen wir das kleinste aus.

DEFINITION 4.18. Es seien $a, b \in \mathbb{Z} \setminus \{0\}$. Dann ist $\mathrm{kgV}(a, b)$ definiert durch

$$\mathrm{kgV}(a, b) = \min \{v \in \mathbb{N} : a \mid v \text{ und } b \mid v\}.$$

Die Menge aller positiven gemeinsamen Vielfachen ist ja für $a, b \in \mathbb{Z} \setminus \{0\}$ bestimmt nicht leer, da sie $|a \cdot b|$ enthält.

SATZ 4.19. *Seien $a, b \in \mathbb{Z} \setminus \{0\}$, und sei $s \in \mathbb{Z}$ so, dass $a \mid s$ und $b \mid s$. Dann gilt:*

$$\mathrm{kgV}(a, b) \mid s.$$

Jedes gemeinsame Vielfache ist also ein Vielfaches des kgV.

Beweis: Wir dividieren s durch $\mathrm{kgV}(a, b)$ und erhalten somit $r \in \{0, \ldots, \mathrm{kgV}(a, b) - 1\}$ und $q \in \mathbb{Z}$, sodass

$$s = q \cdot \mathrm{kgV}(a, b) + r.$$

Also gilt $r = s - q \cdot \mathrm{kgV}(a, b)$. Sowohl s also auch $q \cdot \mathrm{kgV}(a, b)$ sind Vielfache von a und Vielfache von b. Ihre Differenz r ist also ebenfalls ein Vielfaches von a und von b. Da $r < \mathrm{kgV}(a, b)$, und da $\mathrm{kgV}(a, b)$ das kleinste gemeinsame Vielfache ist, muss $r = 0$ gelten. Also ist s ein Vielfaches von $\mathrm{kgV}(a, b)$.

Zwischen ggT und kgV kann man folgenden Zusammenhang herstellen:

SATZ 4.20. *Seien $a, b \in \mathbb{N}$. Dann gilt* $\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = ab$.

Beweis: Wir zeigen als erstes $ab \mid \mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b)$. Seien dazu $u, v \in \mathbb{Z}$ so, dass $\mathrm{ggT}(a, b) = ua + vb$. Dann gilt

$$\begin{aligned} \mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) &= (ua + vb)\mathrm{kgV}(a, b) \\ &= uab\frac{\mathrm{kgV}(a, b)}{b} + vba\frac{\mathrm{kgV}(a, b)}{a} \\ &= ab(u\frac{\mathrm{kgV}(a, b)}{b} + v\frac{\mathrm{kgV}(a, b)}{a}). \end{aligned}$$

Wir zeigen nun $\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) \mid ab$. Sei $x := \frac{ab}{\mathrm{ggT}(a,b)}$. Dann gilt $x = a\frac{b}{\mathrm{ggT}(a,b)} = b\frac{a}{\mathrm{ggT}(a,b)}$. Also gilt $a \mid x$ und $b \mid x$. Wegen Satz 4.19 gilt dann $\mathrm{kgV}(a, b) \mid x$, und somit $\mathrm{kgV}(a, b) \cdot \mathrm{ggT}(a, b) \mid x \cdot \mathrm{ggT}(a, b) = ab$. □

ÜBUNGSAUFGABEN 4.21.

(1) Bestimmen Sie für a und b jeweils $\mathrm{ggT}(a,b)$, und zwei ganze Zahlen $u, v \in \mathbb{Z}$, sodass

$$\mathrm{ggT}(a,b) = u \cdot a + v \cdot b.$$

   (a) $a = 254$, $b = 120$.
   (b) $a = 71$, $b = 79$.
   (c) $a = 610$, $b = 987$.

(2) Seien $a, b, x \in \mathbb{N}$ und $u, v \in \mathbb{Z}$ so, dass

$$x = ua + vb.$$

Zeigen Sie: Wenn x sowohl a als auch b teilt, so gilt $x = \mathrm{ggT}(a,b)$.

(3) Seien $a, b \in \mathbb{N}$, $y \in \mathbb{Z}$ so, dass $a \mid y$, $b \mid y$, $\mathrm{ggT}(a,b) = 1$. Zeigen Sie (ohne Primfaktorzerlegung): $a \cdot b \mid y$.

(4) Seien $a, b \in \mathbb{Z}$ (nicht beide 0), und sei $k \in \mathbb{N}$. Zeigen Sie: $\mathrm{ggT}(ka, kb) = k\,\mathrm{ggT}(a,b)$.

(5) Seien $a, b, c \in \mathbb{N}$ so, dass $a \mid b$. Zeigen Sie $\mathrm{ggT}(a,c) \mid \mathrm{ggT}(b,c)$ und $\mathrm{kgV}(a,c) \mid \mathrm{kgV}(b,c)$.

(6) Seien $a, c \in \mathbb{Z}$, $b, d \in \mathbb{N}$. Zeigen Sie: Wenn die Brüche $\frac{a}{b}$ und $\frac{c}{d}$ gekürzt, und die Nenner b und d teilerfremd sind, so ist auch der Bruch $\frac{ad+bc}{bd}$ gekürzt.

(7) * Sei $n \in \mathbb{N}$, und seien $a_1, a_2, \ldots, a_n$ in $\mathbb{N}$. Wir definieren G_1, G_2 und G_3 durch:
   (a) $G_1(a_1) := a_1$, $G_1(a_1, a_2, \ldots, a_n) = \mathrm{ggT}(G_1(a_1, a_2, \ldots, a_{n-1}), a_n)$.
   (b) $G_2(a_1, a_2, \ldots, a_n) := \max\{z \in \mathbb{N} : z \mid a_i \text{ für alle } i \in \{1, 2, \ldots, n\}\}$.
   (c) $G_3 := \min\{z \in \mathbb{N} : \text{ es gibt } \lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{Z}, \text{ sodass } z = \sum_{i=1}^{n} \lambda_i a_i\}$.

Zeigen Sie, dass G_1, G_2 und G_3 gleich sind.

4. Primfaktorzerlegung

Definition 4.22 (Primzahl). Eine Zahl $p \in \mathbb{N}$ ist genau dann eine *Primzahl*, wenn folgende beiden Bedingungen gelten:

(1) $p > 1$.
(2) Für alle $a, b \in \mathbb{N}$ mit $p = a \cdot b$ gilt $a = 1$ oder $b = 1$.

Satz 4.23. *Es gibt unendlich viele Primzahlen.*

Beweisskizze: Für $m \in \mathbb{N}_0$ sei $F_m := 2^{2^m} + 1$ die m-te Fermat-Zahl[4]. Durch Induktion kann man beweisen, dass für alle $m \in \mathbb{N}$ gilt:

$$\prod_{i=0}^{m-1} F_i = F_m - 2.$$

Also gilt für $i < j$, dass $\mathrm{ggT}(F_i, F_j) \mid \mathrm{ggT}(F_j - 2, F_j) \mid \mathrm{ggT}(F_j - 2, 2) \mid 2$. Da $\mathrm{ggT}(F_i, F_j)$ ungerade ist, gilt daher $\mathrm{ggT}(F_i, F_j) = 1$. Sei nun für jedes $i \in \mathbb{N}_0$ die Zahl q_i der kleinste natürliche Teiler von F_i, der ≥ 2 ist. Dann ist q_i eine Primzahl. Weiters gilt für alle $i, j \in \mathbb{N}_0$ mit $i \neq j$, dass $q_i \neq q_j$, da $q_i = q_j$ zur Folge hätte, dass $q_i \mid \mathrm{ggT}(F_i, F_j)$. □

[4]Pierre de Fermat (1607-1665) vermutete, dass alle F_m Primzahlen sind. Dass ist für $m \leq 4$ wahr. Im Jahr 1732 fand Euler mit 641 einen Teiler von F_5. Man hat bis heute kein $m \geq 5$ gefunden, für das F_m prim ist und kann für einige m beweisen, dass F_m zusammengesetzt ist (z.B. für $5 \leq m \leq 32$). Wenn F_m prim ist, so kann man ein regelmässiges F_m-Eck mit Verwendung von lediglich Zirkel und Lineal konstruieren. Für $F_2 = 17$ gab Gauß (1777-1855) im Jahr 1797 eine Konstruktion des 17-Ecks an.

SATZ 4.24 (Fundamentallemma). *Sei p eine Primzahl, und seien $a, b \in \mathbb{Z}$. Falls p ein Produkt $a \cdot b$ teilt, so teilt p einen der beiden Faktoren a oder b.*

Beweis: Wir nehmen an, dass $p \nmid a$ und $p \mid ab$. Dann gilt $\mathrm{ggT}(a, p) = 1$, also gibt es $u, v \in \mathbb{Z}$ mit $ua + vp = 1$. Folglich gilt $uab + vpb = b$. Da p beide Summanden teilt, gilt $p \mid b$. □

KOROLLAR 4.25. *Sei p_n die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, usw. Für jedes $i \in \mathbb{N}$ seien $\alpha_i, \beta_i \in \mathbb{N}_0$. Wir nehmen an, dass nur endlich viele α_i und nur endlich viele β_i verschieden von 0 sind. Sei $a := \prod_{i \in \mathbb{N}} {p_i}^{\alpha_i}$, und sei $b := \prod_{i \in \mathbb{N}} {p_i}^{\beta_i}$. Dann gilt $a \mid b$ genau dann, wenn $\forall i \in \mathbb{N} : \alpha_i \leq \beta_i$ gilt.*

Beweis: Wir zeigen als erstes, dass $a \mid b$ impliziert, dass $\forall i \in \mathbb{N} : \alpha_i \leq \beta_i$ gilt. Wir nehmen dazu an, dass $a \mid b$ und fixieren $i \in \mathbb{N}$. Wir nehmen nun, im Widerspruch zur Behauptung, an, dass $\alpha_i > \beta_i$. Dann gilt

$$p_i^{\alpha_i - \beta_i} \prod_{j \in \mathbb{N} \setminus \{i\}} p_j^{\alpha_j} \mid \prod_{j \in \mathbb{N} \setminus \{i\}} p_j^{\beta_j}.$$

Nach Satz 4.24 teilt p_i also ein $p_j^{\beta_j}$ mit $j \neq i$. Im Fall $\beta_j = 0$ widerspricht das $p_i > 1$, im Fall $\beta_j > 0$ gilt $p_i \mid p_j$. Da p_j eine Primzahl ist, gilt dann $p_i = p_j$, im Widerspruch zu $i \neq j$. Somit gilt $\alpha_i \leq \beta_i$.

Wir nehmen nun an, dass für alle $i \in \mathbb{N}$ gilt, dass $\alpha_i \leq \beta_i$, und zeigen, dass dann $a \mid b$. Es gilt $a \cdot \prod_{i \in \mathbb{N}} p_i^{\beta_i - \alpha_i} = b$, und somit $a \mid b$. □

SATZ 4.26 (Existenz und Eindeutigkeit der Primfaktorzerlegung). *Sei $\langle p_i \mid i \in \mathbb{N} \rangle = (2, 3, 5, 7, 11, \ldots)$ die Folge aller Primzahlen, und sei $n \in \mathbb{N}$. Dann gibt es genau eine Funktion $\alpha : \mathbb{N} \to \mathbb{N}_0$ mit folgenden Eigenschaften:*

(1) *$\{i \in \mathbb{N} \mid \alpha(i) > 0\}$ ist endlich.*
(2) *$n = \prod_{i \in \mathbb{N}} p_i^{\alpha(i)}$.*

Beweis: Wir zeigen zunächst durch Induktion nach n, dass es ein solches α gibt. Für $n = 1$ setzen wir $\alpha(i) := 0$ für alle $i \in \mathbb{N}$. Für $n > 1$ sei q der kleinste Teiler von n mit $q > 1$. Die Zahl q ist eine Primzahl; es gibt also $j \in \mathbb{N}$ mit $q = p_j$. Nach Induktionsvoraussetzung gibt es $\beta : \mathbb{N} \to \mathbb{N}_0$ mit

$$\frac{n}{q} = \prod_{i \in \mathbb{N}} p_i^{\beta(i)},$$

also gilt $n = p_j^{\beta(j)+1} \cdot \prod_{i \in \mathbb{N} \setminus \{j\}} p_i^{\beta(i)}$. Somit leistet α mit $\alpha(i) = \beta(i)$ für $i \neq j$ und $\alpha(j) = \beta(j) + 1$ das Gewünschte. Nun zeigen wir die Eindeutigkeit:

Seien γ und δ so, dass $\{i \in \mathbb{N} \mid \gamma(i) > 0\}$ und $\{i \in \mathbb{N} \mid \delta(i) > 0\}$ endlich sind, und $n = \prod_{i \in \mathbb{N}} p_i^{\gamma(i)} = \prod_{i \in \mathbb{N}} p_i^{\delta(i)}$. Korollar 4.25 liefert, dass für alle $i \in \mathbb{N}$ gilt, dass $\gamma(i) \leq \delta(i)$. Das gleiche Korollar liefert, dass $\delta(i) \leq \gamma(i)$. Also gilt $\gamma = \delta$. □

Übungsaufgaben 4.27.

(1) [**RU87**, p. 28] Sei p_n die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, usw. Zeigen Sie

$$p_n \leq 2^{2^{n-1}}.$$

Hinweis: Euklids Beweis, dass es unendlich viele Primzahlen gibt ([**Euk91**, Buch IX, Satz 20], 270 v.Chr.) beruht auf folgender Überlegung: Seien $q_1, q_2, \ldots, q_n$ Primzahlen. Dann ist der kleinste positive Teiler von $q_1 \cdot q_2 \cdots q_n + 1$ eine Primzahl, die von allen q_i verschieden ist.

(2) Welche Zahlen $q \in \mathbb{N}$ erfüllen folgende Eigenschaft?

Für alle $a, b \in \mathbb{Z}$ mit $q \mid a \cdot b$ gilt $q \mid a$ oder es gibt ein $n \in \mathbb{N}$, sodass $q \mid b^n$.

(3) Sei p_n die n-te Primzahl, d. h. $p_1 = 2$, $p_2 = 3$, usw. Seien $a, b, N \in \mathbb{N}$ mit $a = \prod_{i=1}^{N} p_i^{\alpha_i}$ und $b = \prod_{i=1}^{N} p_i^{\beta_i}$. Zeigen Sie:
   (a) $\mathrm{ggT}(a, b) = \prod_{i=1}^{N} p_i^{\min(\alpha_i, \beta_i)}$.
   (b) $\mathrm{kgV}(a, b) = \prod_{i=1}^{N} p_i^{\max(\alpha_i, \beta_i)}$.

   Folgern Sie daraus, dass für alle $a, b \in \mathbb{N}$ gilt: $\mathrm{kgV}(a, b) \cdot \mathrm{ggT}(a, b) = a \cdot b$.

(4) Seien $a, b, c \in \mathbb{N}$. Zeigen Sie:
   (a) $\mathrm{ggT}(\mathrm{ggT}(a, b), c) = \mathrm{ggT}(a, \mathrm{ggT}(b, c))$.
   (b) $\mathrm{kgV}(\mathrm{kgV}(a, b), c) = \mathrm{kgV}(a, \mathrm{kgV}(b, c))$.
   (c) $\mathrm{ggT}(\mathrm{kgV}(a, b), c) = \mathrm{kgV}(\mathrm{ggT}(a, c), \mathrm{ggT}(b, c))$.
   (d) $\mathrm{kgV}(\mathrm{ggT}(a, b), c) = \mathrm{ggT}(\mathrm{kgV}(a, c), \mathrm{kgV}(b, c))$.

(5) * Sei $n \in \mathbb{N}$, und seien $a_1, a_2, \ldots, a_n$ in $\mathbb{N}$. Wir definieren K_1 und K_2 durch:
   (a) $K_1(a_1) := a_1$, $K_1(a_1, a_2, \ldots, a_n) = \mathrm{kgV}(K_1(a_1, a_2, \ldots, a_{n-1}), a_n)$.
   (b) $K_2(a_1, a_2, \ldots, a_n) := \min\{z \in \mathbb{N} : a_i \mid z \text{ für alle } i \in \{1, 2, \ldots, n\}\}$.

   Zeigen Sie, dass K_1 und K_2 gleich sind.

(6) Sei $n \in \mathbb{N}$, und seien $a_1, a_2, \ldots, a_n$ in $\mathbb{N}$. Wir definieren K_2 durch

$$K_2(a_1, a_2, \ldots, a_n) := \min\{z \in \mathbb{N} : a_i \mid z \text{ für alle } i \in \{1, 2, \ldots, n\}\}.$$

Zeigen Sie, dass alle ganzen Zahlen, die Vielfaches eines jeden a_i sind, auch ein Vielfaches von $K_2(a_1, a_2, \ldots, a_n)$ sind.

Teil 3

Funktionen und Relationen

KAPITEL 5

Funktionen

1. Relationen

DEFINITION 5.1. Seien A, B Mengen. Jede Teilmenge von $A \times B$ heißt auch *Relation von A nach B*.

Beispiele:

- Sei $A := \{\text{Wien}, \text{Niederösterreich}, \text{Oberösterreich}, \text{Salzburg}, \text{Tirol}, \text{Vorarlberg}, \text{Burgenland}, \text{Steiermark}, \text{Kärnten}\}$ die Menge der neun österreichischen Bundesländer, und sei $B := \{\text{Donau}, \text{Inn}, \text{Traun}\}$. Wir definieren eine Relation R durch

  $$R := \{(a, b) \in A \times B \mid a \text{ besitzt einen Teil des Ufers von } b\}.$$

  Wir erhalten $R = \{(\text{Wien}, \text{Donau}), (\text{Niederösterreich}, \text{Donau}), (\text{Oberösterreich}, \text{Donau}), (\text{Tirol}, \text{Inn}), (\text{Oberösterreich}, \text{Inn}), (\text{Steiermark}, \text{Traun}), (\text{Oberösterreich}, \text{Traun})\}$.
- Für $(a, b) \in R$ schreiben wir auch $a\,R\,b$. Sei nun $A := \mathbb{R}$ und $B := \mathbb{Z}$. Wir definieren eine Relation ρ durch

  $$a\,\rho\,b :\Leftrightarrow a \in [b, b+1[$$

  für $a \in A$, $b \in B$. Dann gilt zum Beispiel $(\pi, 3) \in \rho$, $(\sqrt{2}, 1) \in \rho$. Es gilt also $\rho = \{(r, n) \in \mathbb{R} \times \mathbb{N} \mid n \leq r < n + 1\}$.
- Sei nun $A := \mathbb{N}$ und $B := \mathbb{N}$. Wir definieren eine Relation K durch

  $$(a, b) \in K :\Leftrightarrow \exists c \in \mathbb{N}_0 : a + c = b$$

  für $a \in A$, $b \in B$. Wir sehen, dass $K = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\}$. K ist also die „kleiner-gleich“-Relation.
- Nun definieren wir eine Relation $\equiv_5$ von $\mathbb{Z}$ nach $\mathbb{Z}$ durch

  $$a \equiv_5 b :\Leftrightarrow \exists c \in \mathbb{Z} : 5 \cdot c = b - a.$$

  Es gilt also

  $$\equiv_5 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b - a \text{ ist Vielfaches von } 5\}.$$

2. Funktionen

Definition 5.2. Seien A, B Mengen, und sei R eine Relation von A nach B. R ist eine *funktionale Relation von A nach B*, wenn es für alle $a \in A$ genau ein $b \in B$ gibt, sodass $(a, b) \in R$.

Beispiele: Seien $A := \{1, 2, 3\}$, $B := \{a, b, c\}$, $R := \{(1, a), (2, c), (3, c)\}$. Dann ist R eine funktionale Relation von A nach B.

Sei $A := \mathbb{R}$, $B := \mathbb{R}$, $f := \{(r, \sin(r)) \mid r \in \mathbb{R}\}$. Dann ist f eine funktionale Relation von $\mathbb{R}$ nach $\mathbb{R}$.

Sei $A := \mathbb{R}$, $B := \mathbb{R}$, $g := \{(\sin(r), r) \mid r \in \mathbb{R}\}$. Dann ist g keine funktionale Relation von $\mathbb{R}$ nach $\mathbb{R}$, da es kein $y \in \mathbb{R}$ gibt, sodass $(-2, y) \in \mathbb{R}$.

Sei $A := [-1, 1]$, $B := \mathbb{R}$, $h := \{(\sin(r), r) \mid r \in \mathbb{R}\}$. Dann ist h keine funktionale Relation von A nach $\mathbb{R}$, da $(0, 0) \in h$ und $(0, \pi) \in h$. Somit gibt es für $a := 0$ mehr als ein $b \in \mathbb{R}$, sodass $(a, b) \in h$.

Definition 5.3. Seien A, B Mengen, und sei f eine funktionale Relation von A nach B. Für $a \in A$ bezeichnen wir mit $f(a)$ dann jenes $b \in B$, für das $(a, b) \in f$.

Funktionale Relationen von A nach B bezeichnen wir auch einfach als *Funktionen von A nach B*. Funktionen kann man auf verschiedene Arten angeben. Wir betrachten einige gebräuchliche Varianten für die Quadratfunktion q auf den ganzen Zahlen.

(1) Direkt als Menge: $q := \{(x, x^2) \mid x \in \mathbb{Z}\}$. Die Menge kann natürlich auch anders angegeben werden, zum Beispiel durch $q := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid y = x^2\}$.
(2) Durch eine Zuordnungsvorschrift:

$$\begin{array}{rcccc} q & : & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & & x & \longmapsto & x^2. \end{array}$$

Man liest das als „q ist eine Funktion von $\mathbb{Z}$ nach $\mathbb{Z}$, die jedes x aus $\mathbb{Z}$ auf x^2 abbildet“.
(3) Durch Angabe des Funktionswerts, also etwa so: $q : \mathbb{Z} \to \mathbb{Z}$, $q(z) := z^2$ für $z \in \mathbb{Z}$. (Lies: „q ist eine Funktion von $\mathbb{Z}$ nach $\mathbb{Z}$, und $q(z)$ ist gleich z^2 für alle $z \in \mathbb{Z}$.“)

Egal, welche der drei Varianten man wählt: q ist dadurch jedesmal als die gleiche Teilmenge von $\mathbb{Z} \times \mathbb{Z}$ definiert. Die Schreibweise $f : A \to B$ bedeutet *f ist eine Funktion von A nach B*, also einfach *f ist eine funktionale Relation von A nach B*.

Übungsaufgaben 5.4.

(1) Welche der folgenden Relationen sind Funktionen von $\mathbb{N}$ nach $\mathbb{R}$? Begründen Sie Ihre Antwort, und geben Sie jene Relationen, die Funktionen sind, auch in der Form

$$\begin{array}{rccc} \ldots: & \mathbb{N} & \to & \mathbb{R} \\ & x & \mapsto & \ldots \end{array}$$

an.
   (a) $f = \{(x^3, x) \mid x \in \mathbb{R}\} \cap (\mathbb{N} \times \mathbb{R})$.
   (b) $g = \{((x-1)(x-2),\, x) \mid x \in \mathbb{R}\} \cap (\mathbb{N} \times \mathbb{R})$.
   (c) $h = \{(a, b) \in \mathbb{N} \times \mathbb{R} \mid b = \frac{a}{3}\}$.

DEFINITION 5.5 (Einschränkung). Seien A, B Mengen, sei T eine Teilmenge von A, und sei f eine Funktion von A nach B. Mit $f|_T$ bezeichnen wir die Funktion, die durch

$$\begin{array}{rccc} f & : & T & \longrightarrow & B \\ & & t & \longmapsto & f(t) \end{array}$$

gegeben ist. Sie heißt *Einschränkung von f auf T*.

Es gilt also $f|_T = \{(x, y) \in f \mid x \in T\} = f \cap (T \times B)$.

DEFINITION 5.6. Seien A, B Mengen. Mit B^A bezeichnet man die Menge aller Funktionen von A nach B. Genauer:

$$B^A := \{f \in \mathcal{P}(A \times B) \mid f : A \to B\}.$$

SATZ 5.7. *Seien $n, m \in \mathbb{N}$, und sei $A = \{1, \ldots, m\}$, $B := \{1, \ldots, n\}$. Dann hat B^A genau n^m Elemente.*

Beweisskizze: Um zu zählen, wieviele Funktionen f von $\{1, \ldots, m\}$ nach $\{1, \ldots, n\}$ es gibt, beobachten wir, dass wir n Möglichkeiten für $f(1)$, n Möglichkeiten für $f(2)$, ..., und n Möglichkeiten für $f(m)$ haben. Insgesamt gibt es also n^m Funktionen. □

3. Definitions- und Wertebereich

DEFINITION 5.8. Seien A, B Mengen, und sei f eine Funktion von A nach B. Dann heißt A auch der *Definitionsbereich* von f. Der *Wertebereich* von f ist die Menge $\{f(a) \mid a \in A\}$.

Den Wertebereich von f bezeichnet man auch als *Bildbereich* von f. Der Wertebereich einer Funktion von A nach B enthält also jene Elemente in B, die tatsächlich als Funktionswert auftreten. Er muss nicht gleich der ganzen Menge B sein. Wenn f eine Funktion von A nach B ist, so bezeichnen wir B auch als einen *Wertevorrat* oder eine *Zielmenge* von f.

DEFINITION 5.9. Seien A, B Mengen, und sei f eine Funktion von A nach B. Sei $T \subseteq A$. Dann bezeichnen wir mit $f[T]$ die *Bildmenge von T unter f*, die wir mit

$$f[T] = \{f(t) \mid t \in T\}$$

definieren.

Wenn keine Verwechslungen möglich sind, so schreibt man auch $f(T)$ anstelle von $f[T]$. Für die Sinusfunktion sin von $\mathbb{R}$ nach $\mathbb{R}$ ist der Wertebereich also das Intervall $[-1, 1]$. Außerdem gilt $\sin[\{n \cdot \frac{\pi}{4} \mid n \in \mathbb{N}\}] = \{-1, -\frac{\sqrt{2}}{2}, 0, \frac{\sqrt{2}}{2}, 1\}$.

SATZ 5.10. *Seien A, B Mengen, und sei f eine Funktion von A nach B. Seien $C, D \subseteq A$. Dann gilt*

(1) $f(C \cup D) = f(C) \cup f(D)$,
(2) $f(C \cap D) \subseteq f(C) \cap f(D)$.

ÜBUNGSAUFGABEN 5.11.

(1) Beweisen Sie Satz 5.10.
(2) Finden Sie ein Beispiel, für das $f(C \cap D) \neq f(C) \cap f(D)$ ist.

DEFINITION 5.12. Seien A, B Mengen, und sei f eine Funktion von A nach B.

(1) Die Funktion f ist *injektiv*, wenn
$$\forall x, y \in A : f(x) = f(y) \Rightarrow x = y$$
gilt.
(2) Die Funktion f ist *surjektiv auf B*, wenn es für alle $b \in B$ ein $a \in A$ gibt, sodass $f(a) = b$.
(3) Die Funktion f ist *bijektiv von A nach B*, wenn sie injektiv und surjektiv auf B ist.

Die Funktion f ist also injektiv, wenn es kein $x, y \in A$ mit $x \neq y$ und $f(x) = f(y)$ gibt. Wenn für eine Funktion $f : A \to B$ klar ist, welches B gemeint ist, sagt man oft einfach „f ist surjektiv“ anstelle von „f ist surjektiv auf B“. Im folgenden arbeiten wir darauf hin, die Wirkung einer Funktion wieder rückgängig zu machen, also, wenn möglich, aus dem Bild $f(x)$ einer Funktion das Argument x zu rekonstruieren.

SATZ 5.13. *Seien A, B Mengen, und sei f eine Funktion von A nach B. Sei*
$$g := \{(b, a) \in B \times A \mid (a, b) \in f\}.$$
Dann sind äquivalent:

(1) *g ist eine Funktion von B nach A.*
(2) *f ist eine bijektive Funktion von A nach B.*

Beweis: (2)⇒(1): Sei $b \in B$. Wir zeigen, dass es genau ein $a \in A$ gibt, sodass $(b, a) \in g$. Da f bijektiv ist, gibt es ein $a \in A$ mit $f(a) = b$, also mit $(a, b) \in f$. Dann gilt $(b, a) \in g$, und wir haben ein geeignetes $a \in A$ gefunden. Wir zeigen nun, dass es höchstens ein $a \in A$ mit $(b, a) \in g$ gibt. Seien $a_1, a_2 \in A$ so, dass $(b, a_1) \in g$ und $(b, a_2) \in g$. Dann gilt $(a_1, b) \in f$ und $(a_2, b) \in f$, also $b = f(a_1) = f(a_2)$. Da f injektiv ist, gilt $a_1 = a_2$. (1)⇒(2): Wir zeigen als erstes, dass f injektiv ist. Seien $a_1, a_2 \in A$ mit $f(a_1) = f(a_2)$. Also gilt $(a_1, f(a_1)) \in f$ und

$(a_2, f(a_2)) \in f$, und somit $(f(a_1), a_1) \in g$ und $(f(a_2), a_2) \in g$. Da g eine Funktion ist, muss wegen $f(a_1) = f(a_2)$ also auch $a_1 = a_2$ gelten. Somit ist f injektiv. Wir zeigen nun, dass f surjektiv ist. Sei dazu $b \in B$. Da g eine Funktion ist, gibt es ein $a \in A$ mit $(b, a) \in g$. Somit gilt $(a, b) \in f$, und folglich $f(a) = b$. Also liegt b im Wertebereich von f. Somit ist f surjektiv. □

DEFINITION 5.14. Seien A, B Mengen, und sei f eine bijektive Funktion von A nach B. Die Funktion $g : B \to A$ mit $g = \{(b, a) \in B \times A \mid f(a) = b\}$ heißt *die zu f inverse Funktion* oder *Umkehrfunktion von f*, und wird mit f^{-1} abgekürzt.

Die gleiche Schreibweise, f^{-1}, verwendet man auch für etwas anderes:

DEFINITION 5.15. Seien A, B Mengen, und sei f eine Funktion von A nach B. Sei $D \subseteq B$. Dann bezeichnet man mit $f^{-1}[D]$ (oder $f^{-1}(D)$) die Menge, die durch

$$f^{-1}[D] := \{a \in A \mid f(a) \in D\}$$

gegeben ist, und man nennt $f^{-1}[D]$ das *Urbild von D unter f*.

4. Familien und Folgen

Wir können es bestimmt nicht besser formulieren als P. Halmos [**Hal76**, S. 48].

> Gelegentlich wird der Wertebereich einer Funktion für wichtiger gehalten als die Funktion selbst. In einem solchen Falle werden Terminologie und Notation stark verändert. Sei zum Beispiel x eine Funktion von einer Menge I in eine Menge X. [...] Wir wollen jetzt ein Element des Definitionsbereiches I einen *Index* und I selbst die *Indexmenge* nennen; der Wertebereich der Funktion x soll *indizierte Menge* und die Funktion selbst *Familie* heißen; der Wert der Funktion an einer Stelle i, *Term* der Familie genannt, wird (anstelle von $x(i)$) nun x_i geschrieben.

DEFINITION 5.16. Seien I, X Mengen, und sei x eine Funktion von I nach X. Wir schreiben x_i für $x(i)$. Wir definieren nun $\langle x_i \mid i \in I\rangle$ durch

$$\langle x_i \mid i \in I\rangle := \{(i, x_i) \mid i \in I\}.$$

Es gilt also $x = \langle x_i \mid i \in I\rangle$.

Für $\langle x_i \mid i \in I\rangle$ schreibt man auch $(x_i)_{i\in I}$. Wenn f eine Funktion von A nach B, und C eine Teilmenge von A ist, schreibt man

$$\langle f(c) \mid c \in C\rangle \text{ oder } (f(c))_{c\in C}$$

für die Menge $\{(c, f(c)) \mid c \in C\}$.

DEFINITION 5.17. Sei A eine Menge, sei $n \in \mathbb{N}$, und seien $a_1, \ldots, a_n \in A$. Mit dem *n-Tupel* $\langle a_1, \ldots, a_n\rangle$ meinen wir die Familie $\langle a_i \mid i \in \{1, \ldots, n\}\rangle$.

Ein n-Tupel $\langle a_1, \ldots, a_n \rangle$ sehen wir also als eine mit der Indexmenge $\{1, \ldots, n\}$ indizierte Familie an. Das n-Tupel $\langle a_1, \ldots, a_n \rangle$ schreiben wir auch als $(a_1, \ldots, a_n)$; dass jetzt (a, b) zwei verschiedene (aber in der Praxis sehr ähnliche) Bedeutungen haben kann, stört meist nicht.

DEFINITION 5.18. Sei A eine Menge, und sei $n \in \mathbb{N}$. Mit A^n bezeichnen wir die Menge aller n-Tupel aus A, also

$$A^n := \{\langle a_1, \ldots, a_n \rangle \mid a_1, \ldots, a_n \in A\} = \{f \mid f : \{1, \ldots, n\} \to A\}.$$

DEFINITION 5.19. Sei $(X_i)_{i \in I}$ eine mit I indizierte Familie von Mengen. Dann ist

$$\begin{aligned}\prod_{i \in I} X_i &:= \{x : I \to \bigcup \{X_i \mid i \in I\} \;\mid\; \forall i \in I : x(i) \in X_i\} \\ &= \{(x_i)_{i \in I} \mid (x_i)_{i \in I} \text{ ist eine Familie mit } \forall i \in I : x_i \in X_i\}.\end{aligned}$$

Wenn alle X_i die gleiche Menge X sind, erhält man $\prod_{i \in I} X_i = X^I$. Die Menge der reellen Zahlenfolgen ist also zum Beispiel genau die Menge $\mathbb{R}^{\mathbb{N}}$.

Jetzt können wir noch ein Axiom der Mengenlehre angeben, das nicht aus den anderen Axiomen der Mengenlehre folgt. Es hat so überraschende Konsequenzen, dass man seine Verwendung, im Unterschied zur Verwendung der anderen Axiome der Mengenlehre, manchmal explizit macht, und etwa schreibt: „unter Verwendung des Auswahlaxioms gilt“.

AXIOM 5.20 (Auswahlaxiom). *Sei I eine Menge, und sei $(X_i)_{i \in I}$ eine Familie von Mengen. Wir nehmen an, dass für alle $i \in I$ die Menge X_i nicht leer ist. Dann ist auch $\prod_{i \in I} X_i$ nicht leer.*

In einer anderen Formulierung:

> Sei $(X_i)_{i \in I}$ eine Familie von nichtleeren Mengen. Dann gibt es eine Funktion f mit Definitionsbereich I, sodass für alle $i \in I : f(i) \in X_i$ gilt.

Ein solches f heißt auch *Auswahlfunktion*; daher der Name *Auswahlaxiom*.

Im Jahr 1937 zeigte K. Gödel[1]: wenn die üblichen Axiome der Mengenlehre widerspruchsfrei sind, so sind auch die Axiome zusammen mit dem Auswahlaxiom widerspruchsfrei. Das Auswahlaxiom bringt also keine „neuen“ Widersprüche. Im Jahr 1963 zeigte P. Cohen[2], dass man auch das Gegenteil des Auswahlaxioms, also die Existenz einer Familie nichtleerer Mengen, für die es keine Auswahlfunktion gibt, annehmen kann, ohne dadurch neue Widersprüche zu erhalten. Wenn also die üblichen Axiome der Mengenlehre widerspruchsfrei sind, so sind auch die Axiome zusammen mit der Negation des Auswahlaxioms widerspruchsfrei. Das Auswahlaxiom ist also unabhängig von den anderen Axiomen der Mengenlehre; seine Wahrheit wird von den anderen Axiomen nicht bestimmt. Legt man nur die üblichen Axiome der Mengenlehre zu Grunde,

[1] Kurt Gödel, 1906-1978
[2] Paul Cohen, 1934-2007

liegt das Auswahlaxiom also im „gesetzlich nicht geregelten Raum“. Wir werden das Auswahlaxiom als gültig voraussetzen.

ÜBUNGSAUFGABEN 5.21.

(1) (Funktionen) Für eine Funktion $f : X \to Y$ und $A \subseteq X$ schreiben wir $f[A]$ für $\{f(a) \mid a \in X\}$. Für welche Funktionen gilt, dass für alle Teilmengen A, B von X die Menge $f[A \cap B]$ gleich $f[A] \cap f[B]$ ist?

5. Hintereinanderausführung von Funktionen

DEFINITION 5.22. Seien A, B, C Mengen, sei f eine Funktion von A nach B, und sei g eine Funktion von B nach C. Wir definieren $g \circ f$ durch

$$\begin{array}{rccc} g \circ f & : & A & \longrightarrow & C \\ & & a & \longmapsto & g(f(a)). \end{array}$$

Die Funktion $g \circ f$ heißt die *Hintereinanderausführung* oder *funktionale Komposition* von f und g. Man spricht „g nach f“ für $g \circ f$.

SATZ 5.23 (Assoziativität der Hintereinanderausführung). *Seien A, B, C, D Mengen, und sei $f : A \to B$, $g : B \to C$, $h : C \to D$. Dann gilt $(h \circ g) \circ f = h \circ (g \circ f)$.*

Beweis: Zwei Funktionen α und β sind genau dann gleich, wenn sie den gleichen Definitionsbereich haben, und für alle x aus dem Definitionsbereich gilt, dass $\alpha(x) = \beta(x)$. Sei also $x \in A$. Dann gilt $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)) = h((g \circ f)(x)) = (h \circ (f \circ g))(x)$. □

SATZ 5.24 (Hintereinanderausführung und inverse Funktion). *Seien A, B Mengen, sei f eine bijektive Funktion von A nach B, und sei $f^{-1} := \{(b, a) \in B \times A \mid (a, b) \in f\}$ die zu f inverse Funktion. Dann gilt $f^{-1} \circ f = \mathrm{id}_A$ und $f \circ f^{-1} = \mathrm{id}_B$.*

Beweis: Sei $a \in A$. Dann gilt $(a, f(a)) \in f$, und somit $(f(a), a) \in f^{-1}$. Also gilt $f^{-1}(f(a)) = a$. Sei nun $b \in B$, und sei $a \in A$ so, dass $f(a) = b$. Dann gilt $(a, b) \in f$ und somit $(b, a) \in f^{-1}$. Also gilt $b = f(a) = f(f^{-1}(b))$. □

SATZ 5.25. *Seien A, B, C Mengen, sei f eine Funktion von A nach B, und sei g eine Funktion von B nach C.*

(1) *Wenn $g \circ f$ surjektiv auf C ist, so ist auch g surjektiv auf C.*
(2) *Wenn $g \circ f$ injektiv ist, so ist auch f injektiv.*

Beweis: (1) Sei $c \in C$. Da $g \circ f$ surjektiv ist, gibt es $a \in A$, sodass $g(f(a)) = c$. Dann belegt $b := f(a)$, dass es ein $b \in B$ gibt, sodass $g(b) = c$. Somit ist g surjektiv. (2) Seien $a_1, a_2 \in A$ so, dass $f(a_1) = f(a_2)$. Dann gilt auch $g(f(a_1)) = g(f(a_2))$. Da $g \circ f$ injektiv ist, erhalten wir $a_1 = a_2$. Somit ist f injektiv. □

ÜBUNGSAUFGABEN 5.26.

(1) Finden Sie Mengen A, B, C, eine Funktion $f : A \to B$ und eine Funktion $g : B \to C$, sodass g surjektiv und $g \circ f$ nicht surjektiv ist.
(2) Finden Sie Mengen A, B, C und $f : A \to B$, $g : B \to C$, sodass f injektiv und $g \circ f$ nicht injektiv ist.
(3) Finden Sie Mengen A, B, C und $f : A \to B$, $g : B \to C$, sodass $g \circ f$ surjektiv und f nicht surjektiv ist.
(4) Finden Sie Mengen A, B, C und $f : A \to B$, $g : B \to C$, sodass $g \circ f$ injektiv und g nicht injektiv ist.

Mit id_A bezeichnen wir die Funktion von A nach A mit $\mathrm{id}_A(x) = x$ für alle $x \in A$.

SATZ 5.27. *Seien A, B Mengen, sei f eine Funktion von A nach B, und seien l, r Funktionen von B nach A. Wenn $l \circ f = \mathrm{id}_A$ und $f \circ r = \mathrm{id}_B$, so ist f bijektiv, und es gilt $l = r = f^{-1}$.*

Beweis: Nach Satz 5.25 ist f bijektiv. Es gilt also $l = l \circ \mathrm{id}_B = l \circ (f \circ f^{-1}) = (l \circ f) \circ f^{-1} = \mathrm{id}_A \circ f^{-1} = f^{-1}$ und $r = \mathrm{id}_A \circ r = (f^{-1} \circ f) \circ r = f^{-1} \circ (f \circ r) = f^{-1} \circ \mathrm{id}_B = f^{-1}$. □

SATZ 5.28. *Seien A, B, C Mengen, sei f eine bijektive Funktion von A nach B, und sei g eine bijektive Funktion von B nach C. Dann ist $g \circ f$ eine bijektive Funktion von A nach C, und es gilt $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Beweis Es gilt $(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ ((f \circ f^{-1}) \circ g^{-1}) = g \circ (\mathrm{id}_B \circ g^{-1}) = g \circ g^{-1} = \mathrm{id}_C$ und $(f^{-1} \circ g^{-1}) \circ (g \circ f) = (f^{-1} \circ (g^{-1} \circ g)) \circ f = (f^{-1} \circ \mathrm{id}_B) \circ f = f^{-1} \circ f = \mathrm{id}_A$. Somit gilt wegen Satz 5.27, dass $f^{-1} \circ g^{-1} = (g \circ f)^{-1}$. □

6. Permutationen und Signatur

Für $n \in \mathbb{N}$ kürzen wir in diesem Abschnitt die Menge $\{1, 2, \ldots, n\}$ mit $\underline{n}$ ab.

DEFINITION 5.29. Eine *Permutation von $\underline{n}$* ist eine bijektive Abbildung von $\underline{n}$ nach $\underline{n}$.

Wir verwenden für Permutationen verschiedene Schreibweisen: Seien $a_1, \ldots, a_n$ paarweise verschiedene Elemente aus $\underline{n}$. Mit

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

kürzen wir die Funktion f mit $f(i) = a_i$ für $i \in \underline{n}$ ab.

Bestimmte Permutationen bezeichnet man als *Zyklen*. Seien $k \in \mathbb{N}$ und $i_1, \ldots, i_k$ paarweise verschiedene Elemente aus $\underline{n}$. Dann ist $f := (i_1\, i_2\, \ldots\, i_k)$ die Abbildung mit $f(i_r) = i_{r+1}$ für $r \in \{1, \ldots, k-1\}$, $f(i_k) = i_1$ und $f(j) = j$ für $j \in \underline{n} \setminus \{i_1, i_2, \ldots, i_k\}$. Diese Abbildung ist ein *Zyklus der Länge k*. Ein Zweierzyklus, also ein Zyklus der Länge 2, heißt auch *Transposition*.

Die Operation $\circ$ ist die Hintereinanderausführung von Permutationen: es gilt etwa $(1\,2) \circ (1\,3) = (1\,3\,2)$. Manchmal lassen wir das Zeichen $\circ$ weg und schreiben $(1\,2)\,(1\,3) = (1\,3\,2)$. Mit S_n bezeichnen wir die Menge aller Permutationen von $\underline{n}$.

DEFINITION 5.30. Sei $n \in \mathbb{N}$ und $f \in S_n$. Mit $F(f)$ bezeichnen wir die Menge der *Fehlstellen von* f, und definieren sie als

$$F(f) = \{(i,j) \in \underline{n} \times \underline{n} \mid i < j \text{ und } f(i) > f(j)\}.$$

Die *Signatur von* f ist definiert durch

$$\operatorname{sgn}(f) = (-1)^{|F(f)|}.$$

SATZ 5.31 (Multiplikativität der Signatur). *Seien $n \in \mathbb{N}$ und $f, g \in S_n$. Dann gilt*

$$\operatorname{sgn}(f \circ g) = \operatorname{sgn}(f) \cdot \operatorname{sgn}(g).$$

Beweis: Seien die Mengen B, C, D definiert durch

$$\begin{aligned} B &:= \{(i,j) \in \underline{n} \times \underline{n} \mid i < j \text{ und } g(i) < g(j) \text{ und } f(g(i)) > f(g(j))\}, \\ C &:= \{(i,j) \in \underline{n} \times \underline{n} \mid i < j \text{ und } g(i) > g(j) \text{ und } f(g(i)) < f(g(j))\}, \\ D &:= \{(i,j) \in \underline{n} \times \underline{n} \mid i < j \text{ und } g(i) > g(j) \text{ und } f(g(i)) > f(g(j))\}. \end{aligned}$$

Es gilt $F(f \circ g) = B \cup D$ und $F(g) = C \cup D$. Wir bestimmen nun $F(f)$ und definieren dazu I und J durch

$$\begin{aligned} I &:= \{(g(i), g(j)) \mid (i,j) \in B\}, \\ J &:= \{(g(j), g(i)) \mid (i,j) \in C\}. \end{aligned}$$

Wir zeigen als Nächstes:

$$F(f) = I \cup J. \tag{5.1}$$

$\subseteq$: Sei $(i,j) \in F(f)$. Seien $a, b \in \underline{n}$ so, dass $g(a) = i$ und $g(b) = j$.

1.Fall: $a < b$: Dann gilt $a < b$, wegen $i < j$ auch $g(a) < g(b)$, und wegen $(i,j) \in F(f)$ auch $f(i) > f(j)$, also $f(g(a)) > f(g(b))$. Folglich gilt $(a,b) \in B$, und somit $(i,j) = (g(a), g(b)) \in I$.

2. Fall: $a > b$: Dann gilt $b < a$, wegen $i < j$ auch $g(b) > g(a)$, und da (i,j) eine Fehlstelle ist, auch $f(g(b)) < f(g(a))$. Somit gilt $(b,a) \in C$ und damit $(i,j) = (g(a), g(b)) \in J$.

$\supseteq$: Sei $(i,j) \in I \cup J$.

1. Fall: $(i,j) \in I$: Dann gibt es $(a,b) \in B$, sodass $g(a) = i$ und $g(b) = j$. Wegen $(a,b) \in B$ gilt $g(a) < g(b)$ und $f(g(a)) > f(g(b))$. Somit gilt $(g(a), g(b)) \in F(f)$, also $(i,j) \in F(f)$.

2. Fall: $(i,j) \in J$: Dann gibt es $(a,b) \in C$ mit $i = g(b)$ und $j = g(a)$. Wegen $(a,b) \in C$ gilt $g(a) > g(b)$ und $f(g(a)) < f(g(b))$. Dann ist $(g(b), g(a))$ eine Fehlstelle von f, also gilt $(i,j) \in F(f)$.

Das beweist (5.1).

Es gilt $I \cap J = \varnothing$: Sei $(a,b) \in I \cap J$. Dann gibt es wegen $(a,b) \in I$ ein Paar $(i_1, j_1) \in B$ mit $(a,b) = (g(i_1), g(j_1))$, und wegen $(a,b) \in J$ ein Paar $(i_2, j_2) \in C$

mit $(a,b) = (g(j_2), g(i_2)$. Wegen der Injektivität von g gilt $i_1 = j_2$ und $j_1 = i_2$. Da $i_1 < j_1$, gilt $j_2 < i_2$, im Widerspruch zu $(i_2, j_2) \in C$.

Also gilt $|F(f)| = |I| + |J|$. Die Injektivität von g liefert $|B| = |I|$ und $|C| = |J|$. Folglich gilt

$$|F(f)| = |B| + |C|.$$

Somit gilt

$$\begin{aligned}\operatorname{sgn}(f) \cdot \operatorname{sgn}(g) &= (-1)^{|F(f)|} \cdot (-1)^{|F(g|} \\ &= (-1)^{|B|+|C|+|C|+|D|} \\ &= (-1)^{|B|+|D|} \\ &= (-1)^{|F(f\circ g)|}.\end{aligned}$$

Satz 5.32. *Für alle $i, j \in \underline{n}$ mit $i \neq j$ gilt* $\operatorname{sgn}((i\,j)) = -1$.

Beweis: Für den Fall, dass $i = 1$ und $j = 2$ bestimmen wir

$$\operatorname{sgn}((1\,2)) = (-1)^{|F((1\,2))|} = (-1)^1 = -1.$$

Seien nun $i, j \in \underline{n}$ mit $i \neq j$, sei $\tau := (i\,j)$, und sei f eine Permutation mit $f(1) = i$ und $f(2) = j$. Dann gilt

$$(i\,j) = f \circ (1\,2) \circ f^{-1}.$$

Sei dazu $x \in \underline{n}$. Wenn $x \notin \{i, j\}$, so gilt $f^{-1}(x) \notin \{1, 2\}$, und somit $\tau(f^{-1}(x)) = f^{-1}(x)$, also $f(\tau(f^{-1}(x))) = x$. Ausserdem gilt $f \circ (1\,2) \circ f^{-1}\,(i) = j$ und $f \circ (1\,2) \circ f^{-1}\,(j) = i$. Also gilt wegen Satz 5.31

$$\operatorname{sgn}((i\,j)) = \operatorname{sgn}(f)^2 \cdot \operatorname{sgn}((1\,2)) = -1.$$

□

Satz 5.33. *Sei $m \in \mathbb{N}$, $a, b \in \mathbb{N}_0$, $i, j \in \underline{m}$, und sei $\sigma \in S_m$.*

(1) *σ ist ein Produkt von endlich vielen Transpositionen. (Das Produkt von 0 Transpositionen definieren wir dabei als* id*.)*
(2) *Für alle Transpositionen $\rho_1, \ldots, \rho_a$ und $\tau_1, \ldots, \tau_b$ mit $\sigma = \rho_1 \circ \cdots \circ \rho_a = \tau_1 \circ \cdots \circ \tau_b$ teilt 2 die Differenz $a - b$.*
(3) *Für $n \in \mathbb{N}$ und paarweise verschiedene $i_1, \ldots, i_n \in \{1, \ldots, m\}$ gilt*

$$\operatorname{sgn}((i_1\ i_2\ \ldots\ i_n)) = (-1)^{n+1}.$$

Beweis: (1) Sei

$$M(\sigma) := \max(\{0\} \cup \{k \in \{1, \ldots, m\} \mid \sigma(k) \neq k\}).$$

Wir zeigen nun mit Induktion nach n, dass alle Permutationen mit $M(\sigma) = n$ Produkt von Transpositionen sind. Für $n = 0$ gilt $\sigma = \mathrm{id}$; σ ist dann also das Produkt von 0 Transpositionen. Sei nun $n \geq 1$, und sei σ so, dass $M(\sigma) = n$.

Sei $k := \sigma(n)$. Es gilt $k < n$. Sei $\rho := (k\ n) \circ \sigma$. Es gilt $\rho(n) = n$ und $\rho(r) = r$ für alle $r > n$. Also gilt $M(\rho) < n$. Somit gibt es nach Induktionsvoraussetzung Transpositionen $\tau_1, \ldots, \tau_l$ mit $\rho = \tau_1 \circ \cdots \circ \tau_l$. Also gilt $\sigma = (k\ n)^{-1} \circ \tau_1 \circ \cdots \circ \tau_l = (k\ n) \circ \tau_1 \circ \cdots \circ \tau_l$. Somit ist σ ebenfalls ein Produkt von Transpositionen.

(2) Die Signatur von σ ist $(-1)^a = (-1)^b$.

(3) Es gilt $(i_1\ i_2\ \ldots\ i_n) = (i_1\ i_n) \circ (i_1\ i_2\ \ldots,\ i_{n-1})$, somit folgt die behauptete Gleichheit durch Induktion nach n daraus, dass Transpositionen die Signatur -1 haben und die Signatur multiplikativ ist. □

Satz 5.34. *Sei $m \geq 2$, und seien $i, j \in \underline{m}$ mit $i < j$. Sei*

$$A_m := \{f \in S_m \mid \operatorname{sgn}(f) = 1\},$$

und sei $(i\ j) \circ A_m := \{(i\ j) \circ f \mid f \in A_m\}$. Dann gilt $A_m \cap ((i\ j) \circ A_m) = \varnothing$ und $A_m \cup ((i\ j) \circ A_m) = S_m$; außerdem ist $\varphi : A_m \to (i\ j) \circ A_m$, $f \mapsto (i\ j) \circ f$ bijektiv.

Beweis: Alle Elemente in A_m haben Signatur 1, alle Elemente in $(i\ j) \circ A_m$ haben Signatur -1, folglich ist ihr Schnitt leer.

Sei nun $f \in S_m$. Wenn $\operatorname{sgn}(f) = 1$, so liegt f in A_m. Wenn $\operatorname{sgn}(f) = -1$, so gilt $f = (i\ j) \circ (i\ j) \circ f$, und da $(i\ j) \circ f$ in A_m liegt, gilt $f \in (i\ j) \circ A_m$.

Um die Bijektivität von φ zu zeigen, definieren wir $\psi : (i\ j) \circ A_m \to A_m$, $f \mapsto (i\ j) \circ f$. Dann gilt $\psi \circ \varphi = \mathrm{id}_{\mathrm{A_m}}$ und $\varphi \circ \psi = \mathrm{id}_{\mathrm{(i\ j) \circ A_m}}$, folglich ist φ bijektiv. □

Übungsaufgaben 5.35.

(1) Der Beweis von Satz 5.33 (1) liefert eine Zerlegung von $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 6 & 7 & 1 & 5 \end{smallmatrix}\right)$ in ein Produkt von Transpositionen. Geben Sie diese Transpositionen an!
(2) Seien $f, g \in S_m$. Sei $F : S_m \to S_m$, $h \mapsto f \circ h \circ g$. Zeigen Sie, dass F bijektiv ist.
(3) Sei $F : S_m \to S_m$, $F(\sigma) := \sigma^{-1}$ für $\sigma \in S_m$. Zeigen Sie, dass F bijektiv ist.

KAPITEL 6

Relationen

1. Äquivalenzrelationen

Wir nennen eine Relation von A nach A auch eine *Relation auf A*.

DEFINITION 6.1. Sei ρ eine Relation auf A.

(1) ρ ist *reflexiv*, wenn für alle $a \in A$ gilt: $(a, a) \in \rho$.
(2) ρ ist *transitiv*, wenn für alle $a, b, c \in A$ gilt: wenn $(a, b) \in \rho$ und $(b, c) \in \rho$, so gilt auch $(a, c) \in \rho$.
(3) ρ ist *symmetrisch*, wenn für alle $a, b \in A$ gilt: wenn $(a, b) \in \rho$, so gilt auch $(b, a) \in \rho$.

DEFINITION 6.2. Sei ρ eine Relation auf A. Die Relation ρ ist eine *Äquivalenzrelation auf A*, wenn sie reflexiv, transitiv und symmetrisch ist.

DEFINITION 6.3. Sei ρ eine Äquivalenzrelation auf A, und sei $a \in A$. Die *Äquivalenzklasse von a bezüglich ρ* wird mit $[a]_\rho$ oder a/ρ abgekürzt, und ist definiert durch

$$a/\rho := \{b \in A \mid (a, b) \in \rho\}.$$

Eine Teilmenge C von A ist eine *Äquivalenzklasse von ρ*, wenn es ein $a \in A$ gibt, sodass $C = a/\rho$.

LEMMA 6.4. *Sei ρ eine Äquivalenzrelation auf A, und seien $a, b \in A$. Wenn $(a, b) \in \rho$, so gilt $[a]_\rho = [b]_\rho$.*

Beweis: Sei $c \in [a]_\rho$. Dann gilt $(a, c) \in \rho$. Wegen der Symmetrie von ρ gilt auch $(b, a) \in \rho$, und somit wegen der Transitivität von ρ auch $(b, c) \in \rho$. Somit gilt $c \in [b]_\rho$. Sei nun $c \in [b]_\rho$. Dann gilt $(b, c) \in \rho$ und somit wegen $(a, b) \in \rho$ und der Transitivität von ρ auch $(a, c) \in \rho$, und somit $c \in [a]_\rho$. □

ÜBUNGSAUFGABEN 6.5.

(1) Sei ρ eine Äquivalenzrelation auf A, und seien $a, b \in A$. Zeigen Sie, dass folgende Aussagen äquivalent sind:
   (a) $(a, b) \in \rho$.
   (b) $[a]_\rho = [b]_\rho$.
   (c) $a \in [b]_\rho$.
   (d) $[a]_\rho \cap [b]_\rho \neq \varnothing$.
(2) Geben Sie ein Beispiel für eine Äquivalenzrelation auf $A := \{2, 3, 4, 5\}$ an. Geben Sie die Relation in der Form $\rho = \{\dots\}$ an!

2. Partitionen

DEFINITION 6.6. Sei A eine Menge. Eine Teilmenge $\mathcal{P}$ von $\mathcal{P}(A)$ ist eine *Partition von* A, wenn

(1) für alle $P \in \mathcal{P} : P \neq \varnothing$,
(2) $\bigcup\{P \mid P \in \mathcal{P}\} = A$,
(3) für alle $P_1, P_2 \in \mathcal{P}$ mit $P_1 \neq P_2$ gilt $P_1 \cap P_2 = \varnothing$.

Wenn $\mathcal{P}$ eine Partition von A ist, so gibt es für jedes $a \in A$ genau ein $P \in \mathcal{P}$, sodass $a \in P$.

DEFINITION 6.7. Sei ρ eine Äquivalenzrelation auf A. Die *Faktormenge von A modulo ρ* ist die Menge $A/\rho := \{[a]_\rho \mid a \in A\}$.

SATZ 6.8. *Sei ρ eine Äquivalenzrelation auf A. Dann ist die Faktormenge von A bezüglich ρ eine Partition von A.*

Beweis: Sei $P \in A/\rho$. Dann gibt es ein $a \in A$, sodass $P = [a]_\rho = \{b \in A \mid (a, b) \in \rho\}$. Wegen der Reflexivität von ρ gilt $(a, a) \in \rho$, und folglich $a \in [a]_\rho$, also $a \in P$. Somit gilt $P \neq \varnothing$.

Wir zeigen nun, dass jedes $a \in A$ Element eines Elementes von A/ρ ist. Sei dazu $a \in A$. Dann gilt wegen der Reflexivität von ρ, dass $a \in [a]_\rho$. Somit ist a Element eines Elementes von A/ρ, nämlich von $[a]_\rho$.

Seien nun $P, Q \in A/\rho$. Seien $a, b \in A$ so, dass $P = [a]_\rho$ und $Q = [b]_\rho$. Wir nehmen nun an, dass $P \cap Q \neq \varnothing$. Es gibt dann also ein $c \in A$ mit $c \in P$ und $c \in Q$. Also gilt wegen $c \in [a]_\rho$ auch $(a, c) \in \rho$, und wegen $c \in [b]_\rho$ auch $(b, c) \in \rho$. Wegen der Symmetrie von ρ gilt daher auch $(c, b) \in \rho$, und daher, wegen der Transitivität von ρ, auch $(a, b) \in \rho$. Somit gilt nach Lemma 6.4 auch $P = Q$. □

SATZ 6.9. *Sei A eine Menge, und sei $\mathcal{P}$ eine Partition von A. Dann ist*

$$\rho := \{(a, b) \in A \times A \mid \exists P \in \mathcal{P} : a \in P \text{ und } b \in P\}$$

eine Äquivalenzrelation auf A.

DEFINITION 6.10. Sei A eine Menge, und sei ρ eine Äquivalenzrelation auf A. Eine Teilmenge R von A ist ein *Repräsentantensystem* von A modulo ρ, wenn für alle $a \in A$ die Menge $[a]_\rho \cap R$ genau ein Element enthält.

3. Zahlen als Äquivalenzklassen

Mithilfe von Äquivalenzrelationen können wir aus den natürlichen Zahlen die ganzen Zahlen konstruieren. Sei

$$M := \mathbb{N}_0 \times \mathbb{N}_0.$$

Das Paar (a, b) soll $a - b$ beschreiben. Dann sollen (a, b) und (c, d) die gleiche Zahl beschreiben, wenn $a - b = c - d$, also wenn $a + d = c + b$. Daher definieren wir eine Äquivalenzrelation δ durch

$$\big((a, b), (c, d)\big) \in \delta :\Leftrightarrow a + d = c + b.$$

Diese Relation ist reflexiv: Sei $(x, y) \in M$. Dann gilt $x + y = x + y$, also $\big((x, y), (x, y)\big) \in \delta$. Sie ist symmetrisch: Sei $\big((a, b), (c, d)\big) \in \delta$. Dann gilt $a + d = c + b$, also $c + b = a + d$, und somit $\big((c, d), (a, b)\big) \in \delta$. Sie ist transitiv: Seien $\big((a, b), (c, d)\big) \in \delta$ und $\big((c, d), (e, f)\big) \in \delta$. Dann gilt $a + d = c + b$ und $c + f = e + d$. Also gilt $a + d + c + f = c + b + e + d$. Somit gilt $a + f = e + b$, also $\big((a, b), (e, f)\big) \in \delta$. Wir definieren nun Z als die Faktormenge M/δ. Nun ist $\{(n, 0) \mid n \in \mathbb{N}_0\} \cup \{(0, n) \mid n \in \mathbb{N}\}$ ein Repräsentantensystem von M modulo δ. Für $n \in \mathbb{N}$ kürzen wir die Klasse $(0, n)/\delta$ mit $-n$ ab. Für die Klasse $(n, 0)/\delta$ schreiben wir einfach $+n$. Dann gilt $Z = \{-3, -2, -1, +0, +1, +2, +3, \ldots\}$.

Auch für die Einführung der rationalen Zahlen verwenden wir eine Äquivalenzrelation. Dabei klären wir zum Beispiel auch, ob $\frac{3}{4} = \frac{6}{8}$ gilt. Sei $A := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, und sei $(\binom{a}{b}, \binom{c}{d}) \in \rho$ genau dann, wenn $ad = bc$. Dann ist ρ eine Äquivalenzrelation, und $R := \{\binom{a}{b} \in A \mid b > 0, \operatorname{ggT}(a, b) = 1\}$ ist ein Repräsentantensystem. Die Faktormenge A/ρ bezeichnet man als die Menge der *rationalen Zahlen*. Für $[\binom{a}{b}]_\rho$ schreibt man $\frac{a}{b}$. Da $\frac{3}{4} = [\binom{3}{4}]_\rho = [\binom{6}{8}]_\rho = \frac{6}{8}$, gilt also wirklich $\frac{3}{4} = \frac{6}{8}$. Den Repräsentanten aus R eines Bruchs bezeichnet man als seine *gekürzte Darstellung*.

Übungsaufgaben 6.11.

(1) Geben Sie die Partition $\mathcal{P}$ der Menge $M = \{1, 2, 3\}$ an, die von der Äquivalenzrelation $\alpha = \{(1, 1), (2, 2), (3, 3), (1, 3), (3, 1)\}$ induziert wird.
(2) Geben Sie die Äquivalenzrelation β auf $M = \{1, 2, 3, 4\}$ an, die die Partition $\mathcal{P} = \{\{1\}, \{2, 4\}, \{3\}\}$ induziert.

4. Ordnungsrelationen

Definition 6.12. Sei M eine Menge, und sei ρ eine Relation auf M. Die Relation ρ ist *antisymmetrisch*, wenn für alle $x, y \in M$ mit $(x, y) \in \rho$ und $(y, x) \in \rho$ gilt: $x = y$.

Definition 6.13. Sei M eine Menge, und sei ρ eine Relation auf M. Die Relation ρ ist eine *Ordnungsrelation*, wenn sie *reflexiv*, *transitiv* und *antisymmetrisch* ist.

Definition 6.14. Sei M eine Menge, und sei $\leq$ eine Ordnungsrelation auf M. Die Relation $\leq$ ist *linear* (oder *total*) wenn für alle $x, y \in M$ gilt, dass $x \leq y$ oder $y \leq x$.

Ein Paar $(M, \leq)$ aus einer Menge und einer Ordnungsrelation bezeichnen wir als *geordnete Menge*. Wir schreiben auch $a < b$, wenn $a \leq b$ und $a \neq b$.

Definition 6.15. Sei $(M, \leq)$ eine geordnete Menge, und sei $a \in M$.

(1) a ist ein *kleinstes Element* von M, wenn für alle $b \in M$ gilt: $a \leq b$.
(2) a ist ein *minimales Element* von M, wenn es kein $b \in M$ mit $b < a$ gibt.
(3) Sei T eine Teilmenge von M, und sei $m \in M$. Das Element m ist eine *untere Schranke für* T, wenn für alle $t \in T$ gilt: $m \leq t$. (Eine untere Schranke kann, aber muss nicht, in T liegen.)
(4) a is ein *größtes Element* von M, wenn für alle $b \in M$ gilt: $b \leq a$.
(5) a ist ein *maximales Element* von M, wenn es kein b in M mit $a < b$ gibt.
(6) Sei T eine Teilmenge von M, und sei $m \in M$. Das Element m ist eine *obere Schranke für* T, wenn für alle $t \in T$ gilt: $t \leq m$.

Eine geordnete Menge $(M, \leq)$ hat höchstens ein kleinstes Element. Jedes kleinste Element ist minimal.

Teil 4

Die Mächtigkeit von Mengen

KAPITEL 7

Die Mächtigkeit von endlichen Mengen

1. Die Definition der Mächtigkeit

In diesem Kapitel geht es darum, die *Anzahl der Elemente* einer Menge zu bestimmen.

DEFINITION 7.1. Sei M eine Menge. Die Menge M ist *endlich*, wenn es ein $n \in \mathbb{N}_0$ und eine bijektive Funktion $f : \{x \in \mathbb{N} \mid 1 \leq x \leq n\} \to M$ gibt. Eine Menge, die nicht endlich ist, ist *unendlich*.

Wenn $f : \{1, 2, \ldots, n\} \to M$ bijektiv ist, so gilt $M = \{f(1), f(2), \ldots, f(n)\}$. Wir kürzen $\{1, 2, \ldots, n\}$ auch mit $\underline{n}$ ab.

DEFINITION 7.2. Sei M eine endliche Menge. Die *Anzahl der Elemente* von M (oder die *Mächtigkeit* oder die *Kardinalität* von M) ist jenes $n \in \mathbb{N}_0$, für das es eine bijektive Abbildung von $\{1, 2, \ldots, n\}$ nach M gibt. Wir schreiben $n = |M| = \#M$.

Da es für $n \neq m$ keine bijektive Abbildung von $\{1, 2, \ldots, n\}$ nach $\{1, 2, \ldots, m\}$ gibt, ist die Kardinalität einer endlichen Menge damit eindeutig bestimmt.

DEFINITION 7.3. Seien A, B Mengen. Wir sagen, dass A und B *gleichmächtig* sind ($A \sim B$), wenn es eine bijektive Funktion von A nach B gibt.

2. Grundlegende Abzählprinzipien

Eine Möglichkeit, die Kardinalität einer Menge zu bestimmen, ist, eine Bijektion zu einer Menge bekannter Kardinalität zu finden:

SATZ 7.4. *Seien A eine Menge und $n \in \mathbb{N}_0$ mit $\#A = n$. Sei B eine Menge, für die es eine bijektive Abbildung $g : A \to B$ gibt. Dann gilt $\#B = n$.*

SATZ 7.5. *Seien A, B endliche Mengen und $m := \#A$, $n := \#B$. Dann gilt $\#(A \times B) = mn$.*

Beweisskizze: Seien $f_A : A \to \underline{m}$ und $f_B : B \to \underline{n}$ bijektiv. Dann ist $g : A \times B \to \underline{mn}$, $g(a, b) := (f_A(a) - 1)n + f_B(b)$ für $(a, b) \in A \times B$ bijektiv. □

SATZ 7.6. *Seien A, B endliche Mengen mit $A \cap B = \varnothing$. Sei $m := \#A$, $n := \#B$. Dann gilt $\#(A \cup B) = m + n$.*

Beweisskizze: Seien $f_A : A \to \underline{m}$ und $f_B : B \to \underline{n}$ bijektiv. Dann ist $g : A \cup B \to \underline{m+n}$, $g := f_A \cup \{(b, f_B(b) + m) \mid b \in B\}$ bijektiv. □

3. Die Anzahl der Elemente einiger konkreter Mengen

Satz 7.7. *Seien A, B endliche Mengen, und sei $m := \#A$, $n := \#B$. Dann gilt $\#(B^A) = n^m$.*

Beweis: Induktion nach m. Für $m = 0$ gilt $A = \varnothing$, und somit $B^A = \{\varnothing\}$, also $\#(B^A) = 1$. Sei nun $m \geq 1$, und sei $a \in A$. Die Menge $B^{A\setminus\{a\}}$ hat nach Induktionsvoraussetzung n^{m-1} Elemente. Die Abbildung

$$\begin{array}{rccc} \Psi & : & B^A & \longrightarrow & B^{A\setminus\{a\}} \times B \\ & & f & \longmapsto & (f|_{A\setminus\{a\}}, f(a)) \end{array}$$

ist bijektiv; ihre Umkehrung ist

$$\begin{array}{rccc} \Phi & : & B^{A\setminus\{a\}} \times B & \longrightarrow & B^A \\ & & (f, b) & \longmapsto & f \cup \{(a, b)\}. \end{array}$$

Die Menge $B^{A\setminus\{a\}} \times B$ hat wegen der Induktionsvoraussetzung $n^{m-1} \cdot n$ Elemente. Also hat auch B^A genau n^m Elemente. □

Die Zahl n^m ist also die Anzahl der Möglichkeiten, eine Folge der Länge m aus einer n-elementigen Menge auszuwählen. Dabei darf das gleiche Element mehrmals vorkommen, und die Reihenfolge, in der die Elemente ausgewählt werden, ist wesentlich. Man nennt n^m daher auch die Anzahl der *Variationen von n Elementen der Länge m*. Als nächstes überlegen wir, in wievielen Variationen jedes Element höchstens einmal auftritt. Dazu definieren wir die *fallenden Faktoriellen.*

Definition 7.8. Sei $x \in \mathbb{Z}$ und $n \in \mathbb{N}_0$. Dann definieren wir $x^{\underline{n}}$ rekursiv durch $x^{\underline{0}} := 1$ und $x^{\underline{n}} := x \cdot ((x-1)^{\underline{n-1}})$ für $n \in \mathbb{N}$.

Es gilt also $x^{\underline{n}} = x(x-1)(x-2)\dots(x-n+1)$. Diese Notation kollidiert leicht mit der Definition $\underline{m} = \{1, 2, \dots, m\}$. Es wird stets aus dem Kontext klar sein, welche Bedeutung mit dem Unterstreichen gemeint ist.

Satz 7.9. *Seien A, B endliche Mengen, und sei $m := \#A$, $n := \#B$. Dann gilt $\#\{f : A \to B \mid f \text{ ist injektiv}\} = n^{\underline{m}}$.*

Beweis: Wir beweisen die Aussage durch Induktion nach m. Sei $I(A, B) := \{f : A \to B \mid f \text{ ist injektiv}\}$. Wenn $m = 0$, so gilt $A = \varnothing$ und $I(A, B) = \{\varnothing\}$, also $\#I(A, B) = 1 = n^{\underline{0}}$. Für den Induktionsschritt sei $m \geq 1$. Im Fall $n = 0$ gilt $|I(A, B)| = |\varnothing| = 0^{\underline{m}}$. Wir betrachten nun den Fall $n \geq 1$. Wir wählen $a \in A$. Es gilt

$$I(A, B) = \bigcup_{b \in B} \{f \cup \{(a, b)\} \mid f \in I(A \setminus \{a\}, B \setminus \{b\})\}.$$

Auf der rechten Seite werden n disjunkte Mengen vereinigt. Jede dieser n Mengen hat nach Induktionsvoraussetzung $(n-1)^{\underline{m-1}}$ Elemente. Folglich hat $I(A,B)$ genau $(n-1)^{\underline{m-1}} \cdot n = n^{\underline{m}}$ Elemente. □

Die Zahl $n^{\underline{m}}$ ist also die Anzahl der Möglichkeiten, eine Folge der Länge m aus einer n-elementigen Menge so auszuwählen, dass kein Element mehrmals vorkommt. Die Reihenfolge, in der die Elemente ausgewählt werden, ist wesentlich. Man nennt $n^{\underline{m}}$ daher auch die Anzahl der *Variationen von n Elementen der Länge m ohne Wiederholungen.*

Übungsaufgaben 7.10.

(1) Seien A, B nichtleere Mengen, sei $a \in A$ und $b \in B$. Für $b_1, b_2 \in B$ bezeichnen wir mit $\tau_B^{(b_1,b_2)}$ die bijektive Abbildung auf B, die durch $\tau_B^{(b_1,b_2)} : B \to B$ mit $\tau_B^{(b_1,b_2)}(b_1) = b_2$, $\tau_B^{(b_1,b_2)}(b_2) = b_1$, $\tau_B^{(b_1,b_2)}(x) = x$ für $x \in B \setminus \{b_1, b_2\}$ gegeben ist. Für $b_1 \neq b_2$ ist $\tau_B^{(b_1,b_2)}$ also eine Transposition. Wir betrachten nun

$$\begin{array}{rcccl} \Phi & : & I(A,B) & \longrightarrow & I(A\setminus\{a\}, B\setminus\{b\}) \times B \\ & & f & \longmapsto & \Big((\tau_B^{(f(a),b)} \circ f)|_{A\setminus\{a\}},\, f(a) \Big). \end{array}$$

und

$$\begin{array}{rcccl} \Psi & : & I(A\setminus\{a\}, B\setminus\{b\}) \times B & \longrightarrow & I(A,B) \\ & & (g,y) & \longmapsto & \tau_B^{(y,b)} \circ (g \cup \{(a,b)\}). \end{array}$$

Zeigen Sie, dass Φ und Ψ zueinander inverse Bijektionen sind. *Hinweis:* Berechnen Sie $\Psi(\Phi(f))$ und $\Phi(\Psi((g,y)))$ für $f \in I(A,B)$, $g \in I(A\setminus\{a\}, B\setminus\{b\})$ und $y \in B$.

(2) Schließen Sie aus dem vorigen Beispiel, dass fuer $|A| = m$ und $|B| = n$ gilt dass $|I(A,B)| = n^{\underline{m}}$.

Definition 7.11. Seien $m, n \in \mathbb{N}_0$. Wir definieren $m! := m^{\underline{m}}$ und den *Binomialkoeffizienten* $\binom{n}{m} := \frac{n^{\underline{m}}}{m!}$.

Satz 7.12. *Seien $m, n \in \mathbb{N}_0$, und sei B eine Menge mit n Elementen. Dann hat B genau $\binom{n}{m}$ Teilmengen mit m Elementen.*

Beweis: Sei $A := \{1, 2, \ldots, m\}$, und sei

$$F := \{(f, f[A]) \mid f \text{ ist eine injektive Funktion von } A \text{ nach } B\}.$$

Es gilt $|F| = n^{\underline{m}}$. Wir schreiben F nun anders als

$$\begin{aligned} F &= \{(g,T) \mid T \subseteq B,\, |T| = m,\, g : A \to T,\, g \text{ ist bijektiv}\} \\ &= \bigcup_{T\subseteq B, |T|=m} \{(g,T) \mid g : A \to T,\, g \text{ ist bijektiv}\}. \end{aligned}$$

Sei x die Anzahl der m-elementigen Teilmengen von B. Dann ist F die Vereinigung von x paarweise disjunkten Mengen, von denen jede Kardinalität $m!$ hat. Es gilt also $x \cdot (m!) = |F| = n^{\underline{m}}$. □

Die Zahl $\binom{n}{m}$ ist also die Anzahl der Möglichkeiten, m verschiedene Elemente aus einer n-elementigen Menge auszuwählen. Dabei ist die Reihenfolge, in der die Elemente ausgewählt werden, unwesentlich. Mann nennt $\binom{n}{m}$ daher auch die Anzahl der *Kombinationen von n Elementen der Länge m ohne Wiederholungen.*

SATZ 7.13 (Binomischer Lehrsatz). *Seien $a, b \in \mathbb{R}$ und $n \in \mathbb{N}_0$. Dann gilt*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.$$

Beweis: Durch Ausmultiplizieren erhalten wir

$$\begin{aligned}(a+b)^n &= \sum_{f:\{1,2,\ldots,n\}\to\{a,b\}} \prod_{i=1}^{n} f(i) \\ &= \sum_{M\subseteq\{1,2,\ldots,n\}} a^{n-|M|} b^{|M|} \\ &= \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.\end{aligned}$$

□

ÜBUNGSAUFGABEN 7.14.

(1) Zeigen Sie, dass für alle $n \in \mathbb{N}_0$ und $m \in \mathbb{N}$ gilt, dass

$$\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m-1}.$$

Hinweis: Rechnen Sie die rechte Seite aus und heben Sie in beiden Summanden $(n-1)\underline{m-2}$ heraus.

(2) Erklären Sie, wie die Rekursion aus dem vorigen Beispiel zum Pascalschen[1] Dreieck zur Berechnung der Binomialkoeffizienten führt. (Das Pascalsche Dreieck wurde auch von Omar Chayyām (1048-1131), Yang Hui (1238-1298) und Nicolò Tartaglia (1500-1557) er- bzw. gefunden.)

Für disjunkte endliche Mengen A, B gilt $|A \cup B| = |A| + |B|$. Das kann man auf nicht disjunkte endliche Mengen durch $|A \cup B| = |A| + |B| - |A \cap B|$ verallgemeinern. Für die Vereinigung von n Mengen gilt folgender Satz:

SATZ 7.15 (Inklusions- und Exklusionsprinzip). *Seien $A_1, \ldots, A_n$ endliche Mengen. Dann gilt*

$$\left| \bigcup_{i\in\{1,2,\ldots,n\}} A_i \right| = \sum_{\substack{M\subseteq\{1,2,\ldots,n\} \\ M\neq\varnothing}} (-1)^{|M|-1} \left| \bigcap_{j\in M} A_j \right|.$$

Beweis: Sei $B := \bigcup_{i\in\{1,\ldots,n\}} A_i$. Wir definieren eine Funktion

$$\chi : \mathcal{P}(B) \times B \to \{0, 1\}.$$

[1]Blaise Pascal (1623-1662)

Für $C \subseteq B$ und $b \in B$ sei $\chi(C,b) := 1$ wenn $b \in C$, und $\chi(C,b) := 0$, wenn $b \notin C$. Dann gilt

$$\begin{aligned}\sum_{\substack{M\subseteq \underline{n}\\ M\neq\varnothing}} (-1)^{|M|-1} \,|\bigcap_{j\in M} A_j| &= \sum_{\substack{M\subseteq \underline{n}\\ M\neq\varnothing}} (-1)^{|M|-1} \sum_{b\in B} \chi(\bigcap_{j\in M} A_j,\, b) \\ &= \sum_{b\in B} \sum_{\substack{M\subseteq \underline{n}\\ M\neq\varnothing}} (-1)^{|M|-1}\, \chi(\bigcap_{j\in M} A_j, b).\end{aligned} \tag{7.1}$$

Wir fixieren nun $b \in B$ und betrachten

$$\sum_{\substack{M\subseteq \underline{n}\\ M\neq\varnothing}} (-1)^{|M|-1} \chi(\bigcap_{j\in M} A_j, b).$$

Wenn b in genau k der Mengen $A_1, \ldots, A_n$ vorkommt, so liegt b in genau $\binom{k}{2}$ Schnitten von zwei dieser Mengen, in genau $\binom{k}{3}$ Schnitten von 3 dieser Mengen, und schließlich in genau $\binom{k}{k}$ Schnitten von genau k dieser Mengen. Es gilt also

$$\begin{aligned}\sum_{\substack{M\subseteq \underline{n}\\ M\neq\varnothing}} (-1)^{|M|-1}\, \chi(\bigcap_{j\in M} A_j,\, b) &= \sum_{i=1}^{n} \tbinom{k}{i} (-1)^{i-1} \cdot 1 \\ &= \sum_{i=1}^{k} \tbinom{k}{i} (-1)^{i-1} \cdot 1 \\ &= 1 - \sum_{i=0}^{k} \tbinom{k}{i} (-1)^{i} \cdot 1 \\ &= 1 - (1-1)^k.\end{aligned}$$

Der letzte Ausdruck ist 0 für $k = 0$ und 1 für $k \geq 1$. Somit können wir den letzten Ausdruck von (7.1) so ausrechnen:

$$\begin{aligned}\sum_{b\in B} \sum_{\substack{M\subseteq \underline{n}\\ M\neq\varnothing}} (-1)^{|M|-1}\, \chi(\bigcap_{j\in M} A_j, b) &= \sum_{b\in B} \chi(\bigcup_{j\in M} A_j, b) \\ &= \left|\bigcup_{j\in M} A_j\right|.\end{aligned}$$

□

Wir berechnen nun die Anzahl der Partitionen einer n-elementigen Menge in k Klassen. Dazu brauchen wir die *Stirlingzahlen 2. Art*[2].

[2]James Stirling (1692-1770)

DEFINITION 7.16. Für $n, k \in \mathbb{N}_0$ definieren wir die *Stirlingzahlen 2. Art* $S(n,k)$ rekursiv durch

$$\begin{aligned} &S(0,0) = 1, \\ &S(0,k) = 0 && \text{für } k \in \mathbb{N}, \\ &S(n,0) = 0 && \text{für } n \in \mathbb{N}, \\ &S(n,k) = k \cdot S(n-1,k) + S(n-1,k-1) && \text{für } n,k \in \mathbb{N}. \end{aligned}$$

Die folgende Tabelle gibt die Stirlingzahlen 2. Art an:

$S(n,k)$	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$	$k=9$	$k=10$	$k=11$	$k=12$
$n=0$	1	0	0	0	0	0	0	0	0	0	0	0	0
$n=1$	0	1	0	0	0	0	0	0	0	0	0	0	0
$n=2$	0	1	1	0	0	0	0	0	0	0	0	0	0
$n=3$	0	1	3	1	0	0	0	0	0	0	0	0	0
$n=4$	0	1	7	6	1	0	0	0	0	0	0	0	0
$n=5$	0	1	15	25	10	1	0	0	0	0	0	0	0
$n=6$	0	1	31	90	65	15	1	0	0	0	0	0	0
$n=7$	0	1	63	301	350	140	21	1	0	0	0	0	0
$n=8$	0	1	127	966	1701	1050	266	28	1	0	0	0	0
$n=9$	0	1	255	3025	7770	6951	2646	462	36	1	0	0	0
$n=10$	0	1	511	9330	34105	42525	22827	5880	750	45	1	0	0
$n=11$	0	1	1023	28501	145750	246730	179487	63987	11880	1155	55	1	0
$n=12$	0	1	2047	86526	611501	1379400	1323652	627396	159027	22275	1705	66	1

SATZ 7.17. *Sei A eine n-elementige Menge, und sei $k \in \mathbb{N}$. Sei*

$$C := \{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } A \text{ und } \#\mathcal{P} = k\}.$$

Dann gilt $\#C = S(n,k)$.

Beweis: Wir gehen mit Induktion nach n vor. Wenn $n = 0$, so gilt $A = \varnothing$. Die Partition $\mathcal{P} = \varnothing$ ist die einzige Partition von $\varnothing$ in $k = 0$ Klassen, also gilt $S(0,0) = 1$. Es gibt keine Partition von $\varnothing$ in $k \geq 1$ Mengen, also gilt $S(0,k) = 0$. Sei nun $n \geq 1$. Wenn $k = 0$, so gibt es keine Partition von A in k Mengen, also gilt $|C| = 0 = S(n,0)$. Wir betrachten nun den Fall $k \geq 1$. Wir wollen die Kardinalität der Menge

$$C = \{\mathcal{P} \mid \mathcal{P} \text{ ist Partition von } A \text{ in } k \text{ Klassen}\}$$

bestimmen. Wir wählen $a \in A$. Wir erhalten eine Partition von A in k Klassen, indem wir entweder eine Paritition von $A \setminus \{a\}$ in k Klassen bilden und a zu einer dieser k Klassen dazu geben, oder aber eine Partition von $A \setminus \{a\}$ in $k-1$ Klassen bilden, und $\{a\}$ als k-te Klasse zu dieser Partition dazugeben. Daraus erhalten wir die Gleichung.

$$S(n,k) = S(n-1,k) \cdot k + S(n-1,k-1).$$

Ausführlicher können wir dieses Argument so formulieren: Sei

$$X := \{(\mathcal{P}, P) \mid \mathcal{P} \text{ ist Partition von } A \setminus \{a\} \text{ in } k \text{ Klassen und } P \in \mathcal{P}\}.$$

Für jede Partition $\mathcal{P}$ von $A \setminus \{a\}$ in k Klassen sei

$$X_{\mathcal{P}} = \{(\mathcal{P}, P) \mid P \in \mathcal{P}\}.$$

Dann ist X die disjunkte Vereinigung

$$X = \bigcup \{X_{\mathcal{P}} \mid \mathcal{P} \text{ ist Partition von } A \setminus \{a\} \text{ in } k \text{ Klassen}\}.$$

Jedes $X_{\mathcal{P}}$ hat k Elemente, und nach Induktionsvoraussetzung ist X Vereinigung von $S(n-1,k)$ solchen Mengen. Somit gilt $\#X = S(n-1,k) \cdot k$. Sei nun

$$Y := \{(\mathcal{P} \cup \{\varnothing\}, \varnothing) \mid \mathcal{P} \text{ ist Partition von } A \setminus \{a\} \text{ in } k-1 \text{ Klassen}\}.$$

Die Mengen X und Y sind disjunkt. Wir geben nun eine Abbildungen Φ an, die aus einer Partition von $A \setminus \{a\}$ und der Klasse, in die wir a aufnehmen wollen, eine Partition von A baut. Diese Funktion Φ geht von $X \cup Y$ nach C. Für $(\mathcal{P}, P) \in X \cup Y$ definieren wir

$$\Phi(\mathcal{P}, P)) := (\mathcal{P} \setminus \{P\}) \cup \{P \cup \{a\}\}.$$

Wir suchen nun die inverse Funktion von Φ. Für eine Partition $\mathcal{P}$ von A und $x \in A$ definieren wir $[x]_{\mathcal{P}}$ als jenes Element Q von $\mathcal{P}$ mit $x \in Q$. Die Funktion $\Psi : C \to X \cup Y$ ist durch

$$\Psi(\mathcal{P}) := (\{P \setminus \{a\} \mid P \in \mathcal{P}\},\, [a]_{\mathcal{P}} \setminus \{a\})$$

definiert. Wir zeigen nun, dass Φ und Ψ zueinander invers sind. Sei dazu $\mathcal{P} \in C$. Wir berechnen $\Phi(\Psi(\mathcal{P}))$. Es gilt

$$\begin{aligned}
\Phi(\Psi(\mathcal{P})) &= \Phi(\{P \setminus \{a\} \mid P \in \mathcal{P}\},\, [a]_{\mathcal{P}} \setminus \{a\}) \\
&= \big(\big\{P \setminus \{a\} \mid P \in \mathcal{P}\big\} \setminus \big\{[a]_{\mathcal{P}} \setminus \{a\}\big\}\big) \cup \big\{([a]_{\mathcal{P}} \setminus \{a\}) \cup \{a\}\big\} \\
&= \{P \in \mathcal{P} \mid a \notin P\} \cup \{[a]_{\mathcal{P}}\} \\
&= \mathcal{P}.
\end{aligned}$$

Sei nun $(\mathcal{P}, P) \in X \cup Y$. Dann gilt

$$\begin{aligned}
\Psi(\Phi((\mathcal{P}, P)) &= \Psi((\mathcal{P} \setminus \{P\}) \cup \{P \cup \{a\}\}) \\
&= \Big(\big\{Q \setminus \{a\} \mid Q \in (\mathcal{P} \setminus \{P\}) \cup \{P \cup \{a\}\}\big\},\, P\Big) \\
&= \Big(\big\{Q \setminus \{a\} \mid Q \in \mathcal{P} \setminus \{P\}\big\} \cup \big\{Q \setminus \{a\} \mid Q = P \cup \{a\}\big\},\, P\Big) \\
&= (\{Q \mid Q \in \mathcal{P} \setminus \{P\}\} \cup \{P\},\, P) \\
&= (\mathcal{P}, P).
\end{aligned}$$

Somit sind Φ und Ψ bijektiv, und es gilt $|C| = |X| + |Y|$. Nach Induktionsvoraussetzung gilt $|Y| = S(n-1,k-1)$, und somit $|C| = k \cdot S(n-1,k) + S(n-1,k-1) = S(n,k)$. □

Satz 7.18. *Seien A , B endliche Mengen, und sei $m := \#A$, $n := \#B$. Sei C die Menge der surjektiven Funktionen von A auf B. Dann gilt $\#C = S(m,n) \cdot (n\,!)$.*

Beweis: Für eine Funktion $f : A \to B$ sei

$$\mathcal{P}(f) := \{f^{-1}[\{b\}] \mid b \in f[A]\}$$

die von f induzierte Partition. Wir zeigen nun, das für zwei Funktionen $f, g : A \to B$ gilt, dass $\mathcal{P}(f) = \mathcal{P}(g)$ genau dann gilt, wenn es eine bijektive Abbildung $t : f[A] \to g[A]$ mit $g = t \circ f$ gibt.

Nehmen wir dazu zuerst an, dass es ein solches t gibt. Sei $P \in \mathcal{P}(g)$. Dann gibt es ein $b \in B$ mit $P = g^{-1}[\{b\}] = (t \circ f)^{-1}[\{b\}] = f^{-1}[\{t^{-1}(b)\}]$, und somit $P \in \mathcal{P}(f)$. Unter Verwendung von $f = t^{-1} \circ g$ zeigt man auch $\mathcal{P}(g) \subseteq \mathcal{P}(f)$. Seien nun f, g so, dass $\mathcal{P}(f) = \mathcal{P}(g)$. Wir definieren eine Relation t durch

$$\{(f(a), g(a)) \mid a \in A\}.$$

Diese Relation ist eine Funktion von $f[A]$ nach $g[A]$. Seien dazu $a_1, a_2 \in A$ so, dass $f(a_1) = f(a_2)$. Dann gilt $\{a_1, a_2\} \subseteq f^{-1}[\{f(a_1)\}] \in \mathcal{P}(f)$. Somit gilt $f^{-1}[\{f(a_1)\}] \in \mathcal{P}(g)$, und daher gibt es $b \in g$ mit $f^{-1}[\{f(a_1)\}] = g^{-1}[\{b\}]$. Also gilt $f(a_1) = f(a_2) = b$. Somit ist t funktional. Mit der gleichen Begründung erhalten wir, dass auch die Relation $s := \{(g(a), f(a)) \mid a \in A\}$ funktional ist. Somit ist t bijektiv und es gilt für alle $a \in A$, dass $t(f(a)) = g(a)$, also $t \circ f = g$.

Wir betrachten nun

$$F := \{(f, \mathcal{P}(f)) \mid f \text{ ist surjektiv von } A \text{ auf } B\}.$$

Sei x die Anzahl der surjektiven Funktionen von A nach B. Dann gilt $|F| = x$. Sei S die Menge der Partitionen von A in n Klassen. Wir schreiben F nun als

$$F = \bigcup_{\mathcal{P} \in S} \{(f, \mathcal{P}) \mid f \text{ ist surjektiv von } A \text{ auf } B \text{ und } \mathcal{P}(f) = \mathcal{P}\}.$$

Sei $\mathcal{P} \in S$. Es gibt dann eine surjektive Funktion $g : A \to B$ mit $\mathcal{P}(g) = \mathcal{P}$. Dann gilt

$$\{(f, \mathcal{P}) \mid f \text{ ist surjektiv von } A \text{ auf } B \text{ und } \mathcal{P}(f) = \mathcal{P}\} = \{(t \circ g, \mathcal{P}) \mid t \text{ ist bijektiv von } B \text{ nach } B\}.$$

Diese Menge hat $n!$ Elemente. Also ist F die Vereinigung von $S(m, n)$ disjunkten Mengen der Kardinalität $n!$, und somit gilt $x = |F| = S(m, n) \cdot (n!)$.

4. Die Mächtigkeit beliebiger Mengen

Wir rufen uns die Definition davon, dass zwei Mengen gleichmächtig sind, in Erinnerung:

Definition 7.19. Seien A, B Mengen. Wir sagen, dass A und B *gleichmächtig* sind ($A \sim B$), wenn es eine bijektive Funktion von A nach B gibt.

Diese Definition lässt sich auch für unendliche Mengen verwenden.

SATZ 7.20. *Sei C eine Menge. Dann ist $\sim$ auf $\mathcal{P}(C)$ eine Äquivalenzrelation.*

Unendliche Mengen bieten das erstaunliche Phänomen, dass eine Menge gleichmächtig zu einer echten Teilmenge sein kann.

PROPOSITION 7.21. $\mathbb{Z} \sim \mathbb{N} \sim \mathbb{N} \times \mathbb{N}$.

Beweis: Die Funktion

$$\begin{array}{rcccl} f & : & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & & x & \longmapsto & \begin{cases} -2x+2 \text{ wenn } x \leq 0 \\ 2x-1 \text{ wenn } x \geq 1 \end{cases} \end{array}$$

ist bijektiv. Ebenso ist

$$\begin{array}{rcccl} f & : & \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ & & (x,y) & \longmapsto & 2^{x-1} \cdot (2y-1) \end{array}$$

bijektiv. □

DEFINITION 7.22. Eine Menge B ist *abzählbar unendlich*, wenn sie gleichmächtig zu $\mathbb{N}$ ist. Eine Menge ist *abzählbar*, wenn sie endlich oder abzählbar unendlich ist.

DEFINITION 7.23. Seien A, B Mengen. Wir sagen, dass A *höchstens so mächtig wie* B (oder B *mindestens so mächtig wie* A) ist, wenn es eine injektive Funktion von A nach B gibt. Das kürzen wir mit $A \precsim B$ ab. B ist *mächtiger als* A, wenn B mindestens so mächtig wie A ist, und A und B nicht gleichmächtig sind.

ÜBUNGSAUFGABEN 7.24.

(1) Zeigen Sie, dass das reelle Intervall $[0,4]$ gleichmächtig zu $[0,2]$ ist.
(2) Seien A, B Mengen mit $A \precsim B$. Zeigen Sie, dass es eine surjektive Funktion von B auf A gibt.
(3) Seien A, B Mengen, sodass es eine surjektive Funktion s von B auf A gibt. Zeigen Sie, dass dann $A \preceq B$. *Hinweis:* Verwenden Sie das Auswahlaxiom für $\prod_{a \in A} s^{-1}[\{a\}]$.
(4) Wir nehmen an, dass $A_1 \sim A_2$ und $B_1 \sim B_2$. Zeigen Sie, dass dann auch $A_1 \times B_1 \sim A_2 \times B_2$ und $\mathcal{P}(A_1) \sim \mathcal{P}(A_2)$.
(5) Sei A eine Menge. Finden Sie eine bijektive Abbildung von $\mathcal{P}(A)$ nach $\{0,1\}^A$.

Für jede Menge A gilt $A \precsim A$.

SATZ 7.25. *Seien A, B, C Mengen mit $A \precsim B$ und $B \precsim C$. Dann gilt $A \precsim C$.*

Beweis: Die Hintereinanderausführung injektiver Funktionen ist injektiv. □

Nun überlegen wir uns, was passiert, wenn $A \precsim B$ und $B \precsim A$. Dazu beweisen wir zuerst folgendes Lemma.

LEMMA 7.26. *Sei Y eine Menge, und sei U eine Teilmenge von Y. Wir nehmen an, dass es eine injektive Funktion $g : Y \to U$ gibt. Dann sind Y und U gleichmächtig.*

Beweis: Sei $V := Y \setminus U$, und

$$U_1 := \bigcap \{B \subseteq U \mid g[V \cup B] \subseteq B\}.$$

Wir zeigen nun

$$g[V \cup U_1] \subseteq U_1. \tag{7.2}$$

Sei dazu $w \in V \cup U_1$. Wir wollen zeigen, dass $g(w) \in \bigcap \{B \mid B \subseteq U \text{ und } g[V \cup B] \subseteq B\}$. Dazu zeigen wir, dass $g(w)$ in jeder Teilmenge B von U mit $g[V \cup B] \subseteq B$ liegt. Sei also $B \subseteq U$ so, dass $g[V \cup B] \subseteq B$. Wegen $U_1 \subseteq B$ gilt auch $w \in V \cup B$. Daher gilt $g(w) \in g[V \cup B]$, und somit $g(w) \in B$. Somit gilt (7.2).

Nun zeigen wir

$$g[V \cup U_1] = U_1. \tag{7.3}$$

Nehmen wir nun an, dass $g[V \cup U_1] \neq U_1$. Dann gibt es ein $u_1 \in U_1$, sodass $u_1 \notin g[V \cup U_1]$. Dann gilt $g[V \cup (U_1 \setminus \{u_1\})] \subseteq U_1 \setminus \{u_1\}$. Somit ist $B := U_1 \setminus \{u_1\}$ eine der Mengen, die bei der Bildung von U_1 geschnitten wurden. Also gilt $u_1 \notin U_1$, im Widerspruch zur Wahl von u_1. Somit gilt (7.3).

Somit ist $g|_{V \cup U_1}$ eine bijektive Funktion von $V \cup U_1$ nach U_1. Da $Y = V \cup U = (V \cup U_1) \cup (U \setminus U_1)$ und $U = U_1 \cup (U \setminus U_1)$, ist $h := g|_{V \cup U_1} \cup \mathrm{id}_{U \setminus U_1}$ eine bijektive Funktion von Y nach U. □

Dieses Lemma ist der entscheidende Schritt, um den folgenden Satz zu beweisen.

Satz 7.27 (Satz von Cantor-Schröder-Bernstein[3]). *Seien A, B Mengen mit $A \precsim B$ und $B \precsim A$. Dann gilt $A \sim B$.*

Beweis: Sei $f : A \to B$ injektiv und $g : B \to A$ injektiv. Dann ist $f \circ g$ eine injektive Funktion, und es gilt $f \circ g\,[B] \subseteq f[A]$.

Sei nun $Y := B$ und $U := f[A]$. Nun ist $f \circ g$ eine injektive Funktion von Y nach U. Nach Lemma 7.26 gibt es eine bijektive Funktion $h : Y \to U$. Nun ist f bijektiv von A nach $f[A]$, und h^{-1} bijektiv von $f[A]$ nach B, also ist $h^{-1} \circ f$ bijektiv von A nach B. Somit gilt $A \sim B$. □

Zuletzt überlegen wir uns noch, ob für zwei Mengen stets $A \precsim B$ oder $B \precsim A$ gilt, oder ob es Mengen „unvergleichbarer Mächtigkeit“ geben kann. Die Antwort wird sein, dass es unter Annahme des Auswahlaxioms keine solchen Mengen unvergleichbarer Mächtigkeit geben kann. Wir werden im Beweis aber nicht das Auswahlaxiom verwenden, sondern einen Satz, das Lemma von Zorn[4]. Das Lemma von Zorn ist äquivalent zum Auswahlaxiom; wir könnten anstelle des Auswahlaxioms für Mengen also auch das Lemma von Zorn als Axiom fordern und würden dann das Auswahlaxiom als Satz erhalten.

[3]Georg Cantor (1845-1918), Ernst Schröder (1841-1902), Felix Bernstein (1878-1956)
[4]Max August Zorn (1906-1993)

SATZ 7.28 (Lemma von Zorn). *Sei $(M, \leq)$ eine geordnete Menge mit folgender Eigenschaft:*

> *Für alle Teilmengen T von M mit der Eigenschaft, dass $(T, \leq)$ linear geordnet ist, gibt es ein $m \in M$, sodass für alle $t \in T$: $t \leq m$.*

Dann hat M ein maximales Element.

Dabei ist mit $(T, \leq)$ genau genommen $(T, \leq \cap (T \times T))$ gemeint. Die Forderung an M ist, dass jede linear geordnete Teilmenge T von M eine obere Schranke besitzt, die zwar nicht in T, aber sehr wohl in M liegen muss. Der Beweis des Lemmas von Zorn ist aufwändig und benötigt das Auswahlaxiom. In der Praxis ist das Lemma von Zorn ein hilfreiches Instrument zum Beweis für die Existenz von Dingen, die in irgendeinem Sinn „maximal“ sind. Eine Anwendung geben wir im folgenden Satz.

SATZ 7.29 (Vergleichbarkeitssatz). *Seien A, B Mengen. Dann gilt $A \preceq B$ oder $B \preceq A$.*

Beweis: Sei

$\mathcal{F} := \{f \subseteq A \times B \mid$ es gibt $C \subseteq A$, sodass f eine injektive Funktion von C nach B ist$\}$.

Wir verwenden nun das Lemma von Zorn, um zu zeigen, dass $(\mathcal{F}, \subseteq)$ ein maximales Element f_0 besitzt. Sei dazu $\mathcal{T}$ eine mit $\subseteq$ linear geordnete Teilmenge von $\mathcal{F}$. Wir bilden die Menge

$$g := \bigcup \mathcal{T} = \bigcup \{f \mid f \in \mathcal{T}\}.$$

Die Menge g ist also die Vereinigung aller Funktionen in $\mathcal{T}$. Wir zeigen nun als erstes, dass g wieder eine funktionale Relation von einer Teilmenge von A nach B ist. Sei dazu $C := \{a \in A \mid \exists b \in B : (a, b) \in g\}$. Wir zeigen, dass g eine Funktion von C nach B ist. Sei dazu $a \in C$. Aus der Definition von C geht unmittelbar hervor, dass es ein b gibt, sodass $(a, b) \in g$. Um die Funktionalität zu zeigen, müssen wir noch nachweisen, dass dieses b eindeutig ist. Seien also $b_1, b_2 \in B$ so, dass $(a, b_1) \in g$ und $(a, b_2) \in g$. Dann gibt es f_1 und f_2 in $\mathcal{T}$, sodass $(a, b_1) \in f_1$ und $(a, b_2) \in f_2$. Die Menge $\mathcal{T}$ ist linear geordnet, also gilt $f_1 \subseteq f_2$ oder $f_2 \subseteq f_1$. Wenn $f_1 \subseteq f_2$, so gilt $(a, b_1) \in f_2$ und $(a, b_2) \in f_2$. Da f_2 eine Funktion ist, gilt also $b_1 = b_2$. Im Fall $f_2 \subseteq f_1$ erhalten wir $(a, b_2) \in f_1$, und somit $b_1 = b_2$, weil f_1 funktional ist. Somit ist g eine Funktion.

Wir zeigen als nächstes, dass g injektiv ist. Seien dazu $a_1, a_2 \in g$ so, dass $g(a_1) = g(a_2)$. Nach der Konstruktion von g gibt es $h_1, h_2 \in \mathcal{T}$, sodass $(a_1, g(a_1)) \in h_1$ und $(a_2, h(a_2)) \in h_2$, also $h_1(a_1) = g(a_1)$ und $h_2(a_2) = g(a_2)$. Die Menge $\mathcal{T}$ ist linear geordnet, und folglich gilt $h_1 \subseteq h_2$ oder $h_2 \subseteq h_1$. Wenn $h_1 \subseteq h_2$, so gilt $(a_1, g(a_1)) \in h_2$, und somit $h_2(a_1) = g(a_1)$. Dann gilt $h_2(a_1) = g(a_1) = g(a_2) = h_2(a_2)$. Nun verwenden wir, dass h_2 injektiv ist, und erhalten $a_1 = a_2$. Ebenso erhalten wir im Fall $h_2 \subseteq h_1$, dass $a_1 = a_2$. Die Funktion g ist also injektiv.

Somit liegt g in $\mathcal{F}$, und g ist eine obere Schranke für die Menge $\mathcal{T}$. Nun verwenden wir das Lemma von Zorn. Es liefert uns ein maximales Element f_0 von $\mathcal{F}$.

Wenn der Definitionsbereich C_0 von f_0 gleich A ist, so gilt $A \preceq B$.

Wenn f_0 surjektiv auf B ist, so ist f_0 eine bijektive Funktion von C_0 nach B; also ist f_0^{-1} injektiv von B nach C_0, und es gilt $B \preceq A$.

Der verbleibende Fall ist, dass $C_0 \neq A$ und $f_0[C_0] \neq B$. In diesem Fall wählen wir $a_0 \in A \setminus C_0$ und $b_0 \in B \setminus f_0[C_0]$. Dann ist $f_0 \cup \{(a_0, b_0)\}$ ebenfalls eine injektive Funktion, also $f_0 \in \mathcal{F}$, im Widerspruch zur Maximalität von f_0. □

5. Einige abzählbar unendliche Mengen

Satz 7.30. *Es gilt* $\mathbb{Q} \sim \mathbb{N}$.

Beweis: Nach dem Satz von Cantor-Schröder-Bernstein genügt es $\mathbb{N} \precsim \mathbb{Q}$ und $\mathbb{Q} \precsim \mathbb{N}$ zu zeigen. Klarerweise ist $f : \mathbb{N} \to \mathbb{Q}$, $x \mapsto \frac{x}{1}$ injektiv, also gilt $\mathbb{N} \precsim \mathbb{Q}$.
Wir bilden nun eine injektive Abbildung $g : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$ durch

$$g(\tfrac{a}{b}) := (a/\mathrm{ggT}(a,b), b/\mathrm{ggT}(a,b)),$$

für $a, b \in \mathbb{Z}$ mit $b > 0$. Diese Abbildung ist wohldefiniert und injektiv. Da $\mathbb{Z} \times \mathbb{N} \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{N}$, gibt es eine injektive Abbildung von $\mathbb{Z} \times \mathbb{N}$ nach $\mathbb{N}$, und somit gilt $\mathbb{Q} \precsim \mathbb{N}$. (Ebenso ist $h : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$, $(a, b) \mapsto \frac{a}{b}$ surjektiv auf $\mathbb{Q}$. Unter Verwendung des Auswahlaxioms gilt also deshalb $\mathbb{Q} \precsim \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$, und folglich $\mathbb{Q} \precsim \mathbb{Z} \times \mathbb{N} \precsim \mathbb{N} \times \mathbb{N} \precsim \mathbb{N}$.) □

Satz 7.31. *Sei* $\langle A_i \mid i \in \mathbb{N} \rangle$ *eine Familie von Mengen. Wir nehmen an, dass für alle* $i \in \mathbb{N}$ *gilt :* $A_i \precsim \mathbb{N}$. *Dann gilt auch* $\bigcup_{i \in \mathbb{N}} A_i \precsim \mathbb{N}$.

Beweis: Sei $f_i : A_i \to \mathbb{N}$ injektiv. Wir bilden nun $f : \bigcup\{A_i \mid i \in \mathbb{N}\} \to \mathbb{N} \times \mathbb{N}$ durch $f(a) := (k_1, k_2)$, wobei $k_1 := \min\{j \in \mathbb{N} \mid a \in A_j\}$ und $k_2 := f_{k_1}(a)$. Diese Abbildung ist injektiv und beweist $\bigcup\{A_i \mid i \in \mathbb{N}\} \precsim \mathbb{N} \times \mathbb{N}$. Wegen $\mathbb{N} \times \mathbb{N} \precsim \mathbb{N}$ folgt die Behauptung. □

Übungsaufgaben 7.32.

(1) Zeigen Sie, dass für jedes a mit $a \notin \mathbb{N}$ die Menge $\{a\} \cup \mathbb{N}$ gleichmächtig zu $\mathbb{N}$ ist.
(2) Zeigen Sie, dass die Vereinigung einer abzählbar unendlichen mit einer endlichen Menge abzählbar unendlich ist.
(3) Zeigen Sie, dass eine Vereinigung von abzählbar vielen abzählbaren Mengen abzählbar ist, indem Sie eine surjektive Abbildung von $\mathbb{N} \times \mathbb{N}$ auf diese Menge definieren.
(4) Zeigen Sie, dass für jedes $n \in \mathbb{N}$ die Menge $\mathbb{N}^n$ gleichmächtig zu $\mathbb{N}$ ist.
(5) Zeigen Sie, dass für nichtleere abzählbare Menge A die Menge $A^* := \bigcup\{A^n \mid n \in \mathbb{N}\}$ abzählbar unendlich ist.
(6) Zeigen Sie, dass die Menge der endlichen Teilmengen von $\mathbb{N}$ gleichmächtig zu $\mathbb{N}$ ist.

6. Einige überabzählbar unendliche Mengen

Eine Menge C ist *überabzählbar unendlich*, wenn C unendlich und nicht gleichmächtig zu $\mathbb{N}$ ist. Zunächst überlegen wir uns, warum es solche Mengen gibt.

Lemma 7.33. *Sei A eine Menge. Dann gibt es keine surjektive Funktion von A auf $\mathcal{P}(A)$.*

Beweis: Sei $f : A \to \mathcal{P}(A)$. Wir zeigen, dass f nicht surjektiv auf $\mathcal{P}(A)$ sein kann. Wir betrachten dazu

$$B := \{x \in A \mid x \notin f(x)\}.$$

Wir zeigen nun, dass B nicht im Wertebereich von f liegt. Dazu zeigen wir, dass für alle $a \in A$ gilt: $f(a) \neq B$. Sei also $a \in A$.

- *1.Fall:* $a \in f(a)$. Wenn $a \in f(a)$, so gilt $a \notin B$. Das Element a liegt also in $f(a)$, aber nicht in B. Somit gilt $f(a) \neq B$.
- *2. Fall:* $a \notin f(a)$. Wenn $a \notin f(a)$, so gilt $a \in B$. Das Element a liegt also in B, aber nicht in $f(a)$. Somit gilt $f(a) \neq B$.

B liegt also nicht im Wertebereich von f; somit ist f nicht surjektiv auf $\mathcal{P}(A)$. □

Damit haben wir die entscheidende Information, um folgenden Satz zu beweisen:

Satz 7.34 (Satz von Cantor). *Sei A eine Menge. Dann gilt $A \precsim \mathcal{P}(A)$, und $A \nsim \mathcal{P}(A)$.*

Beweis: Die Abbildung $f : A \to \mathcal{P}(A)$, $a \mapsto \{a\}$ ist injektiv, also gilt $A \precsim \mathcal{P}(A)$. Wenn $A \sim \mathcal{P}(A)$, so gibt es eine bijektive Abbildung von A nach $\mathcal{P}(A)$. Diese Abbildung ist surjektiv auf $\mathcal{P}(A)$, im Widerspruch zu Lemma 7.33. Also gilt $A \nsim \mathcal{P}(A)$. □

Damit haben wir also unendliche Mengen gefunden, die nicht abzählbar sind, etwa $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathbb{Z})$, $\{0,1\}^{\mathbb{N}}$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$.

Satz 7.35. *Die Menge $\mathbb{R}$ der reellen Zahlen ist gleichmächtig zu $\mathcal{P}(\mathbb{N})$, also überabzählbar.*

Beweis: Die Funktion $f : \mathcal{P}(\mathbb{N}) \to \mathbb{R}$, $I \mapsto \sum_{i \in I} 10^{-i}$ ist injektiv und belegt $\mathcal{P}(\mathbb{N}) \precsim \mathbb{R}$. Sei nun q eine bijektive Funktion von $\mathbb{N}$ nach $\mathbb{Q}$. Wir schreiben für $q(i)$ kurz q_i. Dann ist $g : \mathbb{R} \to \mathcal{P}(\mathbb{N})$, $r \mapsto \{i \in \mathbb{N} \mid q_i < r\}$ injektiv, da zwischen zwei verschiedenen reellen Zahlen stets eine rationale Zahl liegt. Somit gilt nach dem Satz von Cantor-Schröder-Bernstein $\mathcal{P}(\mathbb{N}) \sim \mathbb{R}$. □

Übungsaufgaben 7.36.

(1) Zeigen Sie, dass das reelle Intervall $[0, 2]$ gleichmächtig zu $\mathbb{R}$ ist.

7. Einige Sätze über unendliche Mengen

In dieser Sektion stellen wir noch einige Sätze über unendliche Mengen zusammen. Diese Sätze haben gemeinsam, dass man für die Beweise das Auswahlaxiom benötigt.

Satz 7.37. *Jede unendliche Menge M enthält eine abzählbar unendliche Teilmenge.*

Beweis: Sei $f : \mathcal{P}(M) \setminus \{\varnothing\} \to M$ so, dass $f(A) \in A$ für alle $A \subseteq M$. So ein f existiert, weil nach dem Auswahlaxiom die Menge $\prod_{A \in \mathcal{P}(M) \setminus \{\varnothing\}} A$ nicht leer ist.

Sei $\mathcal{F}$ die Menge aller endlichen Teilmengen von M. Wir definieren eine Funktion $E : \mathbb{N} \to \mathcal{F}$ rekursiv. Da M nicht leer ist, können wir können wir $E(1) := \{f(M)\}$ definieren, und für alle $n \in \mathbb{N}$: $E(n+1) = E(n) \cup \{f(M \setminus E(n))\}$.

Sei nun $g : \mathbb{N} \to M$ definiert durch $g(n) := f(M \setminus E(n))$. Wir zeigen nun, dass g injektiv ist. Sei $n_1 < n_2$. Es gilt $g(n_2) = f(M \setminus E(n_2)) \notin E(n_2)$. Da $g(n_1) = f(M \setminus E(n_1))$, gilt $g(n_1) \in E(n_1) \cup \{f(M \setminus E(n_1))\}$, also $g(n_1) \in E(n_1 + 1)$, und somit $g(n_1) \in E(n_2)$. Also gilt $g(n_1) \neq g(n_2)$. Folglich ist $g[\mathbb{N}]$ eine abzählbare Teilmenge von M. □

Übungsaufgaben 7.38.

(1) Sei A unendlich und E endlich. Zeigen Sie $A \cup E \sim A$. *Hinweis:* Benutzen Sie eine abzählbare Teilmenge B von A und verwenden Sie $B \cup E \sim B$.
(2) Sei B unendlich. Zeigen Sie, dass es eine Funktion $f : B \to B$ gibt, die injektiv, aber nicht surjektiv ist. *Hinweis:* Lösen Sie das Beispiel zuerst für $B := \mathbb{N}$.
(3) Zeigen Sie $[0, 1] \sim]0, 1[\sim \mathbb{R}$.

Satz 7.39. *Seien A, B Mengen mit $A \precsim B$. Wir nehmen an, dass B unendlich ist. Dann gilt*

(1) *$A \cup B \sim B$;*
(2) *Wenn A nicht leer ist, so gilt $A \times B \sim B$;*
(3) *Wenn A zumindest zwei Elemente enthält, so gilt $A^B \sim \mathcal{P}(B)$.*

Beweis: [**Hal76**, Kapitel 24]. □

Übungsaufgaben 7.40.

(1) Zeigen Sie ohne Verwendung des Teils (3) von Satz 7.39, dass $\mathbb{N}^{\mathbb{R}} \sim \mathcal{P}(\mathbb{R})$.
(2) Zeigen Sie $\mathbb{R}^{\mathbb{N}} \sim \mathbb{R}$. *Hinweis:* Finden Sie eine injektive Abbildung von $\mathcal{P}(\mathbb{N})^{\mathbb{N}}$ nach $\mathcal{P}(\mathbb{N} \times \mathbb{N})$.

8. Erstaunliches über Mengen

Satz 7.41. *Sei A eine Menge, und sei $B := \{a \in A \mid a \notin a\}$. Dann gilt $B \notin A$.*

Beweis: Nehmen wir an, dass $B \in A$.

- *1.Fall: $B \notin B$*: Dann gilt $B \in A$ und $B \notin B$. Also gilt $B \in B$, im Widerspruch zur Fallannahme. Dieser Fall kann also nicht auftreten.
- *2. Fall: $B \in B$*: Dann erfüllt B die Eigenschaft, die unter den Elementen von A jene in B auswählt; es gilt also $B \notin B$, im Widerspruch zur Fallannahme.

Somit ist die Annahme $B \in A$ falsch; es gilt also $B \notin A$. □

Damit gibt es auch keine Menge, die alle Mengen als Elemente enthalten würde: jede Menge M enthält zumindest die Menge $\{m \in M \mid m \notin m\}$ nicht als Element. Der Begriff „die Menge aller Mengen“ ist also widersprüchlich, weil er von einem Objekt, das es nicht gibt, nämlich einer Menge aller Mengen, so spricht, als ob es dieses Objekt gäbe. Dass es eine „Menge aller Mengen“ nicht gibt, ist das *Russell'sche Paradoxon*.

Eine berühmte Vermutung (die Kontinuumshypothese) sagt, dass folgende Frage die Antwort „ja“ hat.

PROBLEM 7.42. *Gilt für jede unendliche Teilmenge A von $\mathbb{R}$: $A \sim \mathbb{R}$ oder $A \sim \mathbb{N}$?*

K. Gödel[5] zeigte, dass die Axiome der Zermelo-Fraenkelschen Mengenlehre, wenn widerspruchsfrei, auch unter Zuhilfenahme des Auswahlaxioms nicht erlauben, die Antwort „nein“ herzuleiten. P. Cohen[6] zeigte, dass die Axiome der Zermelo-Fraenkelschen Mengenlehre und das Auswahlaxiom, wenn widerspruchsfrei, nicht erlauben, die Antwort „ja“ herzuleiten. Die Gültigkeit von „$\forall A \subseteq \mathbb{R} : A \sim \mathbb{R}$ oder $A \sim \mathbb{N}$ oder A ist endlich“ wird also durch die Axiome der Zermelo-Fränkelschen Mengenlehre nicht geregelt.

[5]Kurt Gödel (1906-1978)
[6]Paul Cohen (1934-2007)

Literaturverzeichnis

[BT09] Bramanti, M. und G. Travaglini: *Matematica. Questione di metodo*. Zanichelli, Bologna, 2009.

[Euk91] Euklid: *Die Elemente*. Wissenschaftliche Buchgesellschaft, Darmstadt, 1991. Buch I–XIII. [Book I–XIII], Based on Heiberg's text, Translated from the Greek and edited by Clemens Thaer.

[Hal76] Halmos, P. R.: *Naive Mengenlehre*. Vandenhoeck & Ruprecht, Göttingen, 1976. Vierte Auflage, Aus dem Englischen übersetzt von Manfred Armbrust und Fritz Ostermann, Moderne Mathematik in elementarer Darstellung, No. 6.

[Pea89] Peano, I.: *Arithmetices Principia. Nova methodo exposita*. Fratres Bocca, Rom – Florenz, 1889.

[RU87] Remmert, R. und P. Ullrich: *Elementare Zahlentheorie*. Birkhäuser Verlag, Basel, 1987.