Diskrete Strukturen

und

Lineare Algebra I für Informatiker

Skript zur Vorlesung

Dr. Timo Hanke
Prof. Dr. Gerhard Hiß
Lehrstuhl D für Mathematik
RWTH Aachen

Letzte Aktualisierung:
18. Oktober 2018

Unter der freundlichen Mithilfe von:
Wolf-Daniel Andres, Grischa Studzinski und Florian Weingarten.

Inhaltsverzeichnis

Grundlagen

Kapitel 1

Mathematische Grundbegriffe

1.1 Aussagen

1.1.1 Definition und Beispiele

Definition. *Mathematische Aussagen* oder kurz *Aussagen* sind sprachliche Ausdrücke, die auch Formeln und Symbole enthalten können, und die einen eindeutigen *Wahrheitswert* besitzen, der entweder *wahr* oder *falsch* lautet.

Beispiel. Mathematische Aussagen sind:

(i) '$2 + 3 = 5$' (wahr)

(ii) 'Alle Punkte auf einem Kreis haben den gleichen Abstand zum Mittelpunkt' (wahr)

(iii) 'Jede ganze Zahl größer als 2 ist Summe zweier Primzahlen' (unbekannt)

(iv) 'Jede reelle Zahl ist ein Quadrat einer reellen Zahl' (falsch)

(v) 'Es gibt eine ganze Zahl, deren Quadrat gleich ihrem Doppelten ist' (wahr)

Die Aussage (iii) ist eine mathematische Aussage, denn sie besitzt einen Wahrheitswert, auch wenn uns dieser nicht bekannt ist. Die *Goldbach'sche Vermutung* besagt, dass der Wahrheitswert von (iii) wahr lautet. Keine mathematischen Aussagen sind dagegen 'Aachen ist schön' und 'Die Mensapreise sind zu hoch'.

1.1.2 Zusammensetzung und Verneinung

Definition a. Für beliebige Aussagen A und B definieren wir die Wahrheitswerte für folgende *zusammengesetzte Aussagen*:

(i) Die *Negation* (*Verneinung*) $\neg A$ ist genau dann wahr, wenn A falsch ist.

(ii) Die *Konjunktion* (*und*-Verknüpfung) $A \wedge B$ ist genau dann wahr, wenn sowohl A als auch B wahr ist.

(iii) Die *Disjunktion* (*oder*-Verknüpfung) $A \vee B$ ist genau dann wahr, wenn A oder B wahr ist oder beide wahr sind.

(iv) Das *exklusive oder* $A \operatorname{xor} B$ ist genau dann wahr, wenn A oder B wahr ist, aber nicht beide wahr sind.

(v) Die *Subjunktion* (*wenn-dann*-Verknüpfung) $A \to B$ ist genau dann falsch, wenn A wahr ist und B falsch ist.

(vi) Die *Bijunktion* (*genau-dann*-Verknüpfung) $A \leftrightarrow B$ ist genau dann wahr, wenn A und B den gleichen Wahrheitswert besitzen.

Sprechweise. Zu $\neg A$ sagt man „nicht A“, zu $A \wedge B$ „A und B“, zu $A \vee B$ „A oder B“, zu $A \operatorname{xor} B$ „A x-or B“ oder „entweder A oder B“, zu $A \to B$ „wenn A dann B“, zu $A \leftrightarrow B$ „A gilt genau dann, wenn B gilt“.

Wahrheitstafel. Die Wahrheitswerte der eingeführten zusammengesetzten Aussagen können in folgender Tabelle zusammengefasst werden. Dies ist ein Beispiel für eine *Wahrheitstafel*. Wir schreiben 1 bzw. 0 für die Wahrheitswerte *wahr* bzw. *falsch*.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \operatorname{xor} B$	$A \to B$	$A \leftrightarrow B$
1	1	0	1	1	0	1	1
1	0	0	0	1	1	0	0
0	1	1	0	1	1	1	0
0	0	1	0	0	0	1	1

Beispiel.

(i) Die Verneinung von ‘$2+3 = 5$’ lässt sich als ‘Es gilt nicht, dass $2+3 = 5$ ist’ oder kürzer als ‘$2 + 3$ ist ungleich 5’ formulieren.

(ii) Die Verneinung von 'Das Glas ist voll' lässt sich als 'Das Glas ist nicht voll' formulieren, nicht aber als 'Das Glas ist leer'.

(iii) Die Verneinung von 'Alle Gläser sind voll' lässt sich als 'Nicht alle Gläser sind voll', oder als 'Es gibt ein Glas, das nicht voll ist' formulieren.

(iv) 'Wenn $2+3=6$, dann ist $2+3=7$' ist wahr.

Definition b. Seien A und B Aussagen.

(i) Ist $A \to B$ wahr, dann schreiben wir $A \Rightarrow B$ und sagen: "*Aus A folgt B*" oder "*A impliziert B*" oder "*Wenn A, dann B*" oder "*A ist hinreichend für B*" oder "*B ist notwendig für A*".

(ii) Ist $A \leftrightarrow B$ wahr, dann schreiben wir $A \Leftrightarrow B$ und sagen: "*A genau dann, wenn B*" oder "*A dann und nur dann, wenn B*" oder "*A ist notwendig und hinreichend für B*".

1.1.3 Tautologien

Definition. (i) Ein *logischer Term* ist ein Ausdruck bestehend aus Variablen $A, B, \ldots$ und den Konstanten 1 und 0, die verknüpft sind mit den Symbolen $\neg, \wedge, \vee, \text{xor}, \to, \leftrightarrow$ (und Klammern). Durch Belegung der Variablen mit Wahrheitswerten bekommt der Term selbst einen Wahrheitswert.

(ii) Zwei logische Terme S und T, definiert auf derselben Variablenmenge, heißen *logisch äquivalent* oder *wertverlaufsgleich*, geschrieben $S \equiv T$, wenn S und T denselben Wahrheitswert haben für jede Belegung der Variablen.

(iii) Ein logischer Term T heißt *Tautologie*, wenn $T \equiv w$.

Beispiel a. Im Folgenden stellen wir einige einfachen logischen Äquivalenzen zusammen.

(i)
- $A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$
- $A \vee (B \vee C) \equiv (A \vee B) \vee C$

(ii)
- $A \wedge 1 \equiv A$
- $A \vee 0 \equiv A$

(iii)
- $A \wedge B \equiv B \wedge A$

- $A \vee B \equiv B \vee A$

(iv)
- $A \wedge A \equiv A$
- $A \vee A \equiv A$

(v)
- $A \wedge \neg A \equiv 0$
- $A \vee \neg A \equiv 1$

(vi)
- $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
- $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$

(vii)
- $A \wedge (A \vee B) \equiv A$
- $A \vee (A \wedge B) \equiv A$

Beispiel b. Durch logische Äquivalenzen lassen sich logische Symbole durch andere ersetzen.

(i) $A \operatorname{xor} B \equiv (A \wedge \neg B) \vee (\neg A \wedge B)$.

Wir sagen daher, dass xor durch $\neg, \wedge, \vee$ ausgedrückt werden kann.

(ii) $A \to B \equiv \neg(A \wedge \neg B)$.

(iii) $A \leftrightarrow B \equiv \neg(A \operatorname{xor} B)$.

Übung a. Man zeige, dass xor durch $\neg, \vee$ ausgedrückt werden kann.

Beispiel c. $A \wedge \neg B$ und $A \to ((B \to \neg C) \vee D)$ sind logische Terme, aber keine Tautologien. $(A \to B) \leftrightarrow \neg(A \wedge \neg B)$ ist eine Tautologie. Bedeutsame Tautologien sind:

(i) Modus Ponens:

$$(A \wedge (A \to B)) \to B$$

(ii) Tertium non datur (Gesetz des ausgeschlossenen Dritten):

$$A \vee \neg A$$

(iii) de Morgan-Gesetze:

$$\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B),$$
$$\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$$

(iv) Kontrapositionsgesetz:

$$(A \to B) \leftrightarrow (\neg B \to \neg A)$$

Bemerkung a. Es seien S, T logische Terme. Dann gilt $S \equiv T$ genau dann, $S \leftrightarrow T$ eine Tautologie ist.

Übung b.

(i) Man schreibe die Tautologien auf, die von Beispiel b geliefert werden.

(ii) Ist $(A \leftrightarrow B) \leftrightarrow ((A \to B) \wedge (B \to A))$ eine Tautologie?

(iii) Man folgere aus den Tautologien des Beispiels durch Einsetzen, dass auch $\neg(A \wedge \neg A)$ eine Tautologie ist.

(iv) Gelten die „Distributivgesetze“ $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$ und $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$?

Bemerkung b. Tautologien helfen bei Beweisen: Aus Modus Ponens folgt $(A \wedge (A \to B)) \Rightarrow B$; zeigt man also, dass A wahr ist und $A \Rightarrow B$ gilt (d.h. dass $A \to B$ wahr ist), so folgt, dass auch B wahr ist.

Möchte man $A \Rightarrow B$ zeigen, so kann man nach dem Kontrapositionsgesetz anstelle dessen auch $\neg B \Rightarrow \neg A$ zeigen (z.B. statt ‘Wenn x kein Quadrat ist, dann $x < 0$’ zeigt man ‘Wenn $x \geq 0$, dann x ein Quadrat’).

1.1.4 Aussageformen

Definition. Eine *Aussageform* ist ein sprachlicher Ausdruck, der Variablen enthält, und der für jede Belegung aller vorkommenden Variablen mit konkreten Objekten zu einer Aussage wird. (Diese letzte Bedingung führt dazu, dass die Auswahl der Objekte, mit denen die Variablen belegt werden können, i.A. eingeschränkt ist; siehe Beispiel (i) unten.)

Bemerkung. Eine Aussageform ist selbst keine Aussage. Die Zusammensetzung von Aussageformen mittels $\neg, \wedge, \vee, \to, \leftrightarrow$, etc. ist wieder eine Aussageform.

Beispiel.

(i) ‘Wenn $x > 0$, dann ist x ein Quadrat.’ ist eine Aussageform. Wird die Variable x mit einer beliebigen reellen Zahl belegt, so erhalten wir eine Aussage (einen eindeutigen Wahrheitswert).

Hier setzen wir implizit voraus, dass die Variable x nur mit Objekten belegt wird, für die die Aussage $x > 0$ Sinn ergibt (definiert ist).

(ii) ‘Person x hat mindestens 50% der Klausur-Punkte erzielt’ ist eine Aussageform. Wird die Variable x mit einer beliebigen Person belegt, so erhalten wir eine Aussage (einen eindeutigen Wahrheitswert).

(iii) Es sei $A(x)$ die Aussageform 'Person x hat in der Klausur volle Punktzahl erzielt' und $B(x)$ die Aussageform 'Person x hat das Modul bestanden'. Dann ist auch $A(x) \to B(x)$ eine Aussageform.

Für jede Belegung der Variable x mit einer Person ist $A(x) \to B(x)$ eine wahre Aussage. Es gilt also $A(x) \Rightarrow B(x)$. Das liegt daran, dass der Fall $A(x)$ wahr und $B(x)$ falsch (der einzige Fall in dem $A(x) \to B(x)$ falsch ist) nicht vorkommt.

(iv) Es sei $A(t)$ die Aussageform 'Der Projektor im Hörsaal ist zum Zeitpunkt t aus' und $B(t)$ die Aussageform 'Der Hörsaal ist zum Zeitpunkt t leer'.

Für jede Belegung der Variable t mit einem Zeitpunkt ist $A(t) \to B(t)$ eine Aussage. Deren Wahrheitswert hängt allerdings von t ab. Wann ist sie falsch?

Bemerkung. Wenn $A(x) \to B(x)$ unabhängig von x stets wahr ist (wie in Beispiel (iii)), gilt also $A(x) \Rightarrow B(x)$, dann drückt dies offensichtlich einen kausalen Zusammenhang aus.

1.1.5 Sprachliche Konventionen

Wir einigen uns auf folgende Konventionen

(i) Wir sagen: „Die Aussage A *gilt*“, falls A den Wahrheitswert 1 hat (also wahr ist).

(ii) $A := B$ bedeutet: Das Symbol A wird durch das Symbol B definiert.

(iii) $A :\Leftrightarrow B$ bedeutet: Die Aussage A wird durch die Aussage B definiert (A hat per Definition den gleichen Wahrheitswert wie B).

(iv) *Ein* bedeutet stets „mindestens ein“ und ist von „genau ein“ zu unterscheiden.

(v) In einer Aufzählung von Objekten $x_1, \ldots, x_n$ heißen $x_1, \ldots, x_n$ *paarweise verschieden*, wenn keine zwei Objekte der Aufzählung gleich sind (d.h. wenn in der Aufzählung keine Wiederholungen vorkommen). Davon zu unterscheiden ist „verschieden“ im Sinne von „nicht alle gleich“. Wenn wir von „n verschiedenen Objekten $x_1, \ldots, x_n$“ sprechen, impliziert das, dass $x_1, \ldots, x_n$ paarweise verschieden sind.

1.2 Mengen

1.2.1 Definition und Beispiele

> "Unter einer *Menge* verstehen wir jede Zusammenfassung M von bestimmten wohlunterscheidbaren Objekten unserer Anschauung oder unseres Denkens [welche die *Elemente* von M genannt werden] zu einem Ganzen."
>
> Georg Cantor, 1895

Bei der Auslegung von Cantor's Begriff einer „Zusammenfassung" ist allerdings Vorsicht geboten. Das wusste schon Cantor selbst und zeigte, dass die Betrachtung der „Menge aller Mengen" zu einem Widerspruch führt: nach der *Zweiten Cantor'schen Antinomie* wäre sie „größer" als sie selbst. Man kann auch ohne Betrachtung der „Größe" einer Menge einen rein logischen Widerspruch aus der „Menge aller Mengen" ableiten, die *Russel'sche Antinomie* (siehe Übung b unten). Wir einigen uns auf die folgende Definition des Mengenbegriffs.

Definition a. Eine *Menge* M ist etwas, zu dem jedes beliebige Objekt x entweder *Element* der Menge ist, geschrieben $x \in M$, oder nicht, geschrieben $x \notin M$.

Mengen sind also gerade dadurch gekennzeichnet, dass '$x \in M$' für jedes Objekt x eine Aussage ist (einen eindeutigen Wahrheitswert hat), also gerade dadurch, dass '$x \in M$' eine Aussageform ist. Umgekehrt ist für jede Aussageform $A(x)$ die Zusammenfassung aller x, für die $A(x)$ wahr ist, eine Menge (vgl. Schreibweise (iii) unten).

Bemerkung a. Mengen, die sich selbst enthalten führen nicht per se zu einem Widerspruch. In der weit verbreitetsten Mengenlehre (der *Zermelo-Fraenkel-Mengenlehre*), der wir uns anschließen wollen, sind Mengen, die sich selbst als Elemente enthalten, allerdings nicht erlaubt.

Definition b. Sind M, N zwei Mengen, so heißt N eine *Teilmenge* von M und M eine *Obermenge* von N, geschrieben $N \subseteq M$, wenn für alle $x \in N$ gilt: $x \in M$. Das Zeichen $\subseteq$ bzw. die Aussage $N \subseteq M$ heißt *Inklusion*.

Zwei Mengen M und N heißen *gleich*, geschrieben $M = N$, wenn $M \subseteq N$ und $N \subseteq M$.

Eine Menge M heißt *endlich*, wenn M nur endlich viele Elemente besitzt. Man schreibt in diesem Fall $|M|$ für die Anzahl der Elemente von M. Anderenfalls heißt M *unendlich* und man schreibt $|M| = \infty$.

Schreibweise. Es folgen die gebräuchlichsten Methoden, Mengen zu beschreiben.

(i) *Aufzählen.* Die Elemente werden aufgelistet und mit Mengenklammern eingeschlossen. Reihenfolge und Wiederholungen spielen bei der Mengenaufzählung keine Rolle, z.B.

$$\{1, 3, 17\} = \{3, 1, 17\} = \{1, 3, 17, 1, 3\}.$$

(ii) *Beschreiben.* Mengen können durch Worte beschrieben werden, etwa:

$$\begin{aligned}&\text{Menge der natürlichen Zahlen} = \{1, 2, 3, 4, 5, \ldots\}\\ &\text{Menge der ganzen Zahlen} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}\end{aligned}$$

(iii) *Aussondern.* Es sei M eine Menge. Ist $A(x)$ eine Aussageform, so bezeichnet

$$\{x \in M \mid A(x)\}$$

diejenige Teilmenge von M, die aus allen Elementen besteht, für die $A(x)$ wahr ist (gesprochen „Menge aller x aus M mit $A(x)$“). Benennen wir beispielsweise die Menge der natürlichen Zahlen mit $\mathbb{N}$, so ist $\{n \in \mathbb{N} \mid n \text{ ist ungerade}\}$ die Menge der ungeraden natürlichen Zahlen, also $\{1, 3, 5, 7, \ldots\}$.

(iv) *Abbilden.* Seien M und N Mengen und $e(x)$ für jedes $x \in M$ ein Element aus N. (Wir greifen hier dem Begriff der *Abbildung* vor.) Dann ist

$$\{e(x) \mid x \in M\}$$

eine Teilmenge von N (insbesondere eine Menge), die Menge aller Elemente der Form $e(x)$ von N, wobei x alle Elemente aus M durchläuft. Ist z.B. $\mathbb{N}$ die Menge der natürlichen Zahlen, dann ist $\{n^2 \mid n \in \mathbb{N}\}$ die Menge der Quadratzahlen (hier ist $M = N = \mathbb{N}$). Ist $\mathbb{R}$ die Menge der rellen Zahlen, dann ist $\{|x| \mid x \in \mathbb{R}\}$ die Menge der nicht-negativen rellen Zahlen. Abbilden und Aussondern können kombiniert werden, sodass z.B. $\{n^2 \mid n \in \mathbb{N}, n \text{ ungerade}\}$ die Menge aller Quadrate von ungeraden natürlichen Zahlen bezeichnet, also $\{1, 9, 25, 49, \ldots\}$.

Bemerkung b. In der Regel schreibt man die Menge $\{n^2 \mid n \in \mathbb{N}, n \text{ ungerade}\}$ auch kurz und intuitiv als $\{n^2 \mid n \in \mathbb{N} \text{ ungerade}\}$, ohne sich Gedanken über Abbilden und Aussondern zu machen. Man muss beide Schreibweisen aber penibel trennen, wenn man die Menge beispielsweise in ein Computeralgebra-System eingeben möchte.

Beispiel. Häufig auftretende Mengen sind:

Symbol	Beschreibung	Definition
$\emptyset$	leere Menge	$\{\}$
$\mathbb{N}$	natürliche Zahlen	$\{1, 2, 3, \ldots\}$
$\mathbb{N}_0$	natürliche Zahlen einschl. 0	$\{0, 1, 2, 3, \ldots\}$
$\underline{n}$	n-elementige Menge, $n \in \mathbb{N}_0$	$\{1, 2, \ldots, n\}$, $\underline{0} := \emptyset$
$\mathbb{P}$	Primzahlen	$\{2, 3, 5, 7, 11, 13, \ldots\}$
$\mathbb{Z}$	ganze Zahlen	$\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$\mathbb{Q}$	rationale Zahlen	$\{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}\}$
$\mathbb{R}$	reelle Zahlen	$\{a_1 a_2 \ldots a_r, b_1 b_2 \ldots : a_i, b_i \in \{0, 1, \ldots, 9\}\}$
$\mathbb{R}_{>0}$	positive reelle Zahlen	$\{x \in \mathbb{R} \mid x > 0\}$
$\mathbb{R}_{\geq 0}$	nicht-negative reelle Zahlen	$\{x \in \mathbb{R} \mid x \geq 0\}$
$\mathbb{C}$	komplexe Zahlen	$\{a + bi : a, b \in \mathbb{R}\}$

Nur die erste und vierte der Mengen der Tabelle sind endlich, nämlich $|\emptyset| = 0$ und $|\underline{n}| = n$ für alle $n \in \mathbb{N}_0$. Es gilt:

$$\emptyset = \underline{0} \subseteq \underline{1} \subseteq \underline{2} \subseteq \ldots \subseteq \mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

Übung a. Was gilt für eine Menge M:

(i) $x \in M$ xor $x \notin M$ für alle x?

(ii) $x \in M \Leftrightarrow \neg(x \notin M)$?

(iii) $\neg(x \in M) \Leftrightarrow x \notin M$?

Übung b (Russel's Antinomie). Die „Menge aller Mengen" würde als Teilmenge enthalten die „Menge" $\mathcal{M}$ aller Mengen, die sich nicht selbst als Element enthalten. Ist dann $\mathcal{M} \in \mathcal{M}$ oder $\mathcal{M} \notin \mathcal{M}$?

1.2.2 Quantifizierte Aussagen

Es sei $A(x)$ eine Aussageform. Nach Definition (1.1.4) ist $A(x)$ für jedes x eine Aussage. Setzt man in $A(x)$ für x in ein konkretes Objekt ein, so sagt man, x wird *spezifiziert*. Zwei weitere Möglichkeiten, aus $A(x)$ eine Aussage zu machen, bestehen darin, x zu *quantifizieren*:

'Für alle $x \in M$ gilt $A(x)$' und 'Es gibt ein $x \in M$, für das $A(x)$ gilt'.

Hierbei ist M eine Menge. Diese sprachlichen Ausdrücke sind Aussagen, denn x ist keine (freie) Variable mehr!

Beispiel.

(i) Sei $A(x)$ die Aussageform '$x > 5$'. Dann ist 'Es existiert ein $x \in \mathbb{N}$ mit $A(x)$' wahr, weil z.B. $A(7)$ wahr ist. Dagegen ist 'Für alle $x \in \mathbb{N}$ gilt $A(x)$' falsch, weil z.B. $A(2)$ falsch ist.

(ii) Sei $A(t)$ die Aussageform 'Zum Zeitpunkt t gilt: Projektor ist aus $\rightarrow$ Hörsaal ist leer'. Ist t ein konkreter Zeitpunkt, an dem der Projektor an ist oder der Hörsaal leer, so ist die Aussage $A(t)$ wahr. Da es solche Zeitpunkte gibt, ist 'Es gibt eine Zeit t mit $A(t)$' wahr. Ist t dagegen ein konkreter Zeitpunkt, an dem der Projektor aus ist und der Hörsaal nicht leer, so ist die Aussage $A(t)$ falsch. Da es auch solche Zeitpunkte gibt, ist auch 'Es gibt eine Zeit t mit $\neg A(t)$' wahr und 'Für alle Zeiten t gilt $A(t)$' falsch.

(iii) Die Verneinung von 'Für alle $x \in M$ gilt $A(x)$' lässt sich als 'Es existiert $x \in M$ mit $\neg A(x)$' bzw. 'Es existiert $x \in M$ für das $A(x)$ nicht gilt' formulieren. Die Verneinung von 'Für alle $x \in \mathbb{R}$ gilt $x^2 > 0$' lässt sich als 'Es existiert ein $x \in \mathbb{R}$ mit $x^2 \leq 0$' formulieren.

(iv) Die Verneinung von 'Es existiert ein $x \in M$ mit $A(x)$' lässt sich als 'Für alle $x \in M$ gilt $\neg A(x)$' formulieren. Die Verneinung von 'Es gibt eine Person im Hörsaal, die ihr Handy aus hat' lässt sich als 'Alle Personen im Hörsaal haben ihr Handy an' formulieren.

Bemerkung. Gelegentlich schreibt man (missbräuchlich) nur eine Aussageform $A(x)$ auf, meint damit aber die Aussage 'Für alle $x \in M$ gilt $A(x)$'. Das geht nur, wenn die Menge M aus dem Zusammenhang klar ist.

Übung. Wie lautet der Wahrheitswert der Aussagen 'Für alle $x \in \emptyset$ gilt $A(x)$' und 'Es gibt $x \in \emptyset$ mit $A(x)$'?

1.2.3 Konstruktion von Mengen

Definition (Mengenoperationen)**.** Es seien M, N beliebige Mengen.

(i) $M \cap N := \{x \in M \mid x \in N\}$ heißt *Durchschnitt* von M und N.

(ii) $M \cup N := \{x \mid x \in M \text{ oder } x \in N\}$ heißt *Vereinigung* von M und N.

(iii) $M \backslash N := \{x \in M \mid x \notin N\}$ heißt die *Differenzmenge*, gesprochen „M ohne N".

(iv) $M \times N := \{(x, y) \mid x \in M \text{ und } y \in N\}$ heißt *kartesisches Produkt* von M und N.
Hierbei ist (x, y) ein *geordnetes Paar*. Zwei geordnete Paare (x, y) und (x', y') sind genau dann gleich, wenn $x = x'$ und $y = y'$.

(v) $\mathrm{Pot}(M) := \{S \mid S \subseteq M\}$ heißt die *Potenzmenge* von M.

Beispiel.

(i) Die leere Menge ist Teilmenge jeder beliebigen Menge (auch von sich selbst).

(ii) Es gilt:

$$\begin{aligned} \mathrm{Pot}(\emptyset) &= \{\emptyset\}, \\ \mathrm{Pot}(\{1\}) &= \{\emptyset, \{1\}\}, \\ \mathrm{Pot}(\{1,2\}) &= \{\emptyset, \{1\}, \{2\}, \{1,2\}\}, \\ &\vdots \end{aligned}$$

(iii) Für Mengen M und N gilt:

- $M \cap N = N \Leftrightarrow N \subseteq M$.
- $M \cup N = N \Leftrightarrow M \subseteq N$.

Bemerkung. Für Mengen L, M, N gelten folgende Rechenregeln.

(i)
- $L \cap (M \cap N) = (L \cap M) \cap N$
- $L \cup (M \cup N) = (L \cup M) \cup N$

(ii)
- $L \cap M = M \cap L$
- $L \cup M = M \cup L$

(iii)
- $L \cap L = L$
- $L \cup L = L$

(iv)
- $L \cap (M \cup N) = (L \cap M) \cup (L \cap N)$
- $L \cup (M \cap N) = (L \cup M) \cap (L \cup N)$

(v)
- $L \cap (L \cup M) = L$
- $L \cup (L \cap M) = L$

Übung.

(i) Wie viele Elemente hat $\mathrm{Pot}(\underline{n})$ für $n \in \mathbb{N}_0$?

1.2.4 Indexmengen

Definition a. Es sei $n \in \mathbb{N}$. Für Zahlen $a_1, \ldots, a_n$, Mengen $M_1, \ldots, M_n$ und Aussagen $A_1, \ldots, A_n$ definieren wir:

(i) $\sum_{i=1}^{n} a_i := a_1 + \ldots + a_n$

(ii) $\prod_{i=1}^{n} a_i := a_1 \cdot \ldots \cdot a_n$

(iii) $\bigcup_{i=1}^{n} M_i := M_1 \cup \ldots \cup M_n$

(iv) $\bigcap_{i=1}^{n} M_i := M_1 \cap \ldots \cap M_n$

(v) $\bigvee_{i=1}^{n} A_i := A_1 \vee \ldots \vee A_n$

(vi) $\bigwedge_{i=1}^{n} A_i := A_1 \wedge \ldots \wedge A_n$

Diese *Aufzählschreibweisen* können teilweise auf beliebige *Indexmengen* I verallgemeinert werden, die auch unendlich sein dürfen:

Definition b. Für jedes $i \in I$ sei M_i eine Menge.

(i) Wir definieren $\bigcup_{i \in I} M_i$ durch

$$x \in \bigcup_{i \in I} M_i :\Leftrightarrow \text{ es gibt } i \in I \text{ mit } x \in M_i$$

(ii) Wir definieren $\bigcap_{i \in I} M_i$ durch

$$x \in \bigcap_{i \in I} M_i :\Leftrightarrow \text{ für alle } i \in I \text{ gilt } x \in M_i$$

Es ist auch sinnvoll, den Begriff „paarweise verschieden“ für beliebig indizierte Objekte auszudehnen:

Definition c. Für jedes $i \in I$ sei x_i ein Objekt. Die Objekte $x_i, i \in I$, heißen *paarweise verschieden*, wenn für alle $i, j \in I$ gilt: $x_i = x_j \Rightarrow i = j$.

Beispiel. (i) Die Zahlen $n^2, n \in \mathbb{N}$, sind paarweise verschieden.

(ii) Die Zahlen $n^2, n \in \mathbb{Z}$, sind nicht paarweise verschieden.

1.2.5 Mengenpartitionen

Definition.

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

(ii) Mengen $M_i, i \in I$, heißen *paarweise disjunkt*, wenn für alle $i, j \in I$ mit $i \neq j$ gilt: $M_i \cap M_j = \emptyset$.

(iii) Es sei $\mathcal{M}$ eine Menge von Mengen ($\mathcal{M}$ darf hier unendlich sein). Die Elemente von $\mathcal{M}$ heißen *paarweise disjunkt*, wenn je zwei davon disjunkt sind, d.h. wenn für alle $M, M' \in \mathcal{M}$ mit $M \neq M'$ gilt: $M \cap M' = \emptyset$.

(iv) Es sei M eine Menge. Eine *Partition* von M ist eine Menge $\mathcal{P}$ nichtleerer, paarweise disjunkter Teilmengen von M mit $M = \bigcup_{C \in \mathcal{P}} C$. Die Elemente $C \in \mathcal{P}$ heißen *Teile* der Partition.

Bemerkung. Für jede Partition $\mathcal{P}$ von M ist $\mathcal{P} \subseteq \mathrm{Pot}(M) \setminus \{\emptyset\}$.

Beispiel.

(i) $\mathcal{P} = \{\{n \in \mathbb{N} \mid n \text{ gerade}\}, \{n \in \mathbb{N} \mid n \text{ ungerade}\}\}$ stellt eine Partition von $\mathbb{N}$ mit zwei Teilen dar.

(ii) $\mathcal{P} = \{\{n \in \mathbb{N} \mid n \text{ hat } k \text{ Dezimalstellen}\} \mid k \in \mathbb{N}\}$ stellt eine Partition von $\mathbb{N}$ mit unendlich vielen Teilen dar.

(iii) Die einzige Partition von $\emptyset$ ist $\mathcal{P} = \emptyset$.

Übung. Man mache sich klar:

(i) Sind M, N endliche, disjunkte Mengen, so gilt $|M \cup N| = |M| + |N|$.

(ii) Sind $M_1, \ldots, M_n$ endliche, paarweise disjunkte Mengen, so gilt

$$|\bigcup_{i=1}^{n} M_i| = \sum_{i=1}^{n} |M_i|.$$

1.3 Beweisprinzipien

1.3.1 Direkter Beweis

Prinzip. Ziel: $A \Rightarrow B$ (d.h. $A \to B$ ist wahr).

Um das Ziel zu zeigen, nehmen wir an, dass A wahr ist und folgern daraus mittels logischer Schlüsse, dass B wahr ist. Wenn das gelungen ist, ist $A \Rightarrow B$ bewiesen.

Beispiel. Für alle $n \in \mathbb{N}$ gilt: n ungerade $\Rightarrow n^2$ ungerade.

Beweis. Sei $n \in \mathbb{N}$ beliebig, sei A die Aussage 'n ist ungerade' und B die Aussage 'n^2 ist ungerade'. Wir nehmen an, A ist wahr, d.h. n ist ungerade. Wir folgern, dass B wahr ist: Da n ungerade ist, existiert ein $k \in \mathbb{N}$ mit $n = 2k - 1$. Dann ist $n^2 = (2k-1)^2 = 4k^2 - 4k + 1 = 2(2k^2 - 2k) + 1$, eine ungerade Zahl. Damit ist gefolgert, dass B wahr ist. Nach dem Beweisprinzip des direkten Beweises ist also $A \Rightarrow B$ wahr. Da $n \in \mathbb{N}$ beliebig gewählt war, gilt dies für alle $n \in \mathbb{N}$. □

Übung. Was passiert, wenn sich aus A ein Widerspruch folgern lässt, A also falsch ist?

1.3.2 Beweis durch Kontraposition

Prinzip. Ziel: $A \Rightarrow B$.

Stattdessen zeigen wir, $\neg B \Rightarrow \neg A$. Wenn das gelungen ist, ist $A \Rightarrow B$ bewiesen.

Beweis des Prinzips. Dieses Prinzip beruht auf der bekannten Tautologie $(A \to B) \Leftrightarrow (\neg B \to \neg A)$ aus Beispiel (1.1.3). □

Beispiel. Für alle $n \in \mathbb{N}$ gilt: n^2 gerade $\Rightarrow n$ gerade.

Beweis. Sei $n \in \mathbb{N}$ beliebig, sei A die Aussage 'n^2 ist gerade' und B die Aussage 'n ist gerade'. Wir zeigen $\neg B \Rightarrow \neg A$: Dies ist gleichbedeutend mit 'n ist ungerade $\Rightarrow n^2$ ist ungerade' und wurde schon in (1.3.1) gezeigt. Damit gilt nach dem Beweisprinzip der Kontraposition auch $A \Rightarrow B$. Da $n \in \mathbb{N}$ beliebig gewählt war, gilt dies für alle $n \in \mathbb{N}$. □

1.3.3 Beweis durch Widerspruch

Prinzip. Ziel: A ist wahr.

Wir zeigen, dass $\neg A \Rightarrow (B \wedge \neg B)$ gilt. Wenn das gelungen ist, ist auch A wahr. ($B \wedge \neg B$ ist hier der Widerspruch und die Aussage B kann frei gewählt werden.)

Beweis des Prinzips. $B \wedge \neg B$ ist stets falsch (vgl. Übung 1.1.3). Wenn $\neg A \Rightarrow (B \wedge \neg B)$ gilt, ist also $\neg A \to (B \wedge \neg B)$ wahr. Das kann nur der Fall sein, wenn $\neg A$ falsch ist (vgl. Definition von $\to$), d.h. A wahr ist. □

Beispiel. Es sei A die Aussage $\sqrt{2} \notin \mathbb{Q}$.

Beweis. Wir nehmen an, $\neg A$ ist wahr, d.h. $\sqrt{2} \in \mathbb{Q}$. Dann gibt es $n, m \in \mathbb{N}$, die nicht beide gerade sind und $\sqrt{2} = m/n$ erfüllen ($\sqrt{2}$ wird als Bruch geschrieben und dieser gekürzt). Seien solche n, m gewählt. Durch Quadrieren folgt $2n^2 = m^2$, d.h. m^2 ist gerade. Also ist m gerade nach Beispiel (1.3.2). Sei $k \in \mathbb{N}$ mit $m = 2k$. Dann gilt $2n^2 = m^2 = 4k^2$, also $n^2 = 2k^2$, d.h. n^2 ist gerade. Also ist n gerade nach Beispiel (1.3.2). Insgesamt wurde gezeigt, dass sowohl n als auch m gerade sind. Das ist ein Widerspruch (die Aussage B kann hier 'n und m sind nicht beide gerade' gewählt werden). Also ist die Annahme $\sqrt{2} \in \mathbb{Q}$ falsch, und damit ist die Behauptung $\sqrt{2} \notin \mathbb{Q}$ wahr. □

1.3.4 Vollständige Induktion

Prinzip. Ziel: Für alle $n \in \mathbb{N}$ gilt $A(n)$.
Wir zeigen als *Induktionsanfang*, dass $A(1)$ wahr ist, und als *Induktionsschritt* die Implikation $A(n) \Rightarrow A(n+1)$ für alle $n \in \mathbb{N}$. Dann ist $A(n)$ für alle $n \in \mathbb{N}$ wahr. Man spricht präziser von einer vollständigen Induktion *über* n. Im Induktionsschritt nennt man die Aussage $A(n)$ die *Induktionsvoraussetzung*.

Beweis des Prinzips. Das Prinzip beruht auf der folgenden Eigenschaft von $\mathbb{N}$, die wir als gegeben annehmen:

> Für jede Teilmenge $A \subseteq \mathbb{N}$ gilt: Ist $1 \in A$ und ist für jedes $n \in A$ auch $n + 1 \in A$, dann ist $A = \mathbb{N}$.

Bei der vollständigen Induktion zeigen wir gerade, dass die Menge $A := \{n \in \mathbb{N} \mid A(n) \text{ ist wahr}\}$ diese Bedingung erfüllt, also gleich $\mathbb{N}$ ist. □

Bemerkung. Eine alternative Möglichkeit, die Aussage 'Für alle $n \in \mathbb{N}$ gilt $A(n)$' zu zeigen, wäre, ein *beliebiges* $n \in \mathbb{N}$ zu wählen und dann $A(n)$ mit einem der Prinzipien (1.3.1)–(1.3.3) zu beweisen. (Genau so wurde in Beispiel (1.3.1) und (1.3.2) vorgegangen.) Da vollständige Induktion nur für $\mathbb{N}$ möglich ist, ist diese Alternative sogar der einzige Weg, um Aussagen 'Für alle $x \in M$ gilt $A(x)$' zu zeigen, bei denen die Menge M „größer" als $\mathbb{N}$ ist.

Beispiel. Für alle $n \in \mathbb{N}$ gilt $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Beweis. Wir führen eine vollständige Induktion über n. Sei also $A(n)$ die Aussageform $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Induktionsanfang: Es ist $\sum_{i=1}^{1} i = 1 = \frac{1 \cdot 2}{2}$, d.h. $A(1)$ ist wahr.

Induktionsschritt: Sei jetzt $n \in \mathbb{N}$ beliebig. Wir zeigen $A(n) \Rightarrow A(n+1)$ mittels eines direkten Beweises. Wir nehmen an, dass $A(n)$ wahr ist, d.h.

dass $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ gilt. Dieses ist die Induktionsvoraussetzung (kurz IV). Dann ist

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

Der Induktionsschritt ist damit erledigt, weil dies genau die Aussage $A(n+1)$ ist. □

Bemerkung. Es gibt verschiedene Varianten der Induktion, z.B.

(i) Der Induktionsanfang kann bei $n_0 \in \mathbb{N}$ statt bei 1 gemacht werden. Damit wird die Aussage $A(n)$ für alle $n \geq n_0$ gezeigt.

(ii) Als Induktionsvoraussetzung kann $A(1) \wedge \ldots \wedge A(n)$ anstelle von $A(n)$ verwendet werden, was unter Umständen stärker ist.

(iii) Es gibt die vollständige Induktion nicht nur für $\mathbb{N}$ sondern auch eine sog. *strukturelle Induktion*, die z.B. über einen „Termaufbau“ geführt werden kann. Dies spielt in der Logik und bei formalen Sprachen eine Rolle.

(iv) In der Informatik beweist man die Korrektheit von Algorithmen häufig mit sog. *Schleifeninvarianten*. Im Prinzip beweist man damit die Korrektheit des Algorithmus durch Induktion über die Anzahl der Schleifendurchläufe, und die Schleifeninvariante hat die Rolle der Induktionsvoraussetzung.

Übung. Man zeige mittels vollständiger Induktion, dass sich eine Tafel Schokolade mit n Stücken stets durch $(n-1)$-maliges Durchbrechen in Einzelstücke zerlegen lässt. Hier wird vorausgesetzt, dass einmaliges Durchbrechen ein einzelnes Stück in genau zwei Teile zerlegt. Hinweis: Verwenden Sie als Induktionsvoraussetzung $A(1) \wedge \ldots \wedge A(n)$.

1.4 Abbildungen

1.4.1 Definition und Beispiele

Definition a. Seien M, N Mengen. Eine *Abbildung f von M nach N* ist eine „Vorschrift“ (z.B. eine Formel), die jedem $x \in M$ genau ein Element $f(x) \in N$ zuordnet, geschrieben

$$f : M \to N, \quad x \mapsto f(x).$$

Es heißen: M der *Definitionsbereich* von f, N der *Zielbereich* oder *Wertebereich* von f, $f(x)$ das *Bild* von x unter f, x ein *Urbild* von $f(x)$ unter f.

Zur Angabe einer Abbildung gehört die Angabe von Definitions- und Zielbereich dazu, d.h. zwei Abbildungen $f : M \to N$ und $g : M' \to N'$ sind nur dann gleich, wenn $M = M', N = N'$ und $f(x) = g(x)$ für alle $x \in M$.

Die Menge aller Abbildungen von M nach N wird mit $\mathrm{Abb}(M, N)$ oder mit N^M bezeichnet.

Beispiel a.

(i) $f : \mathbb{N} \to \mathbb{R}, i \mapsto i^2$.

(ii) Es sei M eine Menge von Glasperlen , und sei F die Menge aller Farben. Dann gibt es die Abbildung $f : M \to F, x \mapsto$ Farbe von x.

(iii) Für jede Menge A von Personen gibt es die Abbildung $J : A \to \mathbb{Z}, p \mapsto$ Geburtsjahr von p.

(iv) Die Addition in $\mathbb{Z}$ kann als die Abbildung

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (x, y) \mapsto x + y$$

aufgefasst werden.

(v) Für jede Menge M gibt es die *Identitätsabbildung*

$$\mathrm{id}_M : M \to M, x \mapsto x.$$

(vi) Betrachten wir die Abbildungen

$$\begin{aligned} f &: \mathbb{R} \to \mathbb{R}, \quad x \mapsto \sqrt{x^2}, \\ g &: \mathbb{R} \to \mathbb{R}, \quad x \mapsto |x|, \\ h &: \mathbb{R} \to \mathbb{R}_{\geq 0}, \quad x \mapsto |x|, \end{aligned}$$

so ist $f = g \neq h$.

(vii) $\mathrm{Abb}(\mathbb{R}, \mathbb{R}) = \{\mathbb{R} \to \mathbb{R}\} =$ Menge aller reellen Funktionen.

(viii) Für jede Menge N existiert genau eine Abbildung $\emptyset \to N$.

(ix) Für jede nicht-leere Menge M existiert keine Abbildung $M \to \emptyset$.

Bemerkung. Eine Abbildung $f : \mathbb{N} \to N$ wird auch *Folge in* N genannt. Oft benutzt man für Folgen die Schreibweise $a_1, a_2, a_3, \ldots$ oder $(a_i)_{i\in\mathbb{N}}$, wobei a_i für das Bild $f(i) \in N$ steht. Die Folge aus Beispiel a.(i) würde also auch geschrieben als $1, 4, 9, 16, \ldots$ oder als $(i^2)_{i\in\mathbb{N}}$.

Die Menge aller Folgen in N wird daher auch als $\mathrm{Abb}(\mathbb{N}, N)$ oder $N^{\mathbb{N}}$ geschrieben. Beispielsweise ist $\{0, 1\}^{\mathbb{N}}$ die Menge der Binärfolgen (manchmal auch geschrieben als $2^{\mathbb{N}}$), $\mathbb{R}^{\mathbb{N}}$ die Menge der reellen Folgen, usw.

Definition b. Es sei M eine Menge und $n \in \mathbb{N}$. Ein n-Tupel über M ist eine Abbildung $t : \underline{n} \to M$. Wie bei Folgen schreiben wir $(x_1, \ldots, x_n)$ oder $(x_i)_{i\in\underline{n}}$ für t, wobei $x_i := t(i)$ ist für $i \in \underline{n}$. Wir setzen $M^n := M^{\underline{n}} = \mathrm{Abb}(\underline{n}, M)$.

Beispiel b. (i) Das 5-Tupel $(1, -3, 0, 0, 27)$ über $\mathbb{Z}$ ist z.B. die Abbildung $t : \underline{5} \to \mathbb{Z}$ mit $t(1) = 1, t(2) = -3, t(3) = t(4) = 0, t(5) = 27$.

(ii) Für jede Menge N kann N^2 mit $N \times N$ identifiziert werden. (Hier wird das 2-**Tupel** $(x, y) \in N^2$, d.i. die Abbildung $\{1, 2\} \to N$, $1 \mapsto x$, $2 \mapsto y$, mit dem **geordneten Paar** $(x, y) \in N \times N$ identifiziert.)

Schließlich können wir mit dem Abbildungsbegriff auch kartesische Produkte von mehr als zwei Mengen definieren.

Definition c. Es sei $n \in \mathbb{N}$ und M_i eine Menge für alle $i \in \underline{n}$. Wir setzen

$$M := \bigcup_{i\in\underline{n}} M_i$$

und definieren

$$M_1 \times \cdots \times M_n := \{f : \underline{n} \to M \mid f(i) \in M_i \text{ für alle } i \in \underline{n}\},$$

und nennen $M_1 \times \cdots \times M_n$ das *kartesische Produkt* der Mengen $M_1, \ldots, M_n$.

Wie bei Folgen schreiben wir $(x_1, \ldots, x_n)$ oder $(x_i)_{i\in\underline{n}}$ für $f \in M_1 \times \cdots \times M_n$, wobei $x_i := f(i)$ ist für $1 \le i \le n$.

Es ist also $M_1 \times \cdots \times M_n$ die Menge aller n-Tupel $(x_1, \ldots, x_n) = (x_i)_{i\in\underline{n}} \in M^n$ mit $x_i \in M_i$ für $i \in \underline{n}$.

Beispiel c. Für jede Menge M und jede natürliche Zahl $n \ge 2$ kann M^n mit dem n-fachen kartesischen Produkt $M \times \cdots \times M$ (mit n Faktoren) identifiziert werden.

Ersetzt man in Definition c die Menge $\underline{n}$ durch eine beliebige Indexmenge I, erhält man das kartesische Produkt über I.

Definition d. (i) Es seien I und M Mengen. Eine Abbildung $f : I \to M$ wird gelegentlich auch mit $(x_i)_{i\in I}$ notiert, wobei $x_i := f(i)$ ist für $i \in I$. In diesem Fall nennen wir $(x_i)_{i\in I}$ eine durch I indizierte *Familie* in M.

(ii) Es sei I eine Menge und M_i eine Menge für alle $i \in I$. Wir setzen

$$M := \bigcup_{i\in \underline{n}} M_i$$

und definieren

$$\prod_{i\in I} M_i := \{f : \underline{n} \to M \mid f(i) \in M_i \text{ für alle } i \in I\},$$

und nennen $\prod_{i\in I} M_i$ das *kartesische Produkt* der Mengen $M_i, i \in I$.

In der oben eingeführten Schreibweise gilt also

$$\prod_{i\in I} M_i := \{(x_i)_{i\in I} \mid x_i \in M_i \text{ für alle } i \in I\}.$$

Übung.

(i) Bestimmen Sie $|\operatorname{Abb}(N, M)|$ für endliche Mengen N und M.

(ii) Wie viele Elemente hat $M_1 \times \cdots \times M_n$ für $n \in \mathbb{N}$ und endliche Mengen $M_1, \ldots, M_n$?

(iii) Wie viele Elemente hat M^n für $n \in \mathbb{N}$ und eine endlichen Menge M?

1.4.2 Definition durch Rekursion

Folgen auf einer Menge können *rekursiv* definiert werden.

Beispiel. (i) Auf $\mathbb{R}_{>0}$ existiert genau eine Folge $(a_n)_{n\in\mathbb{N}}$ mit

$$a_1 := 1 \text{ und } a_{n+1} := 1 + \frac{1}{a_n} \text{ für } n \geq 1.$$

(ii) Es sei $a \in \mathbb{R}$. Es gibt genau eine Folge $x = (x_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ mit

$$x_1 = a \text{ und } x_{n+1} = a \cdot x_n \text{ für } n \geq 1.$$

Wir schreiben: $a^n := x_n$ für das n-te Glied dieser Folge.

Alternativ verwenden wir für dieses Vorgehen oft auch die Sprechweise:

Für $a \in \mathbb{R}$ definieren wir die *Potenzen* a^n für $n \in \mathbb{N}$ *rekursiv* durch:

$$a^1 := a \text{ und } a^{n+1} := a \cdot a^n \text{ für } n \geq 1.$$

Die Definition durch Rekursion beruht auf dem folgenden Satz.

Satz. *Es sei N eine Menge, $f\colon N \to N$ Abbildung und $a \in N$.*
Dann gibt es genau eine Folge $(a_n)_{n\in\mathbb{N}}$ in N mit:

- $a_1 = a$
- $a_{n+1} = f(a_n)$ *für* $n \in \mathbb{N}$.

Dieser *Rekursionssatz von Dedekind* kann durch vollständige Induktion bewiesen werden. Wir verzichten hier auf einen Beweis.

Bemerkung. Wir erhalten die Folgen aus Beispiel 1.4.2 mittels der folgenden Abbildungen.

(i) $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$, $x \mapsto 1 + 1/x$.

(ii) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto ax$.

1.4.3 Bild und Urbild

Definition. Es sei $f : M \to N$ eine Abbildung.

(i) Für jede Teilmenge $X \subseteq M$ heißt $f(X) := \{f(x) \mid x \in X\}$ das *Bild von X* unter f.

(ii) Das Bild $f(M)$ von M unter f wird schlicht das *Bild* von f genannt.

(iii) Für jede Teilmenge $Y \subseteq N$ heißt $f^{-1}(Y) := \{x \in M \mid f(x) \in Y\}$ das *Urbild von Y* unter f.

(iv) Die Mengen $f^{-1}(\{y\})$ mit $y \in N$ heißen die *Fasern von f*.

Die Schreibweise f^{-1} für das Urbild hat im Allgemeinen nichts mit Umkehrabbildungen zu tun.

Beispiel. Die Faser der Abbildung J aus Beispiel (1.4.1)a.(i) zu 2000 ist die Menge aller Personen, die im Jahr 2000 geboren sind.

Bemerkung a. Die nicht-leeren Fasern einer Abbildung bilden eine Partition des Definitionsbereichs.

1.4.4 Injektive und surjektive Abbildungen

Definition. Es sei $f : M \to N$ eine Abbildung.

(i) f heißt *surjektiv*, falls $f(M) = N$.

(ii) f heißt *injektiv*, falls für alle $x, x' \in M$ gilt: $f(x) = f(x') \Rightarrow x = x'$.

(iii) f heißt *bijektiv*, falls f injektiv und surjektiv ist.

Bemerkung a. Eine Abbildung $f : M \to N$ ist per Definition injektiv, surjektiv bzw. bijektiv, wenn jedes Element $y \in N$ höchstens ein, mindestens ein bzw. genau ein Urbild hat. Das ist genau dann der Fall, wenn alle Fasern von f höchstens ein, mindestens ein bzw. genau ein Element besitzen, also genau dann, wenn für jedes $y \in N$ die Gleichung $f(x) = y$ höchstens eine, mindestens eine bzw. genau eine Lösung $x \in M$ hat.

Beispiel.

(i) $f : \mathbb{Z} \to \mathbb{Z}, z \mapsto 2z$ ist injektiv, aber nicht surjektiv.

(ii) $f : \mathbb{R} \to \mathbb{R}, x \mapsto 2x$ ist bijektiv.

(iii) $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ ist weder injektiv noch surjektiv. In der Tat ist $f(\mathbb{R}) = \mathbb{R}_{\geq 0}$, also f nicht surjektiv. Weiter ist z.B. $f(2) = 4 = f(-2)$ aber $2 \neq -2$, folglich ist f nicht injektiv.

(iv) Es sei $f : M \to F$ die Abbildung aus Beispiel (1.4.1)a.(ii). Die Faser $f^{-1}(\{\text{rot}\})$ ist die Menge der roten Perlen in M. Es ist f genau dann injektiv, wenn von jeder Farbe höchstens eine Perle in M vorkommt, wenn also keine zwei Perlen aus M die gleiche Farbe haben. Weiter ist f genau dann surjektiv, wenn von jeder Farbe (mindestens) eine Perle in M vorkommt.

(v) Die Abbildung $\emptyset \to N$ ist injektiv. Sie ist genau dann surjektiv, wenn $N = \emptyset$.

(vi) Hashfunktionen (bzw. „Checksummen“ oder „Fingerprints“), z.B. die bekannte md5 : $\{\text{Texte}\} \to \{0,1\}^{128}$, die einen 128-bit Hashwert produziert, sind nicht injektiv (da verschiedene Texte gleichen Hashwert haben können), sind surjektiv (um alle Hashwerte auszunutzen), und haben „gleich große“ Fasern (das macht gerade eine gute Hashfunktion aus!).

(vii) Verschlüsselungsfunktionen, etwa crypt : $\{0,1\}^k \to \{0,1\}^k$, sind injektiv, damit eine eindeutige Entschlüsselung möglich ist.

Übung. Man mache sich klar, dass eine Abbildung $f : M \to N$ genau dann injektiv ist, wenn für alle $x_1, \ldots, x_r \in M$ gilt:

$$x_1, \ldots, x_r \text{ paarweise verschieden} \Leftrightarrow f(x_1), \ldots, f(x_r) \text{ paarweise verschieden.}$$

1.4.5 Einschränkung

Definition. Es sei $f : M \to N$ eine Abbildung und $M' \subseteq M$. Dann heißt die Abbildung

$$f|_{M'} : M' \to N, \quad x \mapsto f(x)$$

die *Einschränkung* von f auf M'.

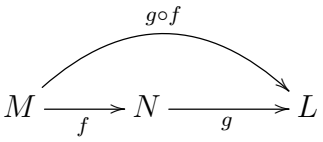
Bemerkung. Jede Abbildung kann durch Einschränkung auf eine geeignete Teilmenge des Definitionsbereichs injektiv gemacht werden. Z.B. ist für f aus Beispiel (1.4.4)(iii) die Einschränkung $f|_{\mathbb{R}_{\geq 0}}$ injektiv, ebenso wie die Einschränkung $f|_{\mathbb{R}_{\leq 0}}$.

1.4.6 Komposition

Definition. Es seien M, N, L Mengen. Weiter seien $f : M \to N$ und $g : N \to L$ zwei Abbildungen. Dann heißt die Abbildung

$$g \circ f : M \to L, \quad x \mapsto (g \circ f)(x) := g(f(x))$$

die *Komposition von g mit f.*



$$x \overset{f}{\longmapsto} f(x) \overset{g}{\longmapsto} g(f(x))$$

Beispiel. Für die Abbildungen

$$f : \mathbb{R} \to \mathbb{R}_{\geq 0}, \quad x \mapsto (x-3)^2,$$
$$g : \mathbb{R}_{\geq 0} \to \mathbb{R}, \quad x \mapsto \sqrt{x}$$

ergeben sich die Kompositionen

$$g \circ f : \mathbb{R} \to \mathbb{R}, x \mapsto \sqrt{(x-3)^2} = |x-3|,$$
$$f \circ g : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, \quad x \mapsto (\sqrt{x}-3)^2$$

Bemerkung. Es seien f, g, h Abbildungen.

(i) Es gilt $(h \circ g) \circ f = h \circ (g \circ f)$, sofern beide Seiten der Gleichung definiert sind. Daher kann die Komposition auch ohne Klammern kurz als $h \circ g \circ f$ geschrieben werden.

1.4.7 Umkehrabbildungen

Definition. Es seien $f : M \to N$ und $g : N \to M$ Abbildungen. Dann heißt g eine *linksseitige (rechtsseitige) Umkehrabbildung von* f, wenn $g \circ f = \mathrm{id}_M$ (wenn $f \circ g = \mathrm{id}_N$). Wir sprechen schlicht von einer *Umkehrabbildung von* f, wenn g sowohl links- als auch rechtsseitige Umkehrabbildung von f ist.

Satz a. *Sei $f : M \to N$ eine Abbildung und sei M nicht leer.*

(i) f besitzt genau dann eine linksseitige Umkehrabbildung, wenn f injektiv ist.

(ii) f besitzt genau dann eine rechtsseitige Umkehrabbildung, wenn f surjektiv ist.

(iii) f besitzt genau dann eine Umkehrabbildung, wenn f bijektiv ist.

Bemerkung. Existiert eine Umkehrabbildung, so ist sie eindeutig bestimmt (Übung). Links- und rechtsseitige Umkehrabbildungen sind im Allgemeinen nicht eindeutig (Beispiel unten).

Schreibweise. Falls f bijektiv ist, so wird die eindeutige Umkehrabbildung mit f^{-1} bezeichnet. Die ist nicht zu verwechseln mit dem Urbild, das ebenfalls mit f^{-1} bezeichnet wird. Was gemeint ist, ergibt sich aus dem Zusammenhang.

Beweis. (i) Es sind zwei Richtungen zu zeigen, wir zeigen zuerst den „wenn“-Teil. Dazu nehmen wir an, f sei injektiv und konstruieren eine linksseitige Umkehrabbildung g. Wähle $x_0 \in M$ beliebig ($M \neq \emptyset$) und definiere $g : N \to M$ durch

$$g(y) := \begin{cases} x & \text{falls } y = f(x) \text{ für ein } x \in M, \\ x_0 & \text{falls } y \notin f(M), \end{cases}$$

Das x in der ersten Zeile ist eindeutig, da f injektiv ist, also ist g wohldefiniert. Damit gilt $(g \circ f)(x) = g(f(x)) = x$ für alle $x \in M$, d.h. $g \circ f = \mathrm{id}_M$ wie gewünscht.

Wir zeigen jetzt die andere Richtung, den „genau dann“-Teil. Dazu nehmen wir an, $g : N \to M$ sei eine linksseitige Umkehrabbildung und folgern, dass f injektiv ist. Aus $g \circ f = \mathrm{id}_M$ folgt, dass für alle $x, x' \in N$ gilt:

$$f(x) = f(x') \Rightarrow g(f(x)) = g(f(x')) \Rightarrow \underbrace{(g \circ f)}_{=\mathrm{id}_N}(x) = \underbrace{(g \circ f)}_{=\mathrm{id}_N}(x') \Rightarrow x = x'.$$

Also ist f tatsächlich injektiv und der Beweis beendet.
(ii), (iii) siehe Vorlesung. □

Beispiel.

(i) $f : \mathbb{R} \to \mathbb{R}, x \mapsto 2x$ ist bijektiv mit der Umkehrabbildung

$$f^{-1} : \mathbb{R} \to \mathbb{R}, \quad x \mapsto \frac{1}{2}x$$

(ii) $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 1}, x \mapsto x^2 + 1$ ist bijektiv mit der Umkehrabbildung

$$f^{-1} : \mathbb{R}_{\geq 1} \to \mathbb{R}_{\geq 0}, \quad x \mapsto \sqrt{x - 1}$$

(iii) $f : \mathbb{Z} \to \mathbb{Q}, a \mapsto a$ ist injektiv, aber nicht surjektiv.

$$\begin{aligned} g \circ f = \mathrm{id}_{\mathbb{Z}} &: \text{z.B. } g(x) := \lfloor x \rfloor \text{ oder } g(x) := \lceil x \rceil \\ f \circ g = \mathrm{id}_{\mathbb{Q}} &: \text{nicht möglich} \end{aligned}$$

(Hier bezeichnet $\lfloor x \rfloor$ die größte ganze Zahl $\leq x$, und $\lceil x \rceil$ die kleinste ganze Zahl $\geq x$.)

(iv) $f : \mathbb{R} \to \mathbb{R}_{\geq 0}, x \mapsto |x|$ ist surjektiv, aber nicht injektiv.

$$\begin{aligned} g \circ f = \mathrm{id}_{\mathbb{R}} &: \text{nicht möglich} \\ f \circ g = \mathrm{id}_{\mathbb{R}_{\geq 0}} &: \text{z.B. } g(x) := x \text{ oder } g(x) := -x \end{aligned}$$

Satz b. *Es seien $f : M \to N$ und $g : N \to L$ zwei bijektive Abbildungen. Wenn $g \circ f$ definiert ist, so ist $g \circ f$ ebenfalls bijektiv und es gilt:*

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

Beweis. als Übung. □

Übung.

(i) Zeigen Sie die restlichen Teile der Bemerkung.

(ii) Zeigen Sie den Satz.

(iii) Gilt der Satz auch, wenn man bijektiv durch injektiv ersetzt?

(iv) Gilt der Satz auch, wenn man bijektiv durch surjektiv ersetzt?

1.4.8 Abbildungen einer Menge in sich

Sind $f, g : M \to M$ zwei Abbildungen einer Menge M in sich, so kann man stets die Kompositionen $f \circ g$ und $g \circ f$ bilden.

Definition. Es sei $f : M \to M$ eine Abbildung und es sei $n \in \mathbb{N}$. Dann setzen wir

$$f^n := \underbrace{f \circ \ldots \circ f}_{n\text{-mal}}, \quad f^0 := \mathrm{id}_M.$$

Falls f bijektiv ist, so definieren wir auch $f^{-n} := (f^{-1})^n$.

Bemerkung.

(i) Es gilt $f^n(x) = f(f(\cdots f(x)))$.

(ii) Für bijektive Abbildungen einer Menge in sich selbst haben wir die üblichen Potenzrechenregeln:

$$f^{a+b} = f^a \circ f^b \quad \text{und} \quad f^{ab} = (f^a)^b \quad \text{für alle } a, b \in \mathbb{Z}.$$

1.4.9 Die Mächtigkeit von Mengen

Definition a. Zwei Mengen M und N heißen *gleichmächtig*, wenn eine bijektive Abbildung $M \to N$ existiert.

Übung a. $\mathbb{N}, \mathbb{Z}$ und $\mathbb{Q}$ sind gleichmächtig.

Satz a (Cantor)**.** *Für jede Menge M sind M und* $\mathrm{Pot}(M)$ *nicht gleichmächtig.*

Beweis. Sei f eine beliebige Abbildung $f : M \to \mathrm{Pot}(M)$. Definiere $A_f := \{x \in M \mid x \notin f(x)\} \in \mathrm{Pot}(M)$. Angenommen, es gibt $m \in M$ mit $f(m) = A_f$. Falls $m \in A_f$, so folgt $m \notin f(m) = A_f$ (Widerspruch). Falls $m \notin A_f = f(m)$, so folgt $m \in A_f$ (Widerspruch). Also ist f nicht surjektiv. □

Übung b. Man folgere aus dem Satz:

(i) $\mathbb{N}$ und $\mathbb{R}$ sind nicht gleichmächtig.

(ii) Die Zusammenfassung aller Mengen ist keine Menge.

Nun können wir eine exakte Definition der Endlichkeit einer Menge geben.

Definition b. Es sei M eine Menge.

(i) M heißt *endlich*, wenn M gleichmächtig zu $\underline{n}$ für ein $n \in \mathbb{N}_0$ ist (Erinnerung: $\underline{0} = \emptyset$).

In diesem Fall definieren wir $|M| := n$, und nennen $|M|$ die *Mächtigkeit* von M (oder die *Anzahl der Elemente* von M).

(ii) M heißt *unendlich*, wenn M nicht endlich ist.

Für Abbildungen zwischen endlichen Mengen gibt es Beziehungen zwischen deren Mächtigkeit.

Bemerkung a. Es seien M, N endliche Mengen und $f : M \to N$ eine Abbildung. Dann gelten $|f(M)| \leq |M|$ und $|f(M)| \leq |N|$.

Übung c. Man folgere aus Bemerkung a, dass für eine injektive Abbildung $f : M \to N$ stets $|M| \leq |N|$ ist, und für eine surjektive Abbildung $f : M \to N$ stets $|M| \geq |N|$ ist.

Genauer kann man bei Abbildungen zwischen endlichen Mengen Injektivität, Surjektivität und Bijektivität wie folgt charakterisieren.

Satz b. *Es sei $f : M \to N$ eine Abbildung und M, N endlich.*

(i) *f injektiv* $\Leftrightarrow |f(M)| = |M|$.

(ii) *f surjektiv* $\Leftrightarrow |f(M)| = |N|$.

(iii) *Ist $|M| = |N|$, dann sind äquivalent:*

- *f injektiv*
- *f surjektiv*
- *f bijektiv*

Darauf beruht das berühmte Dedekind'sche Schubfachprinzip:

Bemerkung b. Werden m Objekte auf n Schubfächer verteilt, und ist $m > n$, dann gibt es ein Schubfach, welches mindestens zwei Objekte enthält.

Dies ist genau die Aussage: Sind M, N endliche Mengen mit $|M| > |N|$, und $f : M \to N$ eine Abbildung, dann ist f nicht injektiv.

Übung. Bestimmen Sie die Anzahl injektiver Abbildungen von $\underline{m}$ nach $\underline{n}$.

Übung. Es sei $f : M \to N$ eine Abbildung zwischen endlichen Mengen. Dann gilt

$$|M| < |N| \Rightarrow f \text{ nicht surjektiv.}$$

1.4.10 Kombinatorische Strukturen als Abbildungen

Tupel, Permutationen, Kombinationen und Multimengen (Definition erst in späterem Kapitel) können mit Abbildungen bestimmter Art identifiziert werden.

Beispiel. Es sei A eine Menge und $k \in \mathbb{N}$.

(i) Eine *k-Permutation* aus A ist eine injektive Abbildung $\underline{k} \to A$. Die Permutation $(a_1, \ldots, a_k)$ entspricht der Abbildung $f : \underline{k} \to A, i \mapsto a_i$.

(ii) Ist $|A| = n \in \mathbb{N}$, so ist eine Permutation aus A eine bijektive Abbildung $\underline{n} \to A$. Die Permutation $(a_1, \ldots, a_n)$ entspricht der Abbildung $f : \underline{n} \to A, i \mapsto a_i$.

(iii) Eine *k-Kombination* aus A ist eine Abbildung $A \to \{0, 1\}$ mit $|f^{-1}(\{1\})| = k$ (die Faser zu 1 hat k Elemente). Die Kombination $M \subseteq A$ entspricht der Abbildung $f : A \to \{0, 1\}$ mit $f(a) = 0$ falls $a \notin M$ und $f(a) = 1$ falls $a \in M$. Die Abbildung f bezeichnet man auch als *charakteristische Funktion* von M.

(iv) Eine *k-Multimenge* ist eine Abbildung $A \to \mathbb{N}_0$ mit $\sum_{a \in A} f(a) = k$. Die Multimenge $M \subseteq A$ entspricht der Abbildung $f : A \to \mathbb{N}_0$, wobei $f(a)$ angibt, wie oft a in M vorkommt. Die Abbildung f wird als *Häufigkeitsfunktion* von M bezeichnet.

Übung. Eine k-elementige Teilmenge M von A kann als k-Kombination oder als k-Multimenge aufgefasst werden. Vergleichen Sie die charakteristische Funktion von M mit der Häufigkeitsfunktion von M.

1.5 Relationen

1.5.1 Definition und Beispiele

Relationen drücken Beziehungen zwischen Elementen von zwei Mengen aus, z.B. wäre „liegt in“ eine Relation zwischen {Städte} und {Länder}. In der Informatik werden Relationen z.B. in relationalen Datenbanken verwendet.

Definition. Es seien M und N zwei Mengen.

(i) Eine Teilmenge $R \subseteq M \times N$ heißt *Relation zwischen M und N*, oder kürzer *Relation auf M* falls $M = N$. Für $(x, y) \in R$ schreiben wir auch xRy und sagen „x steht in Relation zu y bzgl. R“.

(ii) Eine Relation $R \subseteq M \times M$ auf M heißt

(R) *reflexiv*, falls xRx für alle $x \in M$,

(R') *antireflexiv*, falls nicht xRx für alle $x \in M$,

(S) *symmetrisch*, falls $xRy \Rightarrow yRx$ für alle $x, y \in M$,

(A) *antisymmetrisch*, falls $(xRy \wedge yRx) \Rightarrow x = y$ für alle $x, y \in M$,

(T) *transitiv*, falls $(xRy \wedge yRz) \Rightarrow xRz$ für alle $x, y, z \in M$.

(iii) Eine Relation, die (R), (S) und (T) erfüllt, heißt *Äquivalenzrelation*.

(iv) Eine Relation, die (R), (A) und (T) erfüllt, heißt *(partielle) Ordnung*.

(v) Eine Ordnung heißt *Totalordnung*, wenn $xRy \vee yRx$ für alle $x, y \in M$.

Beispiel.

(i) $M = \mathbb{R}$ und $R =$„$\leq$“, d.h. $(x, y) \in R$ genau dann, wenn $x \leq y$.
„$\leq$“ ist reflexiv, antisymmetrisch und transitiv, also eine Ordnung.
„$\leq$“ ist sogar eine Totalordnung.

(ii) $M = \mathbb{R}$ und $R =$„$<$“, d.h. $(x, y) \in R \Leftrightarrow x < y$.
„$<$“ ist antisymmetrisch(!) und transitiv, aber weder reflexiv noch symmetrisch.

(iii) $M = \mathrm{Pot}(N)$ und $R =$„$\subseteq$“.
„$\subseteq$“ ist eine Ordnung. Falls $|N| \geq 2$, so ist „$\subseteq$“ jedoch keine Totalordnung, da z.B. für $\{1\}, \{2\} \in \mathrm{Pot}\,\{1, 2\}$ weder $\{1\} \subseteq \{2\}$ noch $\{2\} \subseteq \{1\}$ gilt.

(iv) $M = \mathbb{Z}$. Die *Teilbarkeitsrelation* „$|$“ ist erklärt durch $x \mid y$ genau dann, wenn ein $z \in \mathbb{Z}$ existiert mit $xz = y$. Sie ist nicht antisymmetrisch, denn $1 \mid -1$ und $-1 \mid 1$ obwohl $1 \neq -1$. Also ist „$|$“ keine Ordnung auf $\mathbb{Z}$.

(v) Die *Teilbarkeitsrelation* „$|$“ ist eine Ordnung auf $\mathbb{N}$, aber keine Totalordnung.

(vi) Auf jeder Menge M stellt die *Gleichheit* „$=$“ eine Äquivalenzrelation dar mit $R = \{(x, x) \mid x \in M\}$.

(vii) Auf einer Menge M von Personen können zwei Relationen V und G erklärt werden durch:

$xVy :\Leftrightarrow x$ ist verwandt mit y,

$xGy :\Leftrightarrow x$ hat das gleiche Geburtsdatum (Tag und Monat) wie y.

Beide sind Äquivalenzrelationen. Ersetzt man „verwandt“ durch „erstgradig verwandt“, so ist V nicht mehr transitiv.

(viii) Jede Abbildung $f : M \to N$ kann als Relation zwischen M und N aufgefasst werden:

$$f = \{(x, f(x)) \mid x \in M\}.$$

Abbildungen sind also eine spezielle Art von Relationen.

(ix) Für jede Abbildung $f : M \to N$ kann man eine Relation R_f auf M erklären durch

$$xR_f y :\Leftrightarrow f(x) = f(y) \text{ (d.h. } x \text{ und } y \text{ liegen in derselben Faser von } f).$$

R_f ist eine Äquivalenzrelation.

(x) $M = \mathbb{Z}$. Die *Paritätsrelation* „$\equiv_2$“, definiert durch

$$x \equiv_2 y :\Leftrightarrow x - y \text{ gerade}$$

ist eine Äquivalenzrelation auf $\mathbb{Z}$.

Übung. Durch welche Datenstruktur würden Sie eine Relation auf einer endlichen Menge in einem Computerprogramm repräsentieren? Wie prüfen Sie anhand dieser Datenstruktur, ob die Relation reflexiv, symmetrisch bzw. antisymmetrisch ist?

Übung. Es seien R eine Relation auf A und $A' \subseteq A$. Dann ist $R' := R \cap (A' \times A')$ eine Relation auf A'. Man mache sich klar, dass jede der Eigenschaften aus Teil (ii) der Definition beim Übergang von R zu R' erhalten bleibt.

Übung. Welche Bedingung muss eine Relation $R \subseteq N \times M$ erfüllen, damit sie im Sinne von Beispiel (ix) als eine Abbildung von N nach M aufgefasst werden kann? Unter welcher Bedingung ist diese Abbildung injektiv, surjektiv bzw. bijektiv? Welche Relation gehört im bijektiven Fall zur Umkehrabbildung?

1.5.2 Äquivalenzrelationen

Definition. Es sei $\sim$ eine Äquivalenzrelation auf M. Für $x \in M$ heißt

$$[x] := [x]_\sim := \{y \in M \mid x \sim y\}$$

die *Äquivalenzklasse von* $\sim$ *zu* x. Die Menge aller Äquivalenzklassen von $\sim$ wird mit $M/_\sim$ bezeichnet.

Bemerkung. Es sei $\sim$ eine Äquivalenzrelation auf M. Dann gilt für alle $x, y \in M$:

(i) $x \in [x]_\sim$,

(ii) $y \in [x]_\sim \Leftrightarrow x \in [y]_\sim$,

(iii) $y \in [x]_\sim \Rightarrow [y]_\sim = [x]_\sim$.

Wegen (iii) bezeichnet man jedes Element einer Äquivalenzklasse als ein *Repräsentant* derselben.

Beweis. als Übung. □

Beispiel.

(i) Für die Gleichheitsrelation auf einer Menge M ist $[x]_= = \{x\}$ und $M/_= = \{\{x\} \mid x \in M\}$.

(ii) Für die Äquivalenzrelationen V und G aus Beispiel (1.5.1)(vii) gilt für jede Person P der Menge:

$$[P]_V = \{\text{Verwandte von } P\},$$
$$[P]_G = \{\text{Personen, die am gleichen Tag Geburtstag feiern wie } P\}.$$

(iii) Es sei $f : N \to M$ eine Abbildung und R_f die Äquivalenzrelation aus Beispiel (1.5.1)(ix). Dann ist

$$[x]_{R_f} = \{x' \in N \mid f(x) = f(x')\} = f^{-1}(\{x\}),$$

für jedes $x \in N$, und $M/_{R_f}$ ist die Menge der nicht-leeren Fasern von f.

(iv) Für die Paritätsrelation aus Beispiel (1.5.1)(x) ist

$$[0]_{\equiv_2} = \{a \in \mathbb{Z} \mid a \text{ gerade}\},$$
$$[1]_{\equiv_2} = \{a \in \mathbb{Z} \mid a \text{ ungerade}\},$$

und $M/_{\equiv_2} = \{[0]_{\equiv_2}, [1]_{\equiv_2}\}$.

Offensichtlich „partitioniert“ eine Äquivalenzrelation die Menge.

Satz. *Es sei M eine Menge.*

(i) Ist $\sim$ eine Äquivalenzrelation auf M, so ist $M/_\sim$ eine Partition von M.

(ii) Ist $\mathcal{P}$ eine Partition von M, so existiert eine Äquivalenzrelation $\sim$ auf M mit $M/_\sim = \mathcal{P}$.

Die Äquivalenzrelationen auf M entsprechen also den Partitionen von M.

Beweis.

(i) Sei $\sim$ eine Äquivalenzrelation auf M und setze $\mathcal{P} := M/_\sim$. Wegen $x \in [x]_\sim$ sind alle Äquivalenzklassen nicht leer und ihre Vereinigung ist ganz M. Es bleibt zu zeigen, dass die Äquivalenzklassen paarweise disjunkt sind (vgl. Definition (1.2.5)(iv)). Betrachte also zwei beliebige Klassen $[x]_\sim, [y]_\sim$ mit $x, y \in M$. Zu zeigen ist:

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

bzw. die Kontraposition

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

Ist aber $z \in [x]_\sim \cap [y]_\sim$, so folgt daraus nach Teil (iii) der Bemerkung $[x]_\sim = [z]_\sim = [y]_\sim$.

(ii) Durch die Vorschrift

$$x \sim y :\Leftrightarrow \ x \text{ und } y \text{ liegen in demselben Teil der Partition}$$

wird eine Äquivalenzrelation definiert. (Man überprüfe das!)
Die Äquivalenzklassen sind offensichtlich genau die Teile von $\mathcal{P}$.

□

1.5.3 Partielle Ordnungen

Es sei $\trianglelefteq$ eine partielle Ordnung auf M.

Definition. Ein Element $m \in M$ heißt *minimal* in M, falls kein $m' \in M$ existiert mit $m' \neq m$ und $m' \trianglelefteq m$. Ein Element $m \in M$ wird ein *Minimum* von M genannt, falls für alle $m' \in M$ gilt: $m \trianglelefteq m'$.

Analog definiert man *maximal* und *Maximum* (Übung).

Bemerkung a. Nach Definition bedeutet

$$\begin{aligned} m \text{ Minimum von } M: &\quad \text{für alle } x \in M \text{ gilt } m \trianglelefteq x. \\ m \text{ minimal in } M: &\quad \text{für alle } x \in M \text{ gilt } x \trianglelefteq m \Rightarrow x = m. \end{aligned}$$

Minimal zu sein ist also zu verstehen als „kein anderes ist kleiner“. Minimum zu sein ist also zu verstehen als „alle anderen sind größer“.

Beispiel. Wir betrachten die Teilbarkeitsrelation „|“ auf $\mathbb{N}$. Minimal zu sein bzgl. „|“ bedeutet „kein anderes ist Teiler“. Minimum zu sein bzgl. „|“ bedeutet „alle anderen sind Vielfache“.

(i) Die Menge $\{2, 3, 4, 6\}$ besitzt kein Minimum, hat aber die minimalen Elemente 2 und 3.

(ii) Die Menge $\{2, 3, 5\}$ besitzt kein Minimum, und jedes Element ist minimal.

(iii) Die Menge $\{2, 4, 6\}$ besitzt das Minimum 2, und 2 ist das einzige minimale Element.

Satz. *Es sei $\trianglelefteq$ eine partielle Ordnung auf M.*

(i) Jedes Minimum von M ist minimal in M.

(ii) Existiert ein Minimum von M, so ist es das einzige minimale Element in M. Insbesondere ist das Minimum eindeutig.

(iii) Bei einer Totalordnung ist jedes minimale Element in M auch Minimum von M (die Begriffe minimal und Minimum sind bei Totalordnungen also identisch).

Beweis. (i) Ist m ein Minimum und $x \trianglelefteq m$, so folgt $x = m$ wegen der Antisymmetrie ($m \trianglelefteq x \wedge x \trianglelefteq m \Rightarrow x = m$).

(ii) Sei m ein Minimum und sei m' minimal. Da m Minimum ist, gilt $m \trianglelefteq m'$. Da m' minimal ist, folgt daraus $m = m'$.

(iii) Sei $\trianglelefteq$ eine Totalordnung auf M und sei $m \in M$ minimal. Zu zeigen ist $m \trianglelefteq x$ für alle $x \in M$. Sei also $x \in M$ beliebig. Bei einer Totalordnung ist $m \trianglelefteq x$ oder $x \trianglelefteq m$. Im ersten Fall sind wir fertig. Im zweiten Fall folgt $x = m$, da m minimal ist, also $x \trianglelefteq m$ wegen der Reflexivität. □

Bemerkung b. Jede nicht-leere Teilmenge von $\mathbb{N}$ hat bzgl. der Ordnung $\leq$ ein Minimum. (Ohne Beweis; das ist ein Axiom der Mengenlehre.)

Übung. Jede endliche Menge mit partieller Ordnung hat ein minimales Element.

Übung. Formuliere Definition, Bemerkung a und Satz für *maximal* und *Maximum* aus.

Übung. Wir können die Begriffe minimal und Minimum auch definieren, wenn die Relation keine Ordnung ist. Zeigen Sie am Beispiel der Teilbarkeitsrelation auf $\mathbb{Z}$ (die keine Ordnung ist), dass dann der Satz nicht mehr gilt.

Literaturverzeichnis

[1] M. Aigner. *Diskrete Mathematik.* Vieweg, 2004.

[2] H. Anton. *Lineare Algebra.* Spektrum, 1995.

[3] A. Beutelspacher. *Lineare Algebra.* Vieweg, 2003.

[4] G. Fischer. *Lineare Algebra.* Vieweg, 2005.

[5] S. Teschl G. Teschl. *Mathematik für Informatiker, Band 1.* Springer, 2007.

[6] K. Jänich. *Lineare Algebra.* Springer, 2003.

[7] A. Steger. *Diskrete Strukturen.* Springer, 2001.

[8] K. Meyberg und P. Vachenauer. *Höhere Mathematik.* Springer, 2001.