Kapitel 1

Grundlagen

1.1 Logik

„Schule des korrekten, klaren und folgerichtigen Denkens“

Eine Aussage ist ein Satz der Umgangssprache, der entweder wahr (W) oder falsch (F) ist.

Beispiele:

2010 hatte Chemnitz etwa 240000 Einwohner.	W
15 ist eine Primzahl.	F
13 ist eine schöne Zahl.	Keine Aussage (solange schön undefiniert ist).
Dieser Satz ist falsch.	Keine Aussage.

♡

Es gibt Aussagen, für die noch nicht bekannt ist, ob sie W oder F sind.

Beispiel: Es gibt unendlich viele Primzahlzwillinge (Paare $(p, p+2)$ mit p und $p+2$ Primzahl). ♡

Eine Aussageform erhält man, indem Objekte einer Aussage durch Variable/Parameter ersetzt werden. Eine Aussageform wird erst durch Einsetzen von Werten zu einer Aussage.

Beispiel:

x teilt y, $x\|y$	ist eine Aussagform $A(x,y)$, deren Wahrheit von x und y abhängt.
$a^2+b^2=c^2$	ist eine Aussageform $B(a,b,c)$. ♡

Wir schreiben nun nur noch A, B, C für Aussagen und Aussageformen (und lassen meistens die Parameter weg)

<u>Verknüpfungen von Aussagen (und Aussageformen)</u>

Negation	$\neg A$	„nicht A“, „non A“,
Konjunktion	$A \wedge B$	„A und B“, [beide müssen wahr sein]
Disjunktion	$A \vee B$	„A oder B“, [mindestens eine muss wahr sein]
Konditional	$A \to B$	„wenn A, dann B“, „aus A folgt B“, „A impliziert B“,
Bikonditional	$A \leftrightarrow B$	„A genau dann, wenn B“, „A äquivalent zu B“.

$\neg$ und $\wedge$ binden stärker als $\vee$,
diese stärker als $\to$,
diese stärker als $\leftrightarrow$,
aber besser ist es zu klammern.

Die Wahrheit der Verknüpfung ergibt sich aus folgender Wahrheitstabelle:

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \to B$	$A \leftrightarrow B$	$A \wedge \neg A$
W	W	F	W	W	W	W	F
W	F	F	F	W	F	F	F
F	W	W	F	W	W	F	F
F	F	W	F	F	W	W	F

Eine Aussage „aus A folgt B“ ($A \to B$) kann sehr wohl falsch sein.
Beachte aber, dass $A \to B$ immer wahr ist, wenn A falsch ist; jeder Schluss aus einer falschen Voraussetzung ist richtig!
Ab und zu schreibt man statt $A \to B$ auch $B \leftarrow A$, aber man darf es nicht mit $B \to A$ verwechseln.

Eine Aussage, die unabhängig vom Wahrheitswert der Teilaussagen immer wahr ist, heißt Tautologie oder aussagenlogisch wahr.

Beispiel: $\neg(A \wedge \neg A)$, das „Gesetz vom ausgeschlossenen Widerspruch“. ♡

Ü: Zeige folgende Tautologien:

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

Beachte: Eigentlich genügen $\neg$ und $\vee$ (oder $\neg$ und $\wedge$), um alle logischen Verknüpfungen formulieren zu können. ⧖

In Beweisen vewendet man auch gerne folgende Tautologien als Schlusstechniken.

Ü: Zeige folgende Tautologien:

$(A \to B) \leftrightarrow (\neg B \to \neg A)$	Umkehrschluss
$(\neg A \to F) \leftrightarrow A$	Indirekter Beweis
$(A \wedge (A \to B)) \to B$	„Modus (ponendo) ponens“
$((A \to B) \wedge \neg B) \to \neg A$	„Modus (tollendo) tollens“

⧖

Verknüpft man zwei Aussageformen mit Parametern, entsteht daraus eine neue Aussageform, deren Parameter sich aus den Parameterbezeichnungen dieser zwei Aussageformen ergeben.

Beispiel: Seien $A(x, y), B(s, t)$ zwei Aussageformen. Durch $A(c, a) \wedge B(a, b)$ entsteht eine Aussageform $C(a, b, c)$ und durch $A(h, h) \vee B(h, h)$ eine Aussageform $D(h)$. ♡

Quantoren
Will man Aussagen über alle möglichen Einsetzungen eines gegebenen „Diskursuniversums“ treffen, verwendet man dafür den Allquantor, in Zeichen „$\forall$“, „für alle“, etwa für eine Aussageform $A(x)$

$$\forall x\ A(x)$$

Beispiel: Für $A(x, y) =$„x hat die Farbe y“ mit x einem Haus und y einer Farbe wäre $\quad \forall x\ A(x, \text{schwarz}) \quad$ die Aussage „Alle Häuser sind schwarz“. ♡

Soll es mindestens eine Einsetzung geben, für die die Aussageform wahr wird, verwendet man den Existenzquantor, in Zeichen „$\exists$“, „es existiert“, „es gibt“,

$$\exists x\ A(x, \text{schwarz}) \qquad \text{wäre „Es gibt ein Haus, das schwarz ist“.}$$

$\forall x$ entspricht der Konjunktion über alle x, daher findet man auch

$$\bigwedge_x \qquad \text{statt} \qquad \forall x$$

Gibt es gar kein geeignetes x, für das die Aussageform zu überprüfen wäre (etwa in „Alle Atome im Vakuum sind leichter als Wasserstoff“), ist es vorteilhaft die Gesamtaussage als wahr gelten zu lassen, denn wahr ist neutral bezüglich der Konjunktion (wenn man eine Aussage mit W „und“-verknüpft, bleibt ihr Wahrheitswert gleich), man kann sie dann getrost über und-Verknüpfungen mit weiteren Aussagen verbinden.

$\exists x$ entspricht der Disjunktion über alle x, daher findet man auch

$$\bigvee_x \qquad \text{statt} \qquad \exists x$$

Gibt es gar kein geeignetes x, für das die Aussageform zu überprüfen wäre, kann es auch nicht mindestens eines geben, und die Gesamtaussage ist falsch. Vorteilhafterweise ist falsch neutral bezüglich der Disjunktion (wenn man eine Aussage mit F „oder“-verknüpft, bleibt ihr Wahrheitswert gleich), man kann sie also problemlos mit weiteren oder-Verknüpfungen verbinden.

Vorsicht! Die Negation führt zur Umkehr der Quantoren!

$$\neg(\forall x\ A(x)) \quad \text{ist äquivalent zu} \quad \exists x\ \neg A(x)$$

$$\neg(\exists x\ A(x)) \quad \text{ist äquivalent zu} \quad \forall x\ \neg A(x)$$

Es ist eine gute Übung, die entsprechenden Aussagen für $A(x, \text{schwarz})$ sprachlich zu formulieren. $\triangledown$

An den Anfang setzt man Axiome, das sind undefinierte Begriffe und Aussagen über diesen Begriffen, die als wahr vorausgesetzt werden.

Die Theorie zu diesen Axiomen besteht dann aus allen aussagenlogisch wahren Aussagen, die durch logische Schlussregeln daraus gewonnen werden können. (Die Mathematik besteht also „nur" aus Tautologien.)

In Beweisen wird zur besseren Sicht- und Erkennbarkeit statt $\to$ meist $\Rightarrow$ und statt $\leftrightarrow$ meist $\Leftrightarrow$ geschrieben (die einfachen Pfeilvarianten kommen zu oft für andere Zwecke zum Einsatz). Bei jeder Aussage muss natürlich nachgewiesen werden, dass sie innerhalb des Axiomensystems eine Tautologie, also immer wahr ist.

Gilt $A \Rightarrow B$, sagt man
A ist hinreichend für B,
B ist notwendig für A (sonst kann A nicht gelten).

Beispiel: Wenn die Taschenlampe brennt, dann ist die Batterie noch gut.
Aber: Nur weil die Batterie noch gut ist, muss die Taschenlampe nicht brennen. B ist also i. A. (im Allgemeinen) keineswegs hinreichend für A. $\heartsuit$

Gilt $A \Leftrightarrow B$, sagt man auch

A ist notwendig und hinreichend für B.

Eine Definition führt einen Namen für ein Objekt oder eine Schreib-/Sprechweise für eine Aussage ein.

Wird ein Name für ein Objekt eingeführt, schreibt man gerne $:=$

Beispiel: $2 := 1 + 1 \qquad 2 + 1 =: 3$ $\heartsuit$

Führt man einen Namen für eine Aussage(form) ein, verwendet man meist $:\Leftrightarrow$

Beispiel: $A(x) :\Leftrightarrow$ Das Haus x ist schwarz. $\heartsuit$

Dabei steht das zu definierende jeweils auf der Seite des Doppelpunkts.

1.2 Mengen

Definition 1.1 (Cantor) *Eine Menge ist eine Zusammenfassung von wohlunterscheidbaren Objekten unseres Denkens oder unserer Anschauung.*

Dass diese Definition nicht ganz ungefährlich ist, zeigt das RUSSELsches Paradoxon

„Die Menge aller Mengen, die sich nicht selbst enthalten“.

Wir nutzen dennoch diese „naive Mengenlehre“ und werden nur mit „ungefährlichen“ Mengen arbeiten.

Die in der Menge enthaltenen Objekte sind die Elemente der Menge.
Für „a ist ein Element der Menge A“ schreiben wir $a \in A$ (auch $A \ni a$).
Für „a ist nicht Element der Menge A“ schreiben wir $a \notin A$ (auch $A \not\ni a$).

Die Elemente einer Menge können durch Aufzählung,

$$\mathbb{N} := \{1, 2, 3, \dots\} \quad \text{die natürlichen Zahlen}$$

[besser wäre die Einführung über die PEANO-Axiome, das dauert hier zu lange],
oder durch Beschreibung der Eigenschaften angegeben werden,

$$\mathbb{Z} := \{x \colon x \in \mathbb{N} \vee -x \in \mathbb{N} \vee x = 0\} \quad \text{die ganzen Zahlen},$$

$$k + \mathbb{N} := \{n + k \colon n \in \mathbb{N}\} \quad \text{für } k \in \mathbb{N}$$

(manchmal schreibt man „|“ statt „:“, also etwa $\{n + k \,|\, n \in \mathbb{N}\}$).

Elemente, die mehrmals aufgezählt werden, sind dennoch nur „einmal“ enthalten (s. spätere Definition der Gleichheit von Mengen),

$$\{a, a, b, c, b\} \text{ ist das gleiche wie } \{a, b, c\}$$

Einige wichtige Mengenbezeichnungen:

$\emptyset$ ... die leere Menge, sie enthält keine Elemente,
$\mathbb{Q}$ ... die rationalen Zahlen (s. später),
$\mathbb{R}$ ... die reellen Zahlen (s. Analysis),
$\mathbb{C}$ ... die komplexen Zahlen (s. Analysis und später).

Eine Menge heißt Teilmenge einer Menge B, in Zeichen $A \subseteq B$ (manchmal auch $A \subset B$), falls jedes Element von A auch Element von B ist,

$$A \subseteq B \;:\Leftrightarrow\; (\forall e \;\; (e \in A \Rightarrow e \in B))$$

Insbesondere gilt für jede Menge A, dass $\emptyset \subseteq A$. Die leere Menge ist also Teilmenge jeder Menge.

Zwei Mengen A und B heißen gleich ($A = B$), falls $A \subseteq B$ und $B \subseteq A$ ist,

$$A = B \;:\Leftrightarrow\; ((A \subseteq B) \wedge (B \subseteq A)) \quad \text{(so zeigt man das auch!)}.$$

Beispiel: Zeige für die übliche Addition: $\forall z \in \mathbb{Z} \;\; \mathbb{Z} = z + \mathbb{Z} := \{z + a \colon a \in \mathbb{Z}\}$.

Beweis: Sei $z \in \mathbb{Z}$ (beliebig). Wir zeigen zuerst
$\underline{\mathbb{Z} \subseteq z + \mathbb{Z}}$: Sei $b \in \mathbb{Z}$, dann ist $a = b - z$ eine ganze Zahl, also $a \in \mathbb{Z}$, daher $b = z + a \in z + \mathbb{Z}$.
$\underline{z + \mathbb{Z} \subseteq \mathbb{Z}}$: Für jedes $b \in z + \mathbb{Z}$ gibt es ein $a \in \mathbb{Z}$ mit $b = z + a$. Als Summe ganzer Zahlen ist b ganze Zahl, also $b \in \mathbb{Z}$. $\square$

Beachte: Ans Ende des Beweises setzt man gerne das $\square$-Symbol oder schreibt q.e.d. (für „quod erat demonstrandum“ [was zu beweisen war]). ♡

Sind sie nicht gleich, schreibt man $A \neq B := \neg(A = B)$.

A heißt echte Teilmenge von B ($A \subset B$ oder $A \subsetneq B$) falls $(A \subseteq B) \wedge (A \neq B)$.

Beispiel: Für $k \in \mathbb{N}$ ist $k + \mathbb{N} \subset \mathbb{N}$ und $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. ♡

Die Potenzmenge einer Menge A ist die Menge aller Teilmengen von A,

$$2^A := \{B \colon B \subseteq A\} \qquad \text{(manchmal auch } \mathcal{P}(A)).$$

Beispiel: $2^{\{0,1\}} = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$, $2^{\emptyset} = \quad \{\emptyset\}$.
Was ist nun $2^{2^{\{0,1\}}}$ und wieviele Elemente enthält diese Menge? ♡

Seien A und B Mengen,

$A \setminus B := \{a \in A \colon a \notin B\}$	ist die Differenzmenge A ohne B,
$A \cap B := \{e \colon e \in A \wedge e \in B\}$	ist der Schnitt von A und B,
$A \cup B := \{e \colon e \in A \vee e \in B\}$	ist die Vereinigung von A und B,
$A \triangle B := (A \cup B) \setminus (A \cap B)$	ist die symmetrische Differenz von A und B.
Gilt $A \cap B = \emptyset$,	so heißen A und B disjunkt (elementfremd).
Für $B \subseteq A$ heißt $A \setminus B$	das Komplement von B bezüglich A.

Beispiel: $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$, $(\mathbb{Q} \cap \mathbb{N}_0) \setminus \mathbb{N} = \{0\} = \mathbb{N} \triangle \mathbb{N}_0$. ♡

Rechengesetze:

1. Kommutativität:
   $A \cap B = B \cap A$, $\qquad A \cup B = B \cup A$,
2. Assoziativität:
   $(A \cap B) \cap C = A \cap (B \cap C)$, $\qquad (A \cup B) \cup C = A \cup (B \cup C)$,
3. Distributivität:
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $\qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
4. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$, $\qquad A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Ü: Zeige die Richtigkeit der Rechengesetze! Als Beispiel erster Teil von 3:

Beweis: $\underline{\subseteq}$: Sei $e \in A \cap (B \cup C)$, dann gilt nach Definition von $\cap$, dass $e \in A$ und $e \in B \cup C$, also nach Definition von $\cup$ auch $e \in B$ oder $e \in C$. Sei o. B. d. A. (ohne Beschränkung der Allgemeinheit [oder o. E. „ohne Einschränkung“]) $e \in B$ (sonst benenne B und C um, das geht nach 1), dann gilt nach Definition von $\cap$, dass $e \in A \cap B$, und nach Definition von $\cup$ damit $e \in (A \cap B) \cup (A \cap C)$.
$\underline{\supseteq}$: Sei $e \in (A \cap B) \cup (A \cap C)$, dann ist nach Definition $e \in (A \cap B)$ oder $e \in (A \cap C)$. O. B. d. A. sei $e \in A \cap B$ (sonst B und C umbenennen, nach

1 erlaubt), also $e \in A$ und $e \in B$. Dann ist auch $e \in B \cup C$ und damit $e \in A \cap (B \cup C)$. $\square$

⧖

Für zwei Mengen A und B ist das Kartesische Produkt $A \times B = \{(a,b) : a \in A, b \in B\}$ die Menge der geordneten Paare von Elementen aus A und B.

Zwei geordnete Paare (a,b) und (c,d) sind gleich, wenn $a = c$ und $b = d$ gilt, formal $\quad (a,b) = (c,d) :\Leftrightarrow (a = c) \wedge (b = d)$.

Beachte: I. A. ist $A \times B \neq B \times A$, weil die Ordnung wichtig ist.

1.3 Abbildungen (Funktionen)

Nun müssen die Mengen und ihre Elemente zueinander in Beziehung gebracht werden, damit auch etwas Dynamik entsteht. Abbildungen tun dies in sehr allgemeiner, aber dennoch kontrollierter Form.

Seien A und B Mengen.

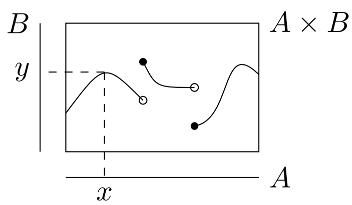
Eine Teilmenge $\Gamma \subseteq A \times B$ heißt Graph einer Abbildung, falls die folgenden beiden Eigenschaften erfüllt sind:

(Graph a) Zu jedem $x \in A$ gibt es ein $y \in B$ mit $(x,y) \in \Gamma$,
(Graph b) $(x,y), (x,y') \in \Gamma \;\Rightarrow\; y = y'$.

Die zugehörige Abbildung definiert man über

$$\begin{aligned} f\colon A &\to B \\ x &\mapsto y \text{ mit } (x,y) \in \Gamma. \end{aligned}$$

Für $(x,y) \in \Gamma$ schreibt man dann $f(x) = y$.



Beispiel: $f\colon \mathbb{R} \to \mathbb{R},\; x \mapsto 1\; (f(x) = 1),\; f\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R},\; (x,y) \mapsto 3x - y$.

Die Sprache ist *keine* Abbildung von Wörtern in Bedeutungen, z. B. „Chemnitz“. Auch mathematische Begriffe haben nicht immer nur eine Bedeutung („Graph“), aber im jeweiligen Zusammenhang muss die Bedeutung eindeutig sein. ♡

Für eine Abbildung $f\colon A \to B,\; x \mapsto y = f(x)$ nennt man

A	Definitionsbereich (von f),	
B	Wertevorrat/Bildraum (von f),	
für $x \in A$	$f(x)$	Bild von x (unter f),
für $A' \subseteq A$	$f(A') := \{f(x) \colon x \in A'\}$	Bild(menge) von A',
für $A' = A$	$f(A)$	Bild von f,
für $B' \subseteq B$	$f^{-1}(B') := \{x \in A \colon f(x) \in B'\}$	Urbildmenge von B',
für $y \in B$	$f^{-1}(\{y\})$	die Faser über y oder das Urbild von y.

Vorsicht! Das Urbild ist keine Funktion von B nach A! Man kann sie aber als Funktion $2^B \to 2^A$ auffassen. In der Praxis werden für einelementige Mengen dennoch oft die Mengenklammern weggelassen, also z. B. $f^{-1}(y)$ statt $f^{-1}(\{y\})$ geschrieben. Hier soll das sauber unterschieden werden. $\triangledown$

Von der Betrachtung aller Abbildungen $A \to B$ auf einmal hat man nicht viel. Deshalb untersucht man immer nur Teilmengen von Funktionen, für die man gewisse grundlegende Eigenschaften fordert, und versucht daraus oder aus dem Zusammenspiel solcher Funktionen weitere Eigenschaften und strukturelle Gemeinsamkeiten abzuleiten.

Eine Abbildung $f \colon A \to B$ heißt

surjektiv, falls $f(A) = B$,
[jedes Element aus B wird getroffen]

injektiv, falls aus $f(x) = f(x')$ folgt, dass $x = x'$,
[jedes Element aus B wird höchstens einmal getroffen]

bijektiv, falls f surjektiv und injektiv ist.

Beispiele:

- $f \colon \mathbb{R} \to \mathbb{R},\ x \mapsto 1$ ist weder surjektiv noch injektiv,
  $f \colon \mathbb{R} \to \{1\},\ x \mapsto 1$ ist surjektiv, aber nicht injektiv,
  $f \colon \mathbb{R} \to \mathbb{R},\ x \mapsto e^x$ (e-Funktion) ist injektiv, aber nicht surjektiv,
  $f \colon \mathbb{R} \to \mathbb{R},\ x \mapsto -3x$ ist surjektiv und injektiv, also bijektiv,
  $f \colon \emptyset \to \emptyset,\ \mapsto$ ist surjektiv und injektiv, also bijektiv.
- Für eine Grundmenge A und eine Teilmenge $S \subseteq A$ ist die charakteristische Funktion von S in A erklärt durch

$$\chi_S \colon A \to \{0,1\}$$
$$a \mapsto \chi_S(a) := \begin{cases} 1 & a \in S, \\ 0 & a \in A \setminus S. \end{cases}$$

  Konkret ergibt sich etwa
  für $A = \{1,2,3\}$, $S = \{2,3\}$ die Funktion $\chi_S = \begin{pmatrix} \chi_S(1) \\ \chi_S(2) \\ \chi_S(3) \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$,

$$\text{für } A = \mathbb{N},\ S = 2\mathbb{N} \text{ die Funktion } \chi_S = \begin{pmatrix} \chi_S(1) \\ \chi_S(2) \\ \chi_S(3) \\ \chi_S(4) \\ \vdots \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ \vdots \end{pmatrix}.$$

♡

Ist f bijektiv, ist die Urbildmenge für jedes $y \in B$ (die Faser) einelementig,

$$f^{-1}(\{y\}) = \{x\} \qquad \text{mit } (x, y) \in \Gamma,$$

wir nutzen dann die gleiche Bezeichnung für die Umkehrabbildung

$$f^{-1}\colon B \to A,\ y \mapsto x \text{ mit } (x, y) \in \Gamma \qquad (\textit{nur} \text{ für } f \text{ bijektiv}).$$

Es gilt dann $f(f^{-1}(y)) = y$ und $f^{-1}(f(x)) = x$ für alle $(x, y) \in \Gamma$.

Falls es die Umkehrabbildung gibt, ist sie eindeutig.

Beispiele:

- Die Identität $\mathrm{id}_A\colon A \to A,\ x \mapsto x$ ist ihre eigene Umkehrabbildung.
- Seien A, B Mengen. Die Kardinalität/Mächtigkeit von A, in Zeichen $|A|$, dient zum Vergleich der „Anzahl“ der Elemente von Mengen. Ohne dies hier voll zu rechtfertigen, sagen wir:
  - Die Kardinalität von A ist kleiner oder gleich der von B, $|A| \leq |B|$, wenn es eine injektive Abb. $f\colon A \to B$ gibt.
  - Gibt es eine bijektive Abb. $f\colon A \to B$, sind beide gleichmächtig, $|A| = |B|$.
  - Die Mächtigkeit von A ist echt kleiner, $|A| < |B|$, falls $|A| \leq |B|$ und $|A| \neq |B|$.

  Gibt es insbesondere ein bijektives $f\colon A \to B$ für
  - $B = \{1, \ldots, n\}$ mit $n \in \mathbb{N}_0$, setzt man $|A| = n$ und nennt A endliche Menge oder endlich,
  - $B = \mathbb{N}$, nennt man A abzählbar unendlich,

  $\}$ beide sind abzählbar.

  Gibt es *keine* surjektive Abb. $f\colon \mathbb{N} \to A$, nennt man A überabzählbare Menge (z. B. $\mathbb{R}$, s. Analysis).

♡

Satz 1.2 *Sind A, B endliche Mengen mit $|A| = |B|$, so ist für $f\colon A \to B$ äquivalent:*
(a) f ist injektiv,
(b) f ist surjektiv,
(c) f ist bijektiv.

Beweis: Sei $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_n\}$, $n \in \mathbb{N}_0$, mit paarweise verschiedenen a_i bzw. b_i.

(a)⇒(b): Wir zeigen „nicht surjektiv“ ⇒ „nicht injektiv“ (Umkehrschluss) mit dem Schubfachprinzip (Dirichlet): Sind n Objekte in m Fächern mit $m < n$, enthält ein Fach mindestens zwei Objekte.
Ist f nicht surjektiv, werden nur $m < n$ Fächer b_i für n Objekte a_j getroffen ⇒ nicht injektiv.

(b)⇒(a): Ist f nicht injektiv, gibt es a_i, a_j, $i \neq j$, mit $f(a_i) = f(a_j)$, also ist $|f(A)| < n$, damit ist f nicht surjektiv.

(b)⇒(c): Da (b)⇔(a) ist f auch injektiv, also bijektiv.

(c)⇒(b): folgt direkt aus der Definition, es ist „trivial“. □

Ü: Zeige: Unter den Abbildungen $\mathbb{N} \to \mathbb{N}$ gibt es sowohl Abbildungen, die injektiv aber nicht surjektiv, als auch Abbildungen, die surjektiv aber nicht injektiv sind (S 1.2 funktioniert also *nur* für endliche Mengen). ⧖

Satz 1.3 *Die Kardinalität einer Menge A ist echt kleiner als die Kardinalität ihrer Potenzmenge 2^A, in Zeichen $|A| < |2^A|$.*

Beweis: Die Abbildung $g\colon A \to 2^A,\ a \mapsto \{a\}$ ist injektiv. Angenommen, es gibt eine bijektive Abbildung $f\colon A \to 2^A,\ a \mapsto S_a$, dann gibt es für die Teilmenge $M = \{a \in A\colon a \notin S_a\}$ ein $m \in A$ mit $M = f(m) = S_m$. Für dieses m ist $m \in M \Leftrightarrow m \notin S_m = M$ ↯. □

Diese Beweistechnik zur Wahl von M geht auf Cantor zurück und wird Cantorsches Diagonalverfahren genannt.

Komposition (Hintereinanderschaltung) von Abbildungen:

Sind $f\colon A \to B$ und $g\colon B \to C$ Abbildungen, dann ist

$$\begin{aligned} g \circ f\colon A &\to C \\ a &\mapsto (g \circ f)(a) = g(f(a)) \end{aligned}$$ die Komposition von g und f.

Vorsicht! Bei manchen Autoren ist $(g \circ f) = f(g(a))$! ▽

Ist $h\colon C \to D$ eine weitere Abb., so gilt Assoziativität:

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

denn: für $a \in A$ gilt $((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = (h(g(f(a))) = h((g \circ f)(a)) = (h \circ (g \circ f))(a)$. □

Beobachtung 1.4 *Für $f\colon A \to B$ und $g\colon B \to A$ sei $g \circ f = \mathrm{id}_A$, dann ist f injektiv und g surjektiv.*

Beweis: Für $a \in A$ gilt: $a = \mathrm{id}_A(a) = g(f(a))$,
also ist $f(a) \in g^{-1}(\{a\}) \neq \emptyset$ und g surjektiv.

Gilt für $a, b \in A$, dass $f(a) = f(b)$, so ist

$$a = \mathrm{id}_A(a) = g(f(a)) = g(f(b)) = \mathrm{id}_A(b) = b,$$

also f injektiv. □

Ü: Geben Sie ein Beispiel für $A = B, f, g$ mit $g \circ f = \mathrm{id}_A$ aber f nicht surjektiv an. ⧖

Beobachtung 1.5 *Für $f, g\colon A \to A$ sei $g \circ f = \mathrm{id}_A$. Ist f bijektiv, dann ist $g = f^{-1}$ die Umkehrabbildung von f. Ist g bijektiv, dann ist $f = g^{-1}$ die Umkehrabbildung von g.*

Beweis: Im Fall f bijektiv ist zu zeigen: Für $a \in A$ ist $g^{-1}(\{a\}) = \{f(a)\}$.
Wie oben zeigt man $f(a) \in g^{-1}(\{a\})$.
Sei nun $c \in g^{-1}(\{a\})$, also $g(c) = a$,
dann gibt es wegen f bijektiv ein eindeutiges $b \in A$ mit $f(b) = c$ und $b = \mathrm{id}_A(b) = g(f(b)) = g(c) = a$, also ist $c = f(a)$.
Im Fall g bijektiv ist wegen B1.4 f injektiv, also für $a \in A$ nur $g(a) \in f^{-1}(\{a\})$ zu zeigen. Sei $b = g(a)$, dann ist $b = \mathrm{id}_A(b) = g(f(b))$ und wegen g injektiv $f(b) = a$ bzw. $b = g(a) \in f^{-1}(\{a\})$. □

Ü: Sind $f\colon A \to B$ und $g\colon B \to C$ injektiv (surjektiv), ist auch $g \circ f$ injektiv (surjektiv). ⧖

Die Komposition ist also immer assoziativ,
ABER: die Komposition ist i. A. nicht kommutativ!

Beispiel: Schon für $f\colon A \to B$ bijektiv ist $\quad f^{-1} \circ f = \mathrm{id}_A \neq f \circ f^{-1} = \mathrm{id}_B$.
♡

Die Menge der Permutationen S_n, $n \in \mathbb{N}_0$:

Eine Permutation $\sigma \in S_n$ ist eine bijektive Abbildung

$$\begin{aligned} \sigma\colon \{1, \dots, n\} &\to \{1, \dots, n\} \\ i \quad &\mapsto \sigma(i) \end{aligned}$$

wobei $\{1, \dots, 0\} := \emptyset$ gesetzt wird und die konkreten Zuweisungen oft über

$$\begin{pmatrix} 1 & 2 & 3 & & n \\ \sigma(1) & \sigma(2) & \sigma(3) & & \sigma(n) \end{pmatrix} \quad \text{oder nur} \quad \sigma(1)\ \sigma(2)\ \sigma(3) \cdots \sigma(n)$$

angegeben werden.

$|S_n| = n! := n \cdot (n-1) \cdot \dots \cdot 1$, „$n$ Fakultät“, „n Faktorielle“, $0! := 1$.

Sind $\sigma, \tau \in S_n$, dann ist auch $\tau \circ \sigma \in S_n$ (nach obiger Ü, da beide bijektiv), ABER i. A. $\tau \circ \sigma \neq \sigma \circ \tau$, etwa für S_3

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \ \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Natürlich kann man auch Funktionen auf Funktionenmengen erklären, z. B. das Signum einer Permutation

$$\begin{aligned} \operatorname{sgn}\colon S_n &\to \{+1, -1\} \\ \sigma &\mapsto \operatorname{sgn}(\sigma) = \begin{cases} +1, \\ -1, \end{cases} \text{falls} \begin{bmatrix} \text{die Anzahl der Paare } (i,j) \\ \text{mit } i > j \text{ aber } \sigma(i) < \sigma(j) \end{bmatrix} \begin{matrix} \text{gerade} \\ \text{ungerade} \end{matrix} \text{ ist.} \end{aligned}$$

Im obigen Beispiel zu S_3: $\operatorname{sgn}(\sigma) = -1$, $\operatorname{sgn}(\tau) = +1$, $\operatorname{sgn}(\mathrm{id}_{\{1,\ldots,n\}}) = 1$.

Ü: Zeige $\quad \operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\tau \circ \sigma) = \operatorname{sgn}(\tau) \cdot \operatorname{sgn}(\sigma)$. ⧖

1.4 Mengen-Familien und Kartesische Produkte

Eine Familie von Mengen A_i, $i \in \mathcal{J}$, besteht aus einer Indexmenge $\mathcal{J}$ und für jedes $i \in \mathcal{J}$ einer Menge A_i, die man als Teilmengen einer oft nicht explizit erwähnten Grundgesamtheit Ω aller relevanten Elemente auffasst; $A_i = A_j$ für verschiedene Indices $i, j \in \mathcal{J}$ ist zulässig. Formal darf man sich eine Familie als Funktion $A\colon \mathcal{J} \to 2^\Omega$, $i \mapsto A(i) := A_i \subseteq \Omega$ vorstellen.

$$\bigcap_{i \in \mathcal{J}} A_i := \{e\colon \text{für alle } i \in \mathcal{J} \text{ ist } e \in A_i\}, \quad \text{für } \mathcal{J} = \emptyset \text{ ist } \bigcap_{\emptyset} = \Omega,$$

$$\bigcup_{i \in \mathcal{J}} A_i := \{e\colon \text{es gibt } i \in \mathcal{J} \text{ mit } e \in A_i\}, \quad \text{für } \mathcal{J} = \emptyset \text{ ist } \bigcup_{\emptyset} = \emptyset.\text{[Warum?]}$$

Das kartesische Produkt zweier Mengen bildet die Grundlage für Funktionen. Wir werden aber viel allgemeinere Konstrukte als nur Paare von Elementen aus zwei Mengen benötigen und führen diese nun in zwei Schritten ein.

Seien $n \in \mathbb{N}_0$ und $A_1, \ldots, A_n$ Mengen, dann ist

$$A_1 \times A_2 \times \cdots \times A_n := \bigtimes_{i=1}^{n} A_i := \{(a_1, \ldots, a_n)\colon a_i \in A_i \text{ für } i = 1, \ldots, n\}.$$

Man nennt $(a_1, \ldots, a_n)$ ein n-Tupel, das man sich als geordnete Liste mit Zeilen 1 bis n vorstellen kann. Insbesondere ist $()$ das 0-Tupel (oder die „leere Liste“), also $\bigtimes_{i=1}^{0} A_i = \{()\}$ eine ein-elementige Menge!
[Diese Definition wird sich später noch als sehr hilfreich erweisen.]

Ganz allgemein werden nun beliebige Elemente als Listenindices zugelassen: Sei A_i, $i \in \mathcal{J}$, eine Familie von Mengen (Teilmengen von Ω), dann bezeichnet ein $\mathcal{J}$-Tupel eine Funktion $x\colon \mathcal{J} \to \Omega,\ i \mapsto x_i \in \Omega$ und

$$\bigtimes_{i\in\mathcal{J}} A_i := \{\mathcal{J}\text{-Tupel } x\colon x_i \in A_i \text{ für } i \in \mathcal{J}\}.$$

Die vorhergehenden Definitionen entpuppen sich als Spezialfälle, wenn man $n \in \mathbb{N}_0$ als Kurzschreibweise der Indexmenge $\mathcal{J} = \{1, \dots, n\}$ interpretiert, wobei $\{1, \dots, 0\} = \emptyset$ gesetzt wird. Wie zuvor ist $\bigtimes_{i\in\emptyset} A_i = \{()\}$ eine einelementige Menge.

Vorsicht! Formal unterscheidet sich das $\{0, 1, 2\}$-Tupel vom 3-Tupel dadurch, dass beim ersten die Indexelemente 0, 1, und 2 sind, beim zweiten 1, 2 und 3! Wenn es nur um die Anzahl der Elemente geht und die Indexverwendung klar ist, wird oft nicht so streng unterschieden. $\triangledown$

Zwei $\mathcal{J}$-Tupel x und y sind gleich falls $x_i = y_i$ für $i \in \mathcal{J}$ gilt, formal

$$x = y \quad :\Leftrightarrow \qquad \forall i \in \mathcal{J}\ (x_i = y_i).$$

Für allgemeine Indexmengen ist die Anordnung im $\mathcal{J}$-Tupel nicht mehr so einfach wie für n-Tupel, sie ist aber auch nicht wichtig. Wenn es eine sinnvolle Anordnung der Menge $\mathcal{J}$ gibt, dann übernimmt man diese meist auch für die Darstellung der Tupel. Aber auch andere Anordnungen sind erlaubt, solange die Zuordnung der Tupelelemente zu den Indexelementen klar bleibt.

Beispiel: Bei Einkaufslisten ist $\mathcal{J}$ die Menge der einkaufbaren Produkte und für $i \in \mathcal{J}$ beschreibt A_i die möglichen Mengenangaben (z. B. $A_i = \mathbb{N}_0$ für Stück, $\mathbb{Q}$ für Anteil an Litern/kg). Für eine Einkaufsliste $L \in \bigtimes_{i\in\mathcal{J}} A_i$ gibt man meist nur die Einträge $\neq 0$ an, für alle anderen wird 0 angenommen. Wie man Einkaufslisten aufschreibt, ist egal, solange die Produktbezeichung (die Indexzuordnung) eindeutig bleibt. $\heartsuit$

Wichtige Spezialfälle:

- Wird in $A_1 \times A_2 \times \cdots \times A_k$ eine Menge A_i durch eine Zahl $n \in \mathbb{N}_0$ ersetzt, steht n für die Menge $\{1, \dots, n\}$ (mit $\{1, \dots, 0\} = \emptyset$) wie zuvor.

  Beispiel: Für $m, n \in \mathbb{N}_0$ ist

  $$m \times n = \{(i, j)\colon i \in \{1, \dots, m\}, j \in \{1, \dots, n\}\}\,.$$

  Statt (i, j) schreibt man kurz ij, wenn keine Verwechslungsgefahr besteht. $\heartsuit$

  Ü: Wieviele und welche Elemente haben die Mengen $1 \times 2 \times 3$, 2×0, 0×3? $\bowtie$

- Gilt für alle $i \in \mathcal{J}$, dass $A_i = A$, sind also alle Mengen der Familie die gleiche Menge A, schreibt man kurz
$$A^{\mathcal{J}} := \bigtimes_{i \in \mathcal{J}} A = \{\mathcal{J}\text{-tupel } x \colon x_i \in A \text{ für } i \in \mathcal{J}\}.$$
Insbesondere ist etwa für $n \in \mathbb{N}_0$
$$A^n = A^{\{1,\dots,n\}} = \bigtimes_{i=1}^{n} A = \{(x_1, \dots, x_n) \colon x_i \in A \text{ für } i = 1, \dots, n\}.$$
[In solchen n-Tupeln legt die Reihenfolge die Indexzuordnung fest, daher ist hier die Reihenfolge wichtig.]

Beispiele:

- $\mathbb{R}^2$ lernt man in der Schule als die Ebene, deren Punkte als Zeilen-2-Tupel (x, y) mit kartesischen Koordination x und y beschrieben werden, kennen. Alternativ kann $\mathbb{R}^2$ auch als Raum der 2-dimensionalen Vektoren aufgefasst werden, dann schreibt man die Elemente meist als Spalten-2-Tupel $\binom{x}{y}$. Genauso kann man $\mathbb{R}^3$ als 3-dimensionalen Raum von Punkten (x, y, z) oder Vektoren $\left(\begin{smallmatrix} x \\ y \\ z \end{smallmatrix}\right)$ auffassen. Wegen der besseren Zuordnung ist die mathematische Bezeichung der Koordinaten aber meist durchnummeriert, also statt $\left(\begin{smallmatrix} x \\ y \\ z \end{smallmatrix}\right)$ eher $\left(\begin{smallmatrix} x_1 \\ x_2 \\ x_3 \end{smallmatrix}\right)$, und $x \in \mathbb{R}^3$ bezeichnet dann gleich den ganzen Punkt/Vektor.
- Für $F = \{\diamondsuit, \heartsuit, \clubsuit, \spadesuit\}$ und $W = \{A, K, D, B, 10, ..., 2\}$ beschreibt $F \times W$ das Französische Blatt.
- Kartenspiel SET: Jede Karte hat 4 Eigenschaften in 3 Ausprägungen:
  Anzahl = $\{1, 2, 3\}$, Form = {Ellipse,Rechteck,Tilde},
  Farbe = {rot,blau,grün}, Füllgrad = {leer,schraffiert,gefüllt},
  und die Menge der Karten ist Anzahl × Form × Farbe × Füllgrad.
- Ist die Grundmenge A eine Menge von Zahlen mit Rechenregeln (also z. B. eine aus $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$), so nennt man ein Element $H \in M(m \times n; A) := A^{m \times n}$ eine $m \times n$ Matrix (über A) und $M(m \times n; A)$ die Menge der $m \times n$ Matrizen über A. Man ordnet die Einträge von H in m Zeilen und n Spalten in folgender Weise an:
$$H = \begin{bmatrix} H_{11} & \dots & H_{1n} \\ \vdots & \ddots & \vdots \\ H_{m1} & \dots & H_{mn} \end{bmatrix}$$
Die Einträge der Matrix heißen auch Matrixelemente und werden oft auch in Kleinschreibung angesprochen, etwa in der Form $H = (h_{ij}) \in \mathbb{R}^{m \times n}$, dann sind h_{ij} und H_{ij} bedeutungsgleich.
Konkret ist z. B. $H = \begin{bmatrix} 5 & -1 & 8 \\ -1 & 6 & 4 \end{bmatrix}$ eine 2×3-Matrix (über $\mathbb{Z}$), und $H_{1,3} = 8$. Beachte, dass man je nach Lesbarkeit und Bedarf für das

Indexpaar (i, j) nur ij oder i, j schreibt. Soeben war $H_{1,3}$ besser lesbar als H_{13}, aber weniger Arbeit als $H_{(1,3)}$. Man verwendet für Matrizen meistens Großbuchstaben, aber natürlich oft andere als H.

♡

Matrizen und Vektoren mit ihren Rechenregeln und Eigenschaften sind ein Kernthema dieser Vorlesung, denn durch sie lassen sich lineare Gleichungssysteme und die später noch einzuführenden linearen Abbildungen hervorragend beherrschen.

Beispiele:

- In der Schule wird die Lösung linearer Gleichungssysteme meist für drei Variablen und drei Gleichungen besprochen, also etwa ein Beispiel der Art

$$\begin{array}{rcrcrcr} x_1 & - & x_2 & + & 3x_3 & = & 6, \\ 2x_1 & + & 5x_2 & - & 4x_3 & = & -5, \\ -x_1 & + & 2x_2 & & & = & 4. \end{array}$$

Die Koeffizienten der Gleichungen – das sind die Zahlen, mit denen die Variablen x_1, x_2, x_3 mutlipliziert werden – fassen wir in einer 3×3 Matrix H zusammen, ebenso die rechte Seite der Gleichungen in einem Vektor b und schreiben für das Gleichungssystem kurz

$$H \cdot x = b \quad \text{mit} \quad H = \begin{bmatrix} 1 & -1 & 3 \\ 2 & 5 & -4 \\ -1 & 2 & 0 \end{bmatrix}, \; x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \text{ und } b = \begin{pmatrix} 6 \\ -5 \\ -4 \end{pmatrix}$$

(es ist ein wenig Geschmacksfrage, wann man eckige und wann man runde Klammern verwendet). Der Ausdruck $H \cdot x$ wird später noch sauber definiert werden; hier steht er einfach für die linke Seite des oberen Gleichungssystems mit dem Vektor der Variablen x, der, wenn möglich, geeignet aus $\mathbb{R}^3$ gewählt werden soll, um das Gleichungssystem zu erfüllen.

Allgemein hat für n Variablen $x_1, \ldots, x_n$ ein reelles lineares Gleichungssystem mit m Gleichungen die Form,

$$\begin{array}{rcccrcl} h_{11}x_1 & + & \ldots & + & h_{1n}x_n & = & b_1 \\ & & \vdots & & & & \vdots \\ h_{m1}x_1 & + & \ldots & + & h_{mn}x_n & = & b_m \end{array}$$

mit gegebenen Koeffizienten $h_{ij} \in \mathbb{R}$ für $i = 1, \ldots, m$, $j = 1, \ldots, n$ und gegebener rechter Seite $b_i \in \mathbb{R}$. Dieses lässt sich mit der $m \times n$ Matrix $H = (h_{ij}) \in \mathbb{R}^{m\times n}$, $x = (x_j) \in \mathbb{R}^n$ und $b = (b_i) \in \mathbb{R}^m$ genauso kurz wie das 3×3 System als $H \cdot x = b$ schreiben.

- Matrizen und Lineare Gleichungssysteme sind *das* Hauptwerkzeug in der angewandten Mathematik, wenn etwas gerechnet werden muss. Fast alles wird darauf zurückgeführt. Besonders große Beispiele findet man etwa in der Datenspeicherung und -analyse bei Netflix (Benutzer $\times$ Filme $\{0,1\}$ Matrix) und Google (Webseiten $\times$ Webseiten Matrix).

$\heartsuit$

Die Menge der Abbildungen von A nach B kann mit B^A identifiziert werden und wird oft mit

$$\mathrm{Abb}(A,B) := B^A \qquad \text{bezeichnet,}$$

denn jedes Element $f \in B^A$ ist ein A-Tupel, das jedem $x \in A$ genau ein $y = (f)_x \in B$ zuordnet,

$$\Gamma := \{(x,(f)_x)\colon x \in A\} \subseteq A \times B \qquad \text{erfüllt (Graph a) und (Graph b).}$$

Beispiel: Für jedes $S \subseteq A$ ist die charakteristische Funktion $\chi_S \in \{0,1\}^A$. Die folgende Funktion ordnet nun jeder Teilmenge ihre charakteristische Funktion zu,

$$\begin{aligned}\chi\colon 2^A &\to \{0,1\}^A\\ S &\mapsto \chi_S\end{aligned}$$

Sie weist jeder Teilmenge $S \subseteq A$ das A-Tupel zu, das in Position a genau dann eine 1 hat, wenn $a \in S$. Jedes A-Tupel aus $\{0,1\}^A$ passt zu genau einer Teilmenge, wird also einmal und nur einmal von χ zugeordnet, daher ist die Funktion χ bijektiv. $\heartsuit$

Ü: Zeige: Sind A, B Mengen mit $|B| \geq 2$, dann ist die Kardinalität von A echt kleiner als die der Abbildungen B^A von A nach B. ⧖

1.5 Relationen

Im Vergleich zu Abbildungen bieten Relationen noch umfassendere Möglichkeiten, Elemente von Mengen zueinander in Beziehung zu setzen.

Eine Relation ist eine Menge, deren Elemente geordnete Paare sind:

Seien A, B Mengen. $R \subseteq A \times B$ ist eine Relation.

Gilt $(a,b) \in R$, stehen a und b in Relation, formal schreibt man dafür

$$aRb \;:\Leftrightarrow\; (a,b) \in R.$$

Beispiele:

1. Für eine Abb. $f\colon A \to B$ ist ihr Graph $\Gamma \subseteq A \times B$ eine Relation.
   Auch die von f induzierte

   Faserung $R_f = \{(a_1, a_2) \in A \times A\colon f(a_1) = f(a_2)\}$ ist eine Relation.

   Konkret gilt für $\cos\colon \mathbb{R} \to \mathbb{R},\ x \mapsto \cos(x)$ mit $k \in \mathbb{Z}$ und $x \in \mathbb{R}$ jeweils $xR_{\cos}(x + 2k\pi)$ und $xR_{\cos}(-x + 2k\pi)$.
2. Die Ordnungsrelation $R_\leq \subseteq \mathbb{R} \times \mathbb{R}$, $aR_\leq b :\Leftrightarrow a \leq b$ für $a, b \in \mathbb{R}$,
   die Teilmengenrelation $R_\subseteq \subseteq 2^A \times 2^A$, $A' R_\subseteq A'' :\Leftrightarrow A' \subseteq A''$ für $A', A'' \in 2^A$.
3. Sei $Z = \mathbb{N}^2$, dann erklärt $R_Z \subseteq Z \times Z$

   $$(n_1, m_1)R_Z(n_2, m_2) :\Leftrightarrow n_1 + m_2 = n_2 + m_1 \quad \text{eine Relation auf } Z.$$

   Konkret: $(1, 7)R_Z(9, 15)$, nicht aber $(1, 7)$ und $(7, 1)$.
   Sei $Q = \mathbb{Z} \times \mathbb{N}$, dann erklärt $R_Q \subseteq Q \times Q$

   $$(z_1, n_1)R_Q(z_2, n_2) :\Leftrightarrow z_1 \cdot n_2 = z_2 \cdot n_1 \quad \text{eine Relation auf } Q.$$

   Konkret: $(-1, 3)R_Z(-4, 12)$, nicht aber $(1, 3)$ und $(-1, 3)$.
4. Kongruenz modulo m: Sei $m \in \mathbb{N}$, $R_m \subseteq \mathbb{Z} \times \mathbb{Z}$

   $$aR_m b \ :\Leftrightarrow\ m | a - b \quad (m \text{ teilt } a - b).$$

   Man schreibt dann auch $\quad a \equiv b \pmod{m}$
   und sagt: a ist kongruent b modulo m.
   [a hat den gleichen Rest wie b bei Division durch m.]
   Konkret: $15 \equiv 3 \mod 12$, $24 \equiv 0 \mod 12$, $-1 \equiv 11 \mod 12$.

♡

Für eine gegebene Relation $R \subseteq A \times B$ sucht man oft für eine
Teilmenge $X \subseteq A$ alle Elemente $B_R(X) := \{b \in B\colon \forall a \in X\ (a, b) \in R\}$
(oder für $Y \subseteq B$ alle Elemente $A_R(Y) := \{a \in A\colon \forall b \in Y\ (a, b) \in R\}$),
die zu allen Elementen der Teilmenge in Relation stehen.

Diese Funktionen $B_R\colon 2^A \to 2^B$, $A_R\colon 2^B \to 2^A$ sind über R eng miteinander verbunden:

Lemma 1.6 (Dualitätslemma für Relationen)
Seien A, B Mengen, $R \subseteq A \times B$ eine Relation und A_R, B_R wie oben, dann gilt für $X, X' \subseteq A$, $Y, Y' \subseteq B$

(a) $X \subseteq X' \Rightarrow B_R(X) \supseteq B_R(X')$, $\quad Y \subseteq Y' \Rightarrow A_R(Y) \supseteq A_R(Y')$,

(b) $X \subseteq A_R(B_R(X))$, $\quad Y \subseteq B_R(A_R(Y))$,

(c) $B_R(X) = B_R(A_R(B_R(X)))$, $\quad A_R(Y) = A_R(B_R(A_R(Y)))$.

Insbesondere erklärt für $\mathcal{A}_R := \{A_R(Y) \colon Y \subseteq B\}$, $\mathcal{B}_R := \{B_R(X) \colon X \subseteq A\}$

$$\begin{array}{rl}\bar{A}_R \colon \mathcal{A}_R & \to \mathcal{B}_R \\ X & \mapsto B_R(X)\end{array} \quad \textit{eine bijektive Abbildung mit} \quad \begin{array}{rl}\bar{A}_R^{-1} = \bar{B}_R \colon \mathcal{B}_R & \to \mathcal{A}_R \\ Y & \mapsto A_R(Y).\end{array}$$

Beweis: in den Übungen. □

Eine Relation $R \subseteq A \times A$ (zwischen Elementen der gleichen Menge) heißt

reflexiv,	wenn aRa	(R)	für alle $a, b, c \in A$ gilt.
symmetrisch,	wenn $aRb \Rightarrow bRa$	(S)	
antisymmetrisch,	wenn $aRb \wedge bRa \Rightarrow a = b$	(A)	
transitiv,	wenn $aRb \wedge bRc \Rightarrow aRc$	(T)	

Zu den vorigen Beispielen:

1. Faserung	R, S, T, aber nicht A,
2. $R_\leq$ und $R_\subseteq$	R, A, T, aber nicht S,
3. R_Z und R_Q	R, S, T, aber nicht A,
4. $a \equiv b \mod m$	R, S, T, aber nicht A.

Äquivalenzrelationen

Ein $R \subseteq A \times A$ heißt Äquivalenzrelation, falls R reflexiv, symmetrisch und transitiv (RST) ist, man verwendet dann gerne $\sim$ statt R.

Für eine Äquivalenzrelation $\sim$ gilt damit für alle $a, b, c \in A$

$$a \sim a, \qquad a \sim b \Leftrightarrow b \sim a, \qquad a \sim b \wedge b \sim c \Rightarrow a \sim c.$$

Auf einer Menge bringt jede Äquivalenzrelation automatisch eine Einteilung dieser Grundmenge in Äquivalenzklassen mit sich:

Eine *nichtleere* Teilmenge $K \subseteq A$ heißt Äquivalenzklasse (bzgl. $\sim$), falls
(a) $x \in K \wedge y \in K \Rightarrow x \sim y$,
(b) $x \in K \wedge y \in A \setminus K \Rightarrow x \not\sim y$.

Für $a \in A$ definiert $K(a) := \{b \in A \colon a \sim b\}$ eine Äquivalenzklasse.
[Das ist übrigens gerade $A_\sim(\{a\})$ aus dem Dualitätslemma.]

Beweis: $K(a) \neq \emptyset$: $a \sim a \Rightarrow a \in K(a)$.
(a): Ist $x \in K(a)$ und $y \in K(a)$, gilt

$$a \sim x \overset{(S)}{\Rightarrow} x \sim a \quad \text{und} \quad x \sim a \wedge a \sim y \overset{(T)}{\Rightarrow} x \sim y.$$

(b): Durch Umkehrschluss: Ist $x \sim y$ und $x \notin K(a)$, stimmt die Aussage. Ist nun $x \in K(a)$, gilt $a \sim x$ und wegen (T) auch $a \sim y$, also $y \in K(a)$ und $y \notin A \setminus K(a)$. □

Man schreibt oft $[a] := K(a)$ für die durch a repräsentierte Äquivalenzklasse.
[Später werden wir oft noch kürzer $\bar{a}$ verwenden.]

Beobachtung 1.7 *Für $a, b \in A$ gilt*
(a) $a \sim b \Leftrightarrow K(a) = K(b)$,
(b) $K(a) \neq K(b) \Rightarrow K(a) \cap K(b) = \emptyset$.

Beweis: (a): „$\Rightarrow$“: Da die Behauptung invariant gegenüber Vertauschung von a und b ist, reicht es $K(a) \subseteq K(b)$ zu zeigen. Sei $c \in K(a)$, dann gilt $a \sim c$. Wegen $b \overset{(S)}{\sim} a \sim c$ und (T) gilt $b \sim c$, also $c \in K(b)$.
„$\Leftarrow$“: Wegen $b \in K(b) = K(a)$ gilt $b \in K(a)$, also $a \sim b$.

(b): Durch Umkehrschluss: Ist $c \in K(a) \cap K(b)$, gilt $a \sim c \overset{(S)}{\sim} b$ und wegen (T) $a \sim b$, nach (a) also $K(a) = K(b)$. □

Definition 1.8 *Eine Familie $K_i \subseteq A, i \in \mathcal{J}$, von Teilmengen einer Grundmenge A heißt Klasseneinteilung oder Partition von A, falls folgende drei Eigenschaften erfült sind:*
(a) $K_i \neq \emptyset$ *für alle* $i \in \mathcal{J}$,
(b) $K_i \cap K_j = \emptyset$ *für alle* $i, j \in \mathcal{J}$ *mit* $i \neq j$,
(c) $A = \bigcup_{i \in \mathcal{J}} K_i$.

Die Beobachtungen oben beweisen:

Satz 1.9 *Die Menge der Äquivalenzklassen $\mathcal{K} = \{K(a) \colon a \in A\}$ einer Äquivalenzrelation auf A ist stets eine Klasseneinteilung von A.*

(Verwende $\mathcal{K}$ selbst als Indexmenge $\mathcal{J}$, $A = \bigcup_{K \in \mathcal{K}} K$.)

Umgekehrt induziert jede Klasseneinteilung eine Äquivalenzrelation:

Satz 1.10 *Ist $\mathcal{K} \subseteq 2^A$ eine Klasseneinteilung von A, dann ist die durch*

$$a \sim_{\mathcal{K}} b :\Leftrightarrow \exists K \in \mathcal{K} \; (a \in K \wedge b \in K)$$

auf A definierte Relation $\sim_{\mathcal{K}}$ eine Äquivalenzrelation

Beweis: %:=„trivial“ (also: man muss nur überprüfen, dass $\sim_{\mathcal{K}}$ den von der Definition der Äquivalenzrelation geforderten Eigenschaften RST genügt; das kann dann noch Arbeit bedeuten, aber die sollte sich selbst erklären).□

Ist K eine Äquivalenzklasse, heißt jedes $a \in K$ Repräsentant der Klasse und es gilt $K = K(a)$. Die Äquivalenzrelation/Klasseneinteilung wird meist verwendet um herauszuarbeiten, welche Elemente der Menge man *nicht mehr* unterscheiden will. Für diese soll es gleichgültig sein, mit welchem Repräsentanten man weiterarbeitet. Man unterschiedet nur noch die Äquivalenzklassen selbst, die „äquivalenten“ Elemente werden „herausfaktorisiert“.

Definition 1.11 *Sei $\sim$ eine Äquivalenzrelation auf A. Die Menge der Äquivalenzklassen heißt Faktormenge oder Quotientenmenge von A bezüglich $\sim$ und wird mit $A_{/\sim}$ oder $[A]$ bezeichnet.*

Beispiele:

zu 1.: Für $f\colon A \to B$ induziert die Faserung die Äquivalenzrelation $\sim_f$. Für $[a] \in A_{/\sim_f}$ und $a' \in A$ gilt $a' \in [a] \Leftrightarrow f(a') = f(a)$, d. h., die Abbildung

$$\begin{aligned} \bar{f}\colon A_{/\sim_f} &\to B \\ [a] &\mapsto f([a]) := f(a) \end{aligned}$$

ist wohldefiniert und nach Konstruktion immer injektiv. [„Wohldefiniertheit" ist immer zu zeigen, wenn eine Definition gleichzeitig eine Behauptung enthält, hier die, dass durch $\bar{f}$ wirklich eine Funktion definiert wird, also der Wert $f([a])$ unabhängig von der Wahl des Repräsentanten von $[a]$ ist.]

Für das Beispiel $\cos\colon \mathbb{R} \to \mathbb{R},\ x \mapsto \cos(x)$ ist $[x] = \{\pm x + 2k\pi : k \in \mathbb{Z}\}$. Jedes $[x]$ hat genau einen Repräsentanten im Intervall $[0, \pi]$, und weil $\mathbb{R} = \bigcup_{x\in[0,\pi]}[x]$ können wir uns unter $\overline{\cos}\colon \mathbb{R}_{/\sim_{\cos}} \to \mathbb{R},\ [x] \mapsto \cos(x)$ einfach die Einschränkung von cos auf $[0, \pi]$ vorstellen, d. h., $\overline{\cos}$ verhält sich genau wie $\cos|_{[0,\pi]}\colon [0, \pi] \to \mathbb{R},\ x \mapsto \cos(x)$.

zu 3.: Für $Z = \mathbb{N}^2$ ist R_Z die Äquivalenzrelation

$$(n_1, m_1) \sim_Z (n_2, m_2) \;:\Leftrightarrow\; n_1 + m_2 = n_2 + m_1$$

Ü: Zeige: $\bar{f}\colon \mathbb{N}^2_{/\sim_Z} \to \mathbb{Z},\ [(n, m)] \mapsto n - m$ ist wohldefiniert und bijektiv. Wie muss man die Addition auf Z erklären, damit die Addition beliebiger Repräsentanten immer in der zu dieser Bijektion passenden Äquivalenzklasse landet? [So führt man formal $\mathbb{Z}$ ein.] ⧖

Für $Q = \mathbb{Z} \times \mathbb{N}$ ist R_Q die Äquivalenzrelation

$$(z_1, n_1) \sim_Z (z_2, n_2) \;:\Leftrightarrow\; z_1 \cdot n_2 = z_2 \cdot n_1$$

Ü: Zeige: $\bar{f}\colon (\mathbb{Z} \times \mathbb{N})_{/\sim_Q} \to \mathbb{Q},\ [(z, n)] \mapsto \frac{z}{n}$ ist wohldefiniert und bijektiv. Wie muss man die Multiplikation auf Q erklären, damit die Multiplikation beliebiger Repräsentanten immer in der zu dieser Bijektion passenden Äquivalenzklasse landet? [So führt man formal $\mathbb{Q}$ ein.] ⧖

zu 4.: Kongruenz modulo $m \in \mathbb{N}$: Statt $a \sim_m b$ schreibt man für $a, b \in \mathbb{Z}$

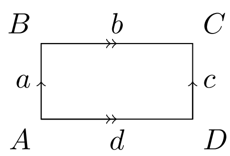
$$a \equiv b \mod m \quad :\Leftrightarrow \quad m | a - b$$

Die Äquivalenzklassen nennt man Restklassen/Kongruenzklassen.

$$\begin{array}{lll}
\text{Restklasse zu} & 0 & : K(0) = \{x : x = m \cdot k, k \in \mathbb{Z}\} \\
\text{— " —} & 1 & : K(1) = \{x : x = m \cdot k + 1, k \in \mathbb{Z}\} \\
 & \vdots & : \\
 & m-1 & : K(m-1) = \{x : x = m \cdot k - 1, k \in \mathbb{Z}\} \\
 & m & : K(m) = K(0) \\
 & -1 & : K(-1) = K(m-1)
\end{array}$$

Ü: Zeige: $\mathbb{Z}_{/\equiv \bmod m} = \{[0], \dots, [m-1]\}$. Wie überträgt sich die Addition aus $\mathbb{Z}$ auf $\mathbb{Z}_{/\equiv \bmod m}$? ⧖

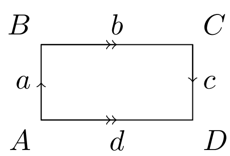
Topologie: Betrachte ein Rechteck $ABCD$ (etwa ein Blatt Papier).



Es bezeichne a die gerichtete Strecke $\overrightarrow{AB}$ von A nach B, b die Strecke $\overrightarrow{BC}$, c die Strecke $\overrightarrow{DC}$ (!) und d die Strecke $\overrightarrow{AD}$ (!).
In der Relation $\sim_{\substack{a=c\\b=d}}$: seien die Punkte auf a äquivalent zu den entsprechenden Punkten auf c, die auf b äquivalent zu denen auf d, und alle Punkte im Rechteck nur zu sich selbst äquivalent.

Welche Gestalt hat $ABCD_{/\sim_{\substack{a=c\\b=d}}}$?

Was passiert, wenn man nun statt dessen c als $\overrightarrow{CD}$ definiert, also AB mit CD gleichsetzt (notfalls erst ohne BC und AD zu identifizieren)?



♡