Kapitel 2

Abbildungen und Relationen

2.1 Abbildungen

Lernziele
Definition von Abbildungen, Definitionsbereich, Wertebereich, Bild, Urbild, Faser, bijektive Abbildungen, Mächtigkeit von Mengen.

Der folgende Begriff der Abbildung ist absolut grundlegend für die gesamte Mathematik. Er formalisiert das Konzept der Zuordnung und beschreibt mögliche Vergleiche zwischen Mengen. Man ist fast versucht zu sagen, dass Mengen eigentlich erfunden wurden, um sagen zu können, was eine Abbildung ist. Aber Fakt ist, dass viele Mengen erst zusammen mit diversen Abbildungen richtig interessant werden, wie wir später noch oft sehen werden. Obwohl man viele Sachverhalte auch ohne Abbildungen beschreiben könnte, haben sich Abbildungen als das sprachliche Mittel der allerersten Wahl durchgesetzt. Wir erinnern nochmal an Definition 1.17 des kartesischen Produkts.

Definition 2.1

Seien M, N Mengen.

1) Eine **Abbildung** oder **Funktion** f von M nach N ist ein Tupel (f, M, N), wobei $f \subseteq M \times N$ eine Teilmenge des kartesischen Produktes $M \times N$ ist mit folgender Bedingung:

Für jedes $m \in M$ gibt es genau ein $n \in N$ mit $(m,n) \in f$.

Man nennt n auch das (bezüglich f) m zugeordnete Element und schreibt $n = f(m)$ statt $(m,n) \in f$.[a] Statt „$f \subseteq M \times N$ Abbildung“ schreibt man:

$$f : M \to N$$

oder ausführlicher:

$$f : M \to N : m \mapsto f(m).$$

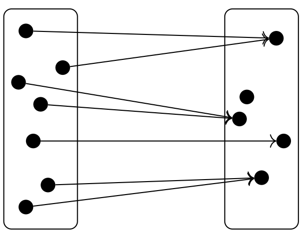
2) Ist $f : M \to N$ eine Abbildung, so heißt M der **Definitionsbereich** von f, N der **Wertebereich** und für $T \subseteq M$ heißt

$$f(T) := \{f(m) \mid m \in T\} \quad (\subseteq N)$$

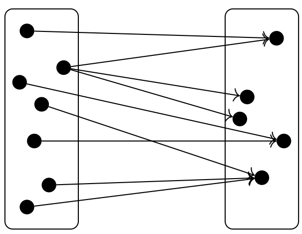
das **Bild** von T unter f, im Falle $T = M$ heißt $\mathrm{Bild}(f) := f(M)$ das **Bild** von f.

[a] Manchmal nennt man auch das, was wir als Funktion bezeichnet haben, den Graph einer Funktion und stellt sich die Funktion als Zuordnung vor.

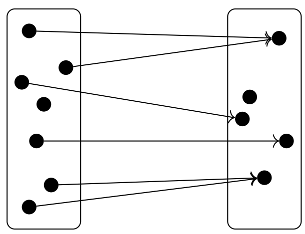
Man beachte, eigentlich sind Abbildungen über zwei Bedingungen definiert, eine Existenz- und eine Eindeutigkeitsbedingung.



Abbildung



keine Abbildung



keine Abbildung

Definition 2.2

Für Mengen M, N wird die Menge aller Abbildungen von M nach N mit N^M bezeichnet. (Also $f : M \to N$ bedeutet dasselbe wie $f \in N^M$.)

$$N^M := \{f \mid f : M \to N\}.$$

Beispiel 2.3

(a) Sei $M := N := \mathbb{R}$. Dann sind $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$ und $g : \mathbb{R} \to \mathbb{R} : x \mapsto x^3$ Abbildungen. Beide haben den Definitionsbereich $\mathbb{R}$ und Wertebereich $\mathbb{R}$. Es ist $\mathrm{Bild}(f) = \mathbb{R}_{\geq 0} = \{x \in \mathbb{R} \mid x \geq 0\}$ und $\mathrm{Bild}(g) = \mathbb{R}$. Formal ist $f = \{(x, x^2) \mid x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$ und $g = \{(x, x^3) \mid x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$.

(b) Zwei Abbildungen $f : M \to N$ und $g : L \to K$ sind gleich, wenn sie den gleichen Definitionsbereich besitzen, d.h. $M = L$, den gleichen Wertebereich besitzen, d.h. $N = K$, und für alle $m \in M = L$ gilt, dass $f(m) = g(m)$ ist.

c) Die Menge der Abbildungen $M^{\underline{n}}$ von $\underline{n}$ in M kann mit der Menge M^n der Menge der M-wertigen Folgen der Länge n identifiziert werden, indem man für jede Abbildung die Bilder angibt.

Definition 2.4

Sei $f : M \to N$ eine Abbildung.

(a) Sei $\emptyset \neq T \subseteq M$ eine Teilmenge von M. Dann heißt die Abbildung

$$f_{|T} : T \to N : t \mapsto f(t)$$

die **Einschränkung** von f auf T.

(b) Die Abbildung

$$\mathrm{Id}_M : M \to M : m \mapsto m$$

heißt die **Identitätsabbildung** oder kurz **Identität** von M.

Beispiel 2.5: (Polynomfunktion)

Eine **reelle Polynomfunktion** f ist eine Abbildung $f : \mathbb{R} \to \mathbb{R}$, für die ein $n \in \mathbb{N}$ und reelle Zahlen $a_0, a_1, \ldots, a_n$ existieren mit

$$\begin{aligned} f(x) &= a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n \\ &= a_0 + x \cdot (a_1 + x \cdot (a_2 + x \cdot (a_3 + \cdots x \cdot (a_{n-1} + x \cdot a_n) \cdots) \end{aligned}$$

für alle $x \in \mathbb{R}$. Die Umrechnung in der zweiten Zeile, die eine schnellere Berechnung der Funktionswerte ermöglicht, nennt man Horner-Schema. Z.B.

$$f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$$

ist eine Polynomfunktion, die Sie als Normalparabel kennen.

Übung 2.6. Man zeige, dass eine reelle Polynomfunktion der Form $f : \mathbb{R} \to \mathbb{R} : x \mapsto ax^2 + bx + c$ mit $a, b, c \in \mathbb{R}$ und $a \neq 0$ nur Fasern aus 0, 1 oder 2 Elementen haben kann.

Beispiel 2.7: (Rationale Funktion)

Eine **reelle rationale Funktion** f ist eine Abbildung $f : \mathbb{R} - H \to \mathbb{R}$, für die zwei Polynomfunktionen $z, h : \mathbb{R} \to \mathbb{R}$ existieren mit

$$f(x) = \frac{z(x)}{h(x)}$$

für alle $x \in \mathbb{R} - H$. Dabei ist $H := h^{-1}(\{0\})$ die Menge der Nullstellen von h. Z.B. ist

$$\mathbb{R} - \{0\} \to \mathbb{R} : x \mapsto \frac{1}{x}$$

eine rationale Funktion.

Beispiel 2.8

Sei $M := N := \mathbb{R}$. Dann ist der Kreis

$$k := \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\}$$

keine Abbildung von $M = \mathbb{R}$ nach $N = \mathbb{R}$. Erstens gibt es nicht zu jedem $x \in M$ ein $y \in N$ mit $(x, y) \in k$, z. B. nicht für $x = 2$. Diesen Übelstand kann man dadurch beheben, dass man $\mathbb{R}$ durch das abgeschlossene Intervall

$$M := [-1, 1] := \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$$

ersetzt. Zweitens existieren für jedes x mit $-1 < x < 1$ zwei $y \in N$ mit $(x, y) \in k$. Wir können diesen Übelstand auch beheben, indem wir zwei Abbildungen definieren:

$$\begin{aligned} k_1 : [-1, 1] &\to \mathbb{R}; x \mapsto \sqrt{1 - x^2} \\ k_2 : [-1, 1] &\to \mathbb{R}; x \mapsto -\sqrt{1 - x^2} \end{aligned}$$

und wir erhalten $k = k_1 \cup k_2$, wobei k_1 und k_2 Abbildungen sind, k jedoch nicht mehr. Der Definitionsbereich für beide k_i ist $M = [-1, 1]$, der Wertebereich $N = \mathbb{R}$ und die Bilder sind $k_1([-1, 1]) = [0, 1]$ und $k_2([-1, 1]) = [-1, 0]$.

Wenn man ein neues Konzept einführt, schaut man zunächst, ob alte Konzepte damit in Beziehung stehen. Wir gehen unsere bisherigen Betrachtungen durch.

Beispiel 2.9: (Aussagenlogik)

Sei $\mathcal{A}$ die Menge aller Aussagen. (Möglicherweise ist dies zu groß für eine Menge, aber es gibt sicher Möglichkeiten $\mathcal{A}$ soweit zu beschneiden, dass eine geeignete Menge dabei herauskommt.)
1.) Die Zuweisung der Wahrheitswerte ist eine Abbildung:

$$W : \mathcal{A} \to \{w, f\} : A \mapsto W(A).$$

2.) Die Verneinung ist eine Abbildung:

$$\neg : \mathcal{A} \to \mathcal{A} : A \mapsto \neg A.$$

3.) Die Konjunktion ist eine Abbildung:

$$\wedge : \mathcal{A} \times \mathcal{A} \to \mathcal{A} : (A, B) \mapsto A \wedge B.$$

(Wenn man $\mathcal{A}$ modifiziert, sollte das modifizierte $\mathcal{A}$ die Eigenschaft haben, dass mit zwei Aussagen auch ihre Konjunktion zu $\mathcal{A}$ gehört.)
4.) Die Disjunktion ist eine Abbildung:

$$\vee : \mathcal{A} \times \mathcal{A} \to \mathcal{A} : (A, B) \mapsto A \vee B.$$

(Wenn man $\mathcal{A}$ modifiziert, sollte das modifizierte $\mathcal{A}$ die Eigenschaft haben, dass mit zwei Aussagen auch ihre Disjunktion zu $\mathcal{A}$ gehört.)
5.) Entsprechendes kann man über die Implikation und die Äquivalenz sagen.
Wir sehen, dass unsere Betrachtung der Aussagenlogik nicht anderes war, als das Studium des Zusammenspiels der Abbildung W mit den Abbildungen $\neg, \wedge, \vee$. (Dieses Zusammenspiel werden wir noch besser verstehen, wenn wir den Begriff der Komposition von Abbildungen betrachtet haben.)

Das nächste Konzept, welches wir in der Sprache der Abbildungen umformulieren wollen, ist das der Teilmenge.

Bemerkung 2.10

Sei M eine Menge.
1) Jede Teilmenge $T \subseteq M$ von M legt eine Abbildung $\chi_T : M \to \{0, 1\}$ fest durch die Vorschrift: $\chi_T(m) = 1$ genau dann, wenn $m \in T$. Es heißt χ_T die **charakteristische Funktion** von T. Sie ist gegeben durch

$$\chi_T : M \to \{0, 1\} : m \mapsto \begin{cases} 1, & m \in T \\ 0, & m \notin T \end{cases}$$

2) Jede Abbildung $\alpha : M \to \{0, 1\}$ legt eine Teilmenge T von M fest, nämlich $T := \{m \in M \mid \alpha(m) = 1\}$, sodass $\alpha = \chi_T$.

Proof. Es ist nur zu zeigen, dass $\alpha = \chi_T$ gilt in 2). Wir verwenden Beispiel 2.3 2). Der Definitionsbereich von α und von χ_T ist jedesmal M, der Wertebereich ist $\{0, 1\}$. Es gilt für $m \in M$, dass $\alpha(m) = 1$ genau dann wenn $m \in T$ also genau dann wenn $\chi_T(m) = 1$ ist. Ansonsten ist $\alpha(m) = \chi_T(m) = 0$. Also stimmen die beiden Abbildungen überein. □

Die Konstruktion im zweiten Teil der Bemerkung ist von allgemeiner Bedeutung. Wir unterstreichen dies durch eine Definition:

Definition 2.11

Sei $f : M \to N$ eine Abbildung. Für $n \in N$ heißt

$$f^{-1}(\{n\}) := \{m \in M \mid f(m) = n\} \qquad (\subseteq M)$$

die **Faser** von f über n, die Faser von n, oder volles Urbild von n.
Für $T \subseteq N$ heißt

$$f^{-1}(T) := \bigcup_{t \in T} f^{-1}(\{t\}) = \{m \in M \mid f(m) \in T\} \quad (\subseteq M)$$

das **volle Urbild** von T unter f.

Beispiel 2.12

1) Sei $T \subseteq M$ und $\chi_T : M \to \{0, 1\}$ die charakteristische Funktion von T. Dann ist $\chi_T^{-1}(\{1\}) = T$ und $\chi_T^{-1}(\{0\}) = M \setminus T$.

2) Sei

$$f : \mathbb{Z} \to \{0, 1\}; n \mapsto \begin{cases} 0 & n \text{ gerade,} \\ 1 & n \text{ ungerade.} \end{cases}$$

Dann ist f die charakteristische Funktion der Teilmenge $U := \{2x+1 \mid x \in \mathbb{Z}\}$ der ungeraden ganzen Zahlen, $f^{-1}(\{1\}) = U$ und $f^{-1}(\{0\}) = \mathbb{Z} \setminus U = 2\mathbb{Z} = \{2x \mid x \in \mathbb{Z}\}$ die Teilmenge der geraden Zahlen.

Hier ist nochmals das Beispiel der Mengenfamilien in der neuen Sprache aufgegriffen:

Beispiel 2.13: (Vergl. Definition 1.26)

Eine über I indizierte Mengenfamilie $T = (T_i)_{i \in I}$ mit $T_i \subseteq M$ ist nichts anderes als eine Abbildung

$$T : I \to \mathrm{Pot}(M) : i \mapsto T_i.$$

Offenbar gilt für $\mathcal{U} := \mathrm{Bild}(T) = \{T_i \mid i \in I\} \subseteq \mathrm{Pot}(M)$:

$$\bigcap_{i\in I} T_i = \bigcap_{S\in\mathcal{U}} S \text{ und } \bigcup_{i\in I} T_i = \bigcup_{S\in\mathcal{U}} S,$$

und zwar unabhängig davon, ob einzelne Fasern von T mehr als ein Element enthalten.

Wir besprechen einen besonders wichtigen Fall von Abbildungen, wo alle Fasern einelementig sind.

Satz 2.14

Sei $f : M \to N$ eine Abbildung. Dann sind folgende Aussagen äquivalent:
1) $f^{-1} := \{(n, m) \in N \times M \mid (m, n) \in f\}$ ist eine Abbildung von N nach M, also

$$f^{-1} : N \to M.$$

2) Für jedes $n \in N$ besteht die Faser $f^{-1}(\{n\})$ von f über n aus genau einem Element von M.
Ist eine und damit auch die andere dieser Bedingungen erfüllt, so heißt f **bijektiv** oder eine **Bijektion** und $f^{-1} : N \to M$ die zu f **inverse Abbildung** oder auch **Umkehrfunktion** (die dann auch bijektiv ist).

Proof. 1) $\Rightarrow$ 2) Wir nehmen an, dass das oben definierte $f^{-1} \subseteq N \times M$ eine Abbildung von N nach M ist. Sei $n \in N$. Man verifiziert für die Faser $f^{-1}(\{n\})$ von f über n:

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

(Man beachte die unterschiedlichen Bedeutungen von f^{-1}, einmal gemäß Definition 2.11 und einmal gemäß der Definition aus Satz 2.14 1.) Die Gleichheit dieser beiden Mengen zeigt man dadurch, dass man verifiziert, dass jede der beiden Mengen in der anderen enthalten ist. (Übung).
2) $\Rightarrow$ 1) Sofort aus der Definition einer Abbildung. $\square$

2.2 Kardinalität von Mengen - Einschub (zum Selbststudium)

Lernziele

Mächtigkeit (Kardinalität von Mengen), abzählbar und überabzählbar unendlich

Zwei Mengen, zwischen denen eine bijektive Abbildung existiert, wird man anschaulich gesprochen als gleich groß ansehen.

Definition 2.15

Eine Menge M heißt **endlich**, falls eine Zahl $n \in \mathbb{Z}_{\geq 0}$ und eine Bijektion $\zeta : \underline{n} \to M$ existieren. Man schreibt $|M| = n$ und sagt M hat n Elemente, oder M hat die **Mächtigkeit** oder **Kardinalität** n. Weiter heißt ζ eine **Abzählfunktion** für M. Existiert keine Abzählfunktion, so heißt M **unendlich**.
Eine Menge M heißt **abzählbar**, falls M endlich ist oder eine Bijektion $\zeta : \mathbb{N} \to M$ existiert. Anderenfalls heißt M **überabzählbar**.

Mit dem folgenden Satz, den wir hier nicht vollständig beweisen halten wir fest: Für endliche Mengen M ist $|M|$ wohldefiniert.

Satz 2.16

Sei M eine Menge von endlichen Mengen. Dann ist

$$M \to \mathbb{Z}_{\geq 0} : X \mapsto |X|$$

eine wohldefinierte Abbildung. Insbesondere gilt $|\underline{n}| = n$ für alle $n \in \mathbb{Z}_{\geq 0}$.

Proof. Wir zeigen sehr bald, dass die Komposition injektiver (surjektiver, bijektiver) Abbildungen wieder injektiv (surjektiv, bijektiv) ist. Daraus läßt sich dann der Beweis der Aussage reduzieren auf die Aussage: ist $\alpha : \underline{n} \to \underline{m}$ bijektiv für $n, m \in \mathbb{N}$, so folgt $n = m$. □

Korrolar 2.17

Seien M, N endliche Mengen. Dann gilt:
1.) Sind M, N **disjunkt**, d. h. $M \cap N = \emptyset$, dann gilt

$$|M \cup N| = |M| + |N|.$$

2.) Allgemein gilt

$$|M \cup N| = |M| + |N| - |M \cap N|,$$

was man auch oft schreibt als

$$|M \cup N| + |M \cap N| = |M| + |N|.$$

3.)
$$|M \times N| = |M| \cdot |N|.$$

Proof. 1.) Bei Vereinigungen von paarweise disjunkten Mengen benutzen wir das Symbol $\uplus$ statt $\cup$. Wir wollen also zeigen $|M \uplus N| = |M| + |N|$. Zu diesem Zweck seien $\alpha : \underline{|M|} \to M$ und $\beta : \underline{|N|} \to N$ Bijektionen. Dann ist

$$\gamma : \underline{|M| + |N|} \to M \uplus N : i \mapsto \begin{cases} \alpha(i) & i \in \underline{|M|} \\ \beta(i - |M|) & i \notin \underline{|M|} \end{cases}$$

auch eine Bijektion (Nachweis Übung), was die Behauptung zeigt. (Frage: Wo und wie ist Satz 2.16 eingegangen?)
2.) Wir haben:

$$\begin{aligned} M &= (M - N) \uplus (M \cap N) \\ N &= (N - M) \uplus (M \cap N) \\ M \cup N &= (M - N) \uplus (M \cap N) \uplus (N - M) \end{aligned}$$

und bekommen nach 1.):

$$\begin{aligned} |M| &= |M - N| + |M \cap N| \\ |N| &= |N - M| + |M \cap N| \\ |M \cup N| &= |M - N| + |M \cap N| + |N - M|. \end{aligned}$$

Zieht man die Summe der ersten beiden Gleichungen von der dritten ab, so steht die Behauptung da.
3.) Wir lassen es als Übungsaufgabe, eine entsprechende Abzählung anzugeben. □

Hier sind zwei Beispiele für zwei abzählbar unendliche Mengen.

Satz 2.18

$\mathbb{Z}$ und $\mathbb{N} \times \mathbb{N}$ sind abzählbar unendlich.

Proof. Dass beide Mengen unendlich sind, ist klar. Wir zeigen nur, dass sie abzählbar sind.
Definiere $\zeta : \mathbb{N} \to \mathbb{Z}$ durch

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

Dann ist ζ eine Bijektion. Die Umkehrabbildung ist gegeben durch

$$\eta : \mathbb{Z} \to \mathbb{N} : z \mapsto \begin{cases} -2z+1 & \text{falls } z \leq 0 \\ 2z & \text{falls } z > 0. \end{cases}$$

Da beides offenbar Abbildungen sind, muss also nur noch für alle $n \in \mathbb{N}$ und alle $z \in \mathbb{Z}$ die Äquivalenz

$$n = \eta(z) \Leftrightarrow z = \zeta(n)$$

gezeigt werden, was wir als Übung lassen.
Für $\mathbb{N} \times \mathbb{N}$ ist dies schon etwas trickreicher und beruht auf dem ersten **Cantorschen Diagonalverfahren.** Man stellt sich $\mathbb{N} \times \mathbb{N}$ als nach rechts und unten unendliches Rechteck vor. Für jedes $n \in \mathbb{N}$ haben wir dann eine “Diagonale”

$$D(n) := \{(a,b) \in \mathbb{N} \times \mathbb{N} | a+b-1 = n\} = \{(1,n), (2,n-1), \ldots, (n,1)\},$$

die aus genau n Elementen besteht. Dann liegt $(a,b) \in \mathbb{N} \times \mathbb{N}$ auf der Diagonalen $D(a+b-1)$ an der a-ten Stelle, sodass sich für (a,b) in der Abzählung die Nummer

$$(\sum_{n=1}^{a+b-2} n) + a = (a+b-1)(a+b-2)/2 + a$$

anbietet. Die Abbildung

$$\alpha : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (a, b) \mapsto (a + b - 1)(a + b - 2)/2 + a$$

ist die Umkehrabbildung der gewünschten Bijektion. $\square$

2.3 Komposition von Abbildungen.

Lernziele

Komposition von Abbildungen, injektive Abbildungen und Linksinverse, surjektive Abbildungen und Rechtsinverse, Charakterisierung endlicher Mengen.

Wir wollen jetzt etwas mit den Abbildungen machen: Abbildungen in andere Abbildungen einsetzen.

Lemma 2.19

Sind $f : S \to T$ und $g : T \to U$ Abbildungen, so ist

$$g \circ f := \left\{ (s, u) \in S \times U \;\middle|\; \begin{array}{c} \text{es existiert ein } t \in T \text{ mit} \\ (s, t) \in f \text{ und } (t, u) \in g \end{array} \right\}$$

eine Abbildung von S nach U: $g \circ f : S \to U$.

Proof. $g \circ f \subseteq S \times U$ ist klar. Sei $s \in S$. Dann existiert ein $t \in T$ mit $(s, t) \in f$, nämlich $t = f(s)$. Da g auch Abbildung ist, existiert auch ein $u \in U$ mit $(t, u) \in g$, nämlich $u = g(t)$. Also ist $(s, u) \in g \circ f$. (Damit ist die Existenz des Bildes verifiziert, jetzt kommt die Eindeutigkeit:) Seien $(s, u), (s, u') \in g \circ f$. Dann gibt es $t \in T$ mit $(s, t) \in f, (t, u) \in g$ und $t' \in T$ mit $(s, t') \in f, (t', u') \in g$. Da f Abbildung ist, folgt $t = t'$. Also folgt jetzt, da g Abbildung ist, $u = u'$. $\square$

Definition 2.20

Die in Lemma 2.19 definierte Abbildung

$$g \circ f : S \to U : s \mapsto g(f(s))$$

heißt die **Komposition** (Hintereinanderausführung) von f mit g.

Beispiel 2.21

1) Ist $f : M \to N$ eine Abbildung und $\emptyset \neq T \subseteq M$ eine Teilmenge mit zugehöriger Einbettung $\iota : T \to M : t \mapsto t$, so gilt für die Einschränkung von f auf T

$$f_{|T} = f \circ \iota.$$

2.) Ist $f : M \to N$ eine bijektive Abbildung, so gilt

$$f \circ f^{-1} = \mathrm{Id}_N \text{ und } f^{-1} \circ f = \mathrm{Id}_M .$$

Eine absolut grundlegende Eigenschaft der Komposition ist die Assoziativität. Der folgende Satz ist zwar sehr einfach zu beweisen, jedoch grundlegend für die gesamte Gruppentheorie und vieles andere in der Mathematik.

Satz 2.22

(**Assoziativität** der Komposition von Abbildungen) Sind $f : A \to B$, $g : B \to C$, $h : C \to D$ Abbildungen, so gilt

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

(Man beachte, $h \circ g : B \to D$ und $g \circ f : A \to C$, so dass alle Kompositionen auf beiden Seiten der Gleichung wohldefinierte Abbildungen von A nach D sind.)

Proof. Sei $a \in A$. Dann gilt: einerseits

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

und andererseits

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

$\square$

Übung 2.23. Sei $g : M \to N$ eine bijektive Abbildung. Man zeige:

$$\overline{g} : M^M \to N^N : f \mapsto g \circ f \circ g^{-1}$$

ist eine Bijektion.

Wir hatten gesagt, eine Abbildung ist genau dann bijektiv, wenn die Faser über jedem Element des Wertebereiches genau ein Element hat. Dies kann man auf zwei Arten abschwächen.

Definition 2.24

Sei $f : M \to N$ eine Abbildung.
1) f heißt **injektiv** oder **eineindeutig**, falls jede Faser von f aus höchstens einem Element besteht, d. h., zu jedem $n \in N$ existiert höchstens ein $m \in M$ mit $f(m) = n$.
2) f heißt **surjektiv** oder eine Abbildung **auf** N, falls keine Faser von f leer ist, d. h. zu jedem $n \in N$ existiert mindestens ein $m \in M$ mit $f(m) = n$, mit anderen Worten: $\text{Bild}(f) = N$.

Beispiel 2.25

1) Sei $T \subseteq M$ eine Teilmenge von M. Dann ist die Einbettung

$$\iota_T : T \to M : t \mapsto t$$

injektiv (oder eine Injektion).
2) Sei M eine nicht leere endliche Menge. Dann ist

$$|\ | : \text{Pot}(M) \to \{0, 1, \dots, |M|\} : T \mapsto |T|$$

eine surjektive Abbildung, die für $|M| > 1$ nicht bijektiv ist. Die Faser von α über n , $0 \leq n \leq |M|$ besteht aus allen n-elementigen Teilmengen von M.

Bijektive Abbildungen $f : M \to N$ waren dadurch gekennzeichnet, dass $f^{-1} : N \to M$ eine Abbildung war. Es gilt dann $f^{-1} \circ f = \mathrm{Id}_M$ und $f \circ f^{-1} = \mathrm{Id}_N$. Hier ist eine Charakterisierung von injektiven und von surjektiven Abbildungen.

Satz 2.26

Sei $f : M \to N$ eine Abbildung. Es gilt:
1) f ist genau dann injektiv, wenn eine Abbildung $g : N \to M$ mit $g \circ f = \mathrm{Id}_M$ existiert. Jedes derartige g ist surjektiv und heißt auch **Linksinverses** von f.
2) f ist genau dann surjektiv, wenn eine Abbildung $\gamma : N \to M$ mit $f \circ \gamma = \mathrm{Id}_N$ existiert. Jedes derartige γ ist injektiv und heißt auch **Rechtsinverses** von f.

Proof. 1) Angenommen, f injektiv. Für $n \in N$ mit $n \in f(M)$ existiert ein eindeutiges $m \in M$ mit $f(m) = n$, da f injektiv ist. Wir definieren $g(n) := m$. Für $n \in N$ mit $n \notin f(M)$ wähle ein beliebiges $m \in M$ und setze $g(n) := m$. Klar: g ist Abbildung von N nach M und $g \circ f = \mathrm{Id}_M$.
Angenommen $g : N \to M$ ist ein Linksinverses von f, d. h. $g \circ f = \mathrm{Id}_M$. Sind $m, m' \in M$ mit $f(m) = f(m')$, so gilt

$$\begin{aligned} m &= \mathrm{Id}_M(m) \\ &= g(f(m)) \\ &= g(f(m')) \\ &= m', \end{aligned}$$

d. h. f ist injektiv.
Sei nun $g : N \to M$ eine beliebige Abbildung mit $g \circ f = \mathrm{Id}_M$. Behauptung: g ist surjektiv. Bew.: Sei $m \in M$, dann gilt $m = \mathrm{Id}_M(m) = g(f(m))$, d. h. $m \in g(N)$. Da $m \in M$ beliebig vorgegeben war, ist somit g surjektiv.
2) Übung. (Hinweis: Wähle aus jeder Faser von f ein Element aus.) $\square$

Beispiel 2.27

Im Allgemeinen sind Links- und Rechtsinverse nicht eindeutig bestimmt.
1,) Die Funktion $f : \mathbb{Z} \to \mathbb{Z} : a \mapsto 2a$, ist injektiv, hat also ein Linksinverses, z.B.

$$g : \mathbb{Z} \to \mathbb{Z} : a \mapsto \begin{cases} a & \text{falls a ungerade ist} \\ a/2 & \text{falls a gerade ist.} \end{cases}$$

Jedoch kann man die ungeraden Zahlen (die ja nicht im Bild der Funktion f sind), auf beliebige ganze Zahlen abbilden. Eine andere Linksinverse wäre z.B.

$$g : \mathbb{Z} \to \mathbb{Z} : a \mapsto \begin{cases} (a-1)/2 & \text{falls a ungerade ist} \\ a/2 & \text{falls a gerade ist.} \end{cases}$$

2.) Ein Rechtsinverses der Funktion $f : \mathbb{R} \to \mathbb{R}_{\geq 0} : x \mapsto x^2$ ist $g : \mathbb{R}_{\geq 0} \to \mathbb{R} : y \mapsto \sqrt{y}$.

Korrolar 2.28

Eine Abbildung ist genau dann bijektiv, wenn sie injektiv und surjektiv ist. In dem Fall ist die Umkehrabbildung das eindeutig bestimmte Links- und Rechtsinverse.

2.4 Partitionen und Äquivalenzrelationen.

Lernziele

Relationen als Teilmengen kartesischer Produkte, Äquivalenzrelationen und Partitionen, Gleichwertigkeit der beiden Begriffe und inhaltliche Ausdeutung, enger Zusammenhang mit Abbildungen.

Relationen in ihrer allgemeinen Form verallgemeinern den Funktionsbegriff: Sie sind einfach Teilmengen eines kartesischen Produktes. Wir beschränken uns auf Relationen auf einer Menge, die dann bestimmte Beziehungen der Elemente der Menge untereinander modellieren sollen. Der wichtigste Begriff ist der der Äquivalenzrelation, der den Gleichheitsbegriff abschwächt und den Begriff der "Gleichheit unter einem bestimmten Gesichtspunkt" formalisiert.

Definition 2.29

Sei M eine Menge.

1) Eine **Relation** R auf M ist eine Teilmenge von $M \times M$. Statt $(m, n) \in R$ schreibt man auch mRn und sagt, m steht in Relation R zu n.

2) Eine Relation R auf M heißt **reflexiv**, falls mRm gilt für alle $m \in M$.

3) Eine Relation R auf M heißt **symmetrisch**, falls mRn immer nRm für alle $m, n \in M$ impliziert.

4) Eine Relation R auf M heißt **transitiv**, falls aus mRn und nRo stets mRo für alle $m, n, o \in M$ folgt.

5) Eine reflexive, symmetrische und transitive Relation R auf M heißt **Äquivalenzrelation**. Statt mRn sagt man auch m und n sind (bezüglich R) äquivalent.

6) Ist R eine Äquivalenzrelation auf M und $m \in M$, so bezeichnet

$$[m]_R := \{n \in M \mid nRm\}$$

die **Äquivalenzklasse** von m.

Nun betrachten wir einige Beispiele.

Beispiel 2.30

1) $\leq$ ist eine Relation auf $\mathbb{R}$, die auch auf der Zahlengeraden visualisiert werden kann. Die Relation $\leq$ ist reflexiv (im Unterschied zu $<$), nicht symmetrisch, allerdings antisymmetrisch und transitiv. Insbesondere ist $\leq$ keine Äquivalenzrelation. Gleiches gilt für die Relation $\geq$ auf $\mathbb{R}$. Nun definieren wir die Relation $=$ als den Durchschnitt von $\leq$ und $\geq$. Dann ist $=$ eine Äquivalenzrelation.

2) Für $n \in \mathbb{N}$ ist $\subseteq$ reflexiv und transitiv, aber nicht symmetrisch auf $\mathrm{Pot}(\underline{n})$. (Es ist sogar eine partielle Ordnung.)

3) $R := M \times M$ ist eine Äquivalenzrelation auf M.

4) $\emptyset \subseteq M \times M$ ist symmetrisch, transitiv, aber nicht reflexiv.

5) Sei M eine Menge von Aussagen. Dann ist $\Leftrightarrow$ eine Äquivalenzrelation auf M.

6) Sei $M := \{G_{a,b} \mid a, b \in \mathbb{R}\}$ wobei $G_{a,b} := \{(x, ax + b) \mid x \in \mathbb{R}\}$ die Gerade durch $(0, b)$ mit Steigung a sei. Dann ist Parallelität von Geraden eine Äquivalenzrelation auf M, $G_{a,b} \sim G_{c,d}$ genau dann wenn $a = c$.

Die nächsten Beispiele helfen uns die obigen besser zu verstehen.

Beispiel 2.31

1) Sei $\Gamma : M \to N$ eine Abbildung. Dann ist $\sim_\Gamma \subseteq M \times M$ definiert durch $m \sim_\Gamma m'$ genau dann, wenn $\Gamma(m) = \Gamma(m')$, eine Äquivalenzrelation. Die Äquivalenzrelation $\sim_\Gamma$ heißt **Bildgleichheit** bezüglich Γ. Die Äquivalenzklassen sind genau die nichtleeren Fasern der Abbildung Γ.
Z. B. sind für $M := \mathbb{R}^2$ und $\Gamma : \mathbb{R}^2 \to \mathbb{R} : (x, y) \mapsto x - y$ oder $\Gamma : \mathbb{R}^2 \to \mathbb{R} : (x, y) \mapsto x^2 + y^2$ sehr anschauliche Beispiele.
Auch die vier Äquivalenzrelationen aus Beispiel 2.30 kann man von hierher sehr klar verstehen:

Bei 1) mit Gleichheit als Äquivalenzrelation wähle $\Gamma := \mathrm{Id}_{\mathbb{R}}$,

Bei 3) wähle eine konstante Funktion $\Gamma := \kappa_a : M \to \{a\}$.

Bei 5) wähle $\Gamma := W : M \to \{0, 1\}$ als die Wahrheitsfunktion.

Bei 6) wähle $\Gamma : M \to \mathbb{R} : G_{a,b} \mapsto a$ als die Steigung.

2) Sei $M = \mathbb{Z}$ und $n \in \mathbb{N}$. Die Abbildung $\mu_n : \mathbb{Z} \to \{0, \dots, n-1\}$ definiert durch $\mu_n(z) := r$ falls

$$z = qn + r \text{ für ein } q \in \mathbb{Z} \text{ und } r \in \{0, \dots, n-1\}$$

ist, liefert uns eine Äquivalenzrelation auf $\mathbb{Z}$: Zwei Zahlen $a, b \in \mathbb{Z}$ heißen **kongruent modulo n**, in Zeichen $a \equiv_n b$ oder $a \equiv b \pmod{n}$, genau dann wenn $\mu_n(a) = \mu_n(b)$ also genau dann wenn $a - b$ durch n teilbar ist.

Äquivalenzrelationen sind inhaltlich, jedoch nicht formal dasselbe wie Partitionen, also Aufteilungen einer Mengen.

Definition 2.32

Sei M eine Menge.

a) Zwei Teilmengen X, Y von M heißen **disjunkt**, falls $X \cap Y = \emptyset$.

b) Eine **Partition** P von M ist eine Menge von nicht leeren Teilmengen von M, also $P \subseteq \mathrm{Pot}(M)$, $X \neq \emptyset$ für alle $X \in P$, mit

$$\text{a) } M = \bigcup_{X \in P} X \text{ und b) } X \cap Y = \emptyset \text{ für alle } X, Y \in P, X \neq Y.$$

Also ist M die disjunkte Vereinigung der Mengen aus P und man schreibt diese beiden Bedingungen kurz so:

$$M = \biguplus_{X \in P} X$$

c) Sei P eine Partition auf M. Die Elemente von P heißen auch **Klassen**. Ist X eine Klasse, so nennt man ein Element von X auch **Vertreter** der Klasse. Eine Teilmenge von M, die aus jeder

Klasse von P genau einen Vertreter enthält, nennt man auch **Vertretermenge** oder **Transversale**. Eine Abbildung $v : P \to M$ mit $v(X) \in X$ für alle $X \in P$ heißt **Vertreterabbildung** oder auch **Transversale**.

Ist P eine Partition von M, so gehört jedes Element von M zu genau einem $X \in P$, d. h.

$$f_P : M \to P : m \mapsto X \in P \text{ mit } m \in X$$

ist eine Abbildung, genannt die **natürliche Abbildung** zu P. Hier ist der Zusammenhang zwischen Äquivalenzrelationen und Partitionen.

Satz 2.33

Sei M eine Menge.

1) Ist $\sim$ eine Äquivalenzrelation auf M, so bilden **Äquivalenzklassen** definiert durch

$$[m_0] := [m_0]_\sim := \{m \in M \mid m \sim m_0\}$$

für $m_0 \in M$ eine Partition von M. Diese wird üblicherweise mit $M/\sim$ bezeichnet.

2) Ist P eine Partition von M, so ist $\sim_P$ definiert durch $m \sim_P n$ genau dann, wenn ein $X \in P$ existiert mit $m \in X$ und $n \in X$ eine Äquivalenzrelation.

3) Es gilt $M/\sim_P = P$ für alle Partitionen P von M und $\sim_{(M/\sim)} = \sim$ für jede Äquivalenzrelation $\sim$ auf M.

Proof. 1) Sei $P := M/\sim = \{[m]_\sim \mid m \in M\}$. Zu zeigen: P ist eine Partition von M.

- $\emptyset \notin P$, da jede Äquivalenzklasse $[m]_\sim$ sicherlich das Element $m \in M$ enthält (da $\sim$ reflexiv ist).
- $\bigcup_{X \in P} X = M$, da jedes $m \in M$ in seiner Äquivalenzklasse $m \in [m]_\sim \in P$ liegt.
- Die wichtigste Eigenschaft ist

Zwei Äquivalenzklassen sind entweder disjunkt oder gleich.

Dazu seien $a, b \in M$ mit $[a]_\sim \cap [b]_\sim \neq \emptyset$. Wir müssen zeigen, dass dann $[a]_\sim = [b]_\sim$ gilt. Dazu sei $c \in [a]_\sim \cap [b]_\sim$. Dann gilt $c \sim a$ und $c \sim b$, also auch $a \sim c$ und $c \sim b$ (Symmetrie) und wegen der Transitivität damit auch $a \sim b$.
Zeigen nur $[a]_\sim \subseteq [b]_\sim$, die Umkehrung geht dann genauso und insgesamt ergibt sich die Gleichheit der beiden Äquivalenzklassen.
Dazu sei $d \in [a]_\sim$. Dann ist $d \sim a$ und wegen $a \sim b$ und der Transitivität gilt dann auch $d \sim b$ und somit $d \in [b]_\sim$.
2) Übung.
3) Sei P eine Partition auf M. Dann ist $M/\!\sim_P = \{[m]_{\sim_P} \mid m \in M\}$. Um zu zeigen, dass diese Partition wieder gleich P ist, bemerken wir, dass

$$[m]_{\sim_P} = \{n \in M \mid \text{ es gibt ein } X \in P \text{ mit } m \in X \text{ und } n \in X\}$$

genau das Element X von P ist, welches m enthält. Also ist

$$M/\!\sim_P = \{X \mid X \in P\} = P.$$

Sei andererseits $\sim$ eine Äquivalenzrelation auf M. Für jedes Paar $m, n \in M$ müssen wir zeigen, dass $m \sim n$ genau dann, wenn $m \sim_{(M/\sim)} n$ gilt. Beides heißt aber, dass m und n zu derselben Menge von $M/\!\sim$ gehören. □

Zur Philosophie von $M/\!\sim$ sei gesagt: Per Definition ist dies zwar eine Partition der Menge M, aber die Idee ist, die Elemente von $M/\!\sim$ nicht als Teilmengen von M anzusehen, sondern als Elemente einer neuen Menge.

Satz 2.34

(1) Es sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Dann gibt es eine Menge P und eine surjektive Abbildung $\Gamma : M \to P$, sodass $\sim = \sim_\Gamma$. Jede Äquivalenzrelation ist also Bildgleichheit unter einer surjektiven Abbildung.

(2) Ist $\Gamma : M \to N$ eine surjektive Abbildung und $P := M/\sim_\Gamma$ die zur Bildgleichheit gehörige Partition, so ist $f : P \to N : [m]_{\sim_\Gamma} \mapsto \Gamma(m)$ eine wohldefinierte Bijektion.

(3) Sind $\Gamma_1 : M \to P_1$ und $\Gamma_2 : M \to P_2$ zwei surjektive Abbildungen, so gilt $\sim_{\Gamma_1} = \sim_{\Gamma_2}$ genau dann, wenn eine Bijektion $f : P_1 \to P_2$ existiert mit $\Gamma_2 = f \circ \Gamma_1$.

Proof. (1) Sei $P := M/\sim$ die Menge aller Äquivalenzklassen und definiere $\Gamma : M \to P : m \mapsto [m]_\sim$. Dann ist Γ surjektiv und die Fasern von Γ sind genau die Äquivalenzklassen von $\sim$.
(2) Wohldefiniertheit: Sei $[m_1] = [m_2]$. Dann ist aber auch $\Gamma(m_1) = \Gamma(m_2)$ und damit das Bild von $[m]$ unter f unabhängig von der Wahl des Vertreters m. Die Abbildung f ist injektiv, denn

$$f([m_1]) = f([m_2]) \Leftrightarrow \Gamma(m_1) = \Gamma(m_2) \Leftrightarrow [m_1] = [m_2].$$

Außerdem ist f surjektiv, da Γ surjektiv ist.
(3) Übung. $\square$

Übung 2.35. Wieviele dreiklassige Äquivalenzrelationen gibt es auf $\underline{7}$? (Hinweis: Benutze den letzten Satz und zähle zuerst die surjektiven Abbildungen $\underline{7} \to \underline{3}$. Wieviele von diesen ergeben dieselbe Äquivalenzrelation auf $\underline{7}$? Suche auch alternative Möglichkeiten des Zählens.)

Bemerkung 2.36. Ist $f : M \to N$ eine Abbildung, so ist

$$\{f^{-1}(\{n\}) \mid n \in f(M)\}$$

die Partition zur Äquivalenzrelation Bildgleichheit $\sim_f$, d. h.

$$M/\sim_f = \{f^{-1}(\{n\}) \mid n \in f(M)\}$$

Jetzt sollte klar sein, dass vom Prinzip her Äquivalenzrelationen, Partitionen und Abbildungen sehr ähnliche Konzepte sind. Man könnte fast sagen, die gleichen Konzepte in verschiedenen Sprachen. Es folgt das Hauptergebnis.

Satz 2.37: Homomorphiesatz für Mengen

Sei $f : M \to N$ eine Abbildung. Dann faktorisiert f als $f = \overline{f} \circ \nu_f$ mit ν_f surjektiv und $\overline{f}$ injektiv, wo

$$\nu_f : M \to M/{\sim_f} : m \mapsto f^{-1}(\{f(m)\})$$

die natürliche Abbildung von $\sim_f$ ist, und $\overline{f}$ durch

$$\overline{f} : M/{\sim_f} \to N : f^{-1}(\{f(m)\}) \mapsto f(m)$$

definiert ist. Statt $f = \overline{f} \circ \nu_f$ sagt man auch, man hat ein kommutatives Diagramm

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, "\nu_f"'] & & N \\ & M/{\sim_f} \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

Hier ist ein Beispiel der Philosophie dieses Satzes aus einem Bereich des mehr alltäglichen Lebens. Die Post hat von Aachen aus viele Briefe zu verschicken. Die Zuordnung der Briefe zu ihren Bestimmungsorten fassen wir als Abbildung f auf. Die Erfahrung hat der Post gelehrt, daß es viel besser ist, die Briefe erst zu sortieren und in Säcken nach Bestimmungsorten zusammenzustellen, bevor man sie in die einzelnen Städte bringt. Dem Zusammenstellen in Säcke entspricht die natürliche Abbildung ν_f. Man beachte, dieser Vorgang findet noch in Aachen statt. Das Verschicken der Säcke ist dann die Abbildung $\overline{f}$, die sich dann nicht mehr ganz so mühsam wie f gestaltet. Hätte man nicht jeden Sack schon mit dem Bestimmungsort beschriftet, brauchte man nur einen Brief in dem Sack anzusehen und wüßte dann schon, wo der ganze Sack hinkommt. Dies ist die Art und Weise, wie wir $\overline{f}$ definiert haben.

Proof. (von 4.42) 1) Klar: ν_f ist eine wohldefinierte surjektive Abbildung.
2) Zeige: $\overline{f}$ ist wohldefiniert, d. h. $f^{-1}(\{f(m)\}) = f^{-1}(\{f(m')\})$ für zwei $m, m' \in M$, impliziert dass $\overline{f}(f^{-1}(\{f(m)\})) = \overline{f}(f^{-1}(\{f(m')\}))$. Man sagt auch, dass man die Unabhängigkeit vom Vertreter der Abbildung nachweist. Aber $f^{-1}(\{f(m)\}) = f^{-1}(\{f(m')\})$ bedeutet nach Definition von Abbildungen, dass $f(m) = f(m')$ gilt, d. h. der Wert ist wohldefiniert und hängt nicht von der Wahl des Vertreters ab.
Zeige: $\overline{f}$ ist injektiv: Übung.
3) Zeige: $f = \overline{f} \circ \nu_f$. Dies folgt sofort aus der Definition der beiden Abbildungen. □

Wir haben gesehen, dass zwar etwas zu beweisen war, der Beweis aber recht einfach wurde, nachdem man sich klargemacht hatte, was überhaupt zu zeigen war. Trotzdem ist der Satz sehr wichtig, denn er sagt uns, dass wir bis zu einem gewissen Grad die Abbildungen einer Menge M in beliebige Mengen einzig und allein durch das Studium der Partitionen von M überblicken können. Lediglich das Problem der Namensgebung für die Klassen der Partitionen, also $\overline{f}$ bleibt offen.

Beispiel 2.38

1) Sei $f : \mathbb{R}^2 \to \mathbb{R} : (x, y) \mapsto \sqrt{x^2 + y^2}$. Die Fasern sind Kreise mit Mittelpunkt $(0, 0)$, also ordnet ν_f jedem Punkt den Kreis zu, auf dem er liegt und $\overline{f}$ ordnet dem Kreis seinen Radius zu.
2) Sei $f : \mathbb{R}^2 \to \mathbb{R} : (x, y) \mapsto x + y$. Die Fasern der Abbildung sind Geraden parallel zu der Gerade mit der Gleichung $y = -x$. Also ν_f stellt fest, auf welcher Gerade der Punkt liegt und $\overline{f}$ identifiziert jede dieser Geraden mit dem Schnittpunkt der x-Achse mit der Geraden.
3) Sei $f : \mathbb{Z} \to \{0, 1\} : x \mapsto x \bmod 2$. Die Fasern dieser Abbildung sind die Mengen der geraden bzw. der ungeraden Zahlen. Also ν_f

stellt fest, zu welcher dieser beiden Mengen eine Zahl gehört und $\overline{f}$ identifiziert jede dieser Mengen mit einem der Standardvertreter.

4) Ist M eine Menge und $P' \subset \mathrm{Pot}(M)$ eine endliche Teilmenge der Potenzmenge der Gestalt $\{A_1, B_1 := M - A_1, A_2, B_2 := M - A_2, \ldots, A_n, B_n := M - A_n\}$, wobei keine Menge mehrfach aufgezählt sein soll. Für $m \in M$ sei

$$[m] := \bigcap_{m \in X \in P'} X.$$

Dann ist $P := \{[x] \mid x \in M\}$ eine Partition von M. Weiter gilt $|P| \leq 2^n$.

Alle diese Aussagen werden unter Benutzung der folgenden Abbildung sofort klar:

$$\xi : M \to \{0,1\}^n : m \mapsto (\chi_{A_1}(m), \chi_{A_2}(m), \ldots, \chi_{A_n}(m))$$

Der Hauptsatz wird auch schon einmal Homomorphiesatz für Mengen genannt. Dies deutet an, dass er erst dann richtig interessant wird, wenn M und N Strukturen tragen, die von f respektiert werden. Dann geht es darum, diese Strukturen auch in den restlichen Konstruktionen wiederzufinden. Zwei Beispiele, sollen das verdeutlichen, um unsere spätere Thematik vorzubereiten.

Beispiel 2.39

Wir greifen die Abbildung $f : \mathbb{Z} \to \{0,1\} : x \mapsto x \bmod 2$ von oben auf und stellen fest, dass die zugehörige Äquivalenzrelation mit der Addition und Multiplikation in den ganzen Zahlen verträglich ist: "ungerade mal ungerade ist ungerade " etc. . Dies erlaubt es uns, auf der Menge $\mathbb{Z}/2\mathbb{Z}$ der Äquivalenzklassen wieder eine wohldefinierte Addition und Multiplikation zu haben. Dies ist der berühmte Körper von zwei Elementen, den wir noch genauer betrachten werden.

Wir halten fest, dass man den Homomorphiesatz von Mengen auch einfach so aussprechen kann: Jede Abbildung kann als Komposition einer injektiven gefolgt von einer surjektiven Abbildung dargestellt werden.

Historisch war der Übergang von den natürlichen Zahlen $1, 2, 3, \ldots$ zu den ganzen Zahlen, wo noch $0, -1, -2, \ldots$ hinzukamen, ein recht langwieriger Prozess. Wie kann man diesen ausdrücken durch die gerade einführten Konzepte? Wir nehmen an, wir kennen $\mathbb{N}$, d. h. wir gehen von den natürlichen Zahlen aus.

Beispiel 2.40

Wir betrachten Gleichungen der Form $x + n = m$ mit $n, m \in \mathbb{N}$. Da diese Gleichungen u. U. unterschiedliche Lösungen haben, führen wir statt x die Unbekannte $x_{(m,n)}$ ein: $x_{(m,n)}+n = m$. Während $x_{(2,1)}+1 = 2$ durchaus eine Lösung in $\mathbb{N}$ hat, nämlich 1, hat $x_{(1,2)} + 2 = 1$ öffenbar keine Lösung in $\mathbb{N}$. Also $\mathbb{N}$ ist zu klein, um all diese Gleichungen zu lösen. Wie kommt man an einen größeren Bereich, wo all diese Gleichungen Lösungen haben?
Selbstverständlich sollten $x_{(m,n)} + n = m$ und $x_{(m+k,n+k)} + n + k = m + k$ für beliebige $k \in \mathbb{N}$ dieselben Lösungen haben. Allgemeiner: $x_{(m,n)} + n = m$ und $x_{(m',n')} + n' = m'$ sollten dieselbe Lösung haben, wenn $n + m' = n' + m$.
Folgende Idee drängt sich auf: Der größere Bereich ist zu definieren als

$$\tilde{\mathbb{Z}} := \mathbb{N} \times \mathbb{N}/\sim \ \text{ mit } (m, n) \sim (m', n') \Leftrightarrow n + m' = n' + m$$

Jetzt ist einiges zu überlegen:
1.) Wie finden wir $\mathbb{N}$ in $\tilde{\mathbb{Z}}$ wieder? Antwort:

$$\nu : \mathbb{N} \to \tilde{\mathbb{Z}} : n \mapsto [(n + 1, 1)]_\sim$$

ist injektiv (Beweis später) (ν wie natürliche Einbettung), also wir identifizieren $n \in \mathbb{N}$ mit $[(n + 1, 1)]_\sim \in \tilde{\mathbb{Z}}$.
2.) Wie addiert man in $\tilde{\mathbb{Z}}$, sodass sich die Addition von $\mathbb{N}$ fortsetzt und andererseits $[(m, n)]_\sim$ eine Lösung von $x_{(m,n)} + n = m$ ist? Genauer:
a) $\nu(a) + \nu(b) = \nu(a + b)$ für alle $a, b \in \mathbb{N}$ und
b) $[(m, n)]_\sim + \nu(n) = \nu(m)$ für alle $m, n \in \mathbb{N}$.

Antwort:

$$+ : \tilde{\mathbb{Z}} \times \tilde{\mathbb{Z}} \to \tilde{\mathbb{Z}} : ([(m,n)]_\sim, [(s,t)]_\sim) \mapsto [(m+s, n+t)]_\sim$$

ist wohldefiniert, also vertreterunabhängig, und erfüllt a) und b). (Beweis später).
Wir sehen sehr leicht, dass $\tilde{\mathbb{Z}}$ gegeben ist durch

$$\ldots, -2 := [(1,3)]_\sim, -1 := [(1,2)]_\sim, 0 := [(1,1)]_\sim,$$
$$1 := [(2,1)]_\sim, 2 := [(3,1)]_\sim, \ldots$$

Mit anderen Worten ganze Zahlen sind nichts anderes als Äquivalenzklassen von Gleichungen, wie wir sie oben sahen.

Übung 2.41. Wir nehmen an, dass $\mathbb{N}$ und $\mathbb{Z}$ bereits bekannt sind. Betrachte

$$- : \mathbb{N} \times \mathbb{N} \to \mathbb{Z} : (m,n) \mapsto m - n.$$

Zeige, dass Bildgleichheit bezüglich $-$ die Äquivalenzrelation $\sim$ aus Beispiel 2.40 ist. Benutze dies, um einen Vorschlag für die Multiplikation in $\tilde{\mathbb{Z}}$ zu machen.