(Frank Lübeck)

Abbildungen (oder Funktionen) (M, N, f)

M, N Mengen, $f \subseteq M \times N$ Abb. $:\Leftrightarrow$

für jedes $x \in M$ gibt es genau ein $(x', y) \in f$ mit $x' = x$.

$\Leftrightarrow$ " genau ein $y \in N$ mit $(x, y) \in f$.

Schreibweisen: $f : M \to N$ (Abb. f von M nach N)

$M \ni x \mapsto f(x) \in N$, wenn $(x, f(x)) \in f$

oder: $M \xrightarrow{f} N$

M: Definitionsbereich von f

N: Wertebereich von f

$\underline{n} := \{1, 2, \dots, n\}$

$n \in \mathbb{N}$, M Menge

<u>n-Tupel in M</u> = Element von $M^{\underline{n}}$, Schreibweise für $f \in \cancel{} M^{\underline{n}}$

$$(a_1, \dots, a_n) \quad \text{mit} \quad a_i = f(i)$$

Schreiben auch M^n statt $M^{\underline{n}}$

<u>Folgen in M</u> = Element von $M^{\mathbb{N}}$, Schreibweise $f \in M^{\mathbb{N}}$

$$(a_i)_{i \in \mathbb{N}} \quad \text{wobei } a_i = f(i) \text{ für } i \in \mathbb{N}.$$

Was sind 1-Tupel in M? Elemente von $M^{\underline{1}}$

$$(a), \quad a \in M$$

Identifizieren oft $M^{\underline{1}}$ und M

also (a) mit a

Kartesische Produkte

Es sei $n \in \mathbb{N}$ und M_i eine Menge für alle $i \in \underline{n}$.
Wir setzen $M := \bigcup_{i \in \underline{n}} M_i$.

Definition
$M_1 \times \cdots \times M_n := \{f : \underline{n} \to M \mid f(i) \in M_i \text{ für alle } i \in \underline{n}\}$, und nennen $M_1 \times \cdots \times M_n$ das *kartesische Produkt* von $M_1, \ldots, M_n$.

Schreibweisen

- Für $f \in M_1 \times \cdots \times M_n$ schreiben wir $(x_1, \ldots, x_n)$ oder $(x_i)_{i \in \underline{n}}$ mit $x_i := f(i)$ für $1 \leq i \leq n$.
- $M_1 \times \cdots \times M_n$ ist also 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 $i \in \underline{n}$.

Familien

Es seien M, I Mengen.

Definition
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 heißt $(x_i)_{i \in I}$ eine durch I indizierte *Familie* in M.

Beispiele

- Für $I = \mathbb{N}$ ist $(x_i)_{i \in I}$ eine Folge in M.
- Für $I = \underline{n}$ ist $(x_i)_{i \in I}$ ein n-Tupel in M.

Kartesische Produkte (Forts.)

Es sei I eine Menge und M_i eine Menge für alle $i \in I$.
Wir setzen $M := \cup_{i \in I} M_i$.

Definition
Die Menge

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

heißt das *kartesische Produkt* der Mengen $M_i, i \in I$.

Beispiel
Sei $I = \mathbb{N}$ und $M_i := \{x \in \mathbb{R} \mid x \leq i\}$ für $i \in \mathbb{N}$.
$M = \prod_{i \in \mathbb{N}} M_i = \{(x_i)_{i \in \mathbb{N}} \mid x_i \leq i \text{ für alle } i \in \mathbb{N}\}$. z.B.: $(i)_{i \in \mathbb{N}} \in M$

$I = \mathrm{Pot}(\mathbb{R}) \setminus \{\emptyset\}$, $X \subseteq \mathbb{R}$ sei $M_X := X$

$M = \prod_{X \in I} X = \prod_{\emptyset \neq X \subseteq \mathbb{R}} X$

Schwierig, ein Element aus M anzugeben!
Auswahlaxiom!: $M \neq \emptyset$

Bild und Urbild

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

Definition

- $X \subseteq M$:

$$\begin{aligned} f(X) &:= \{f(x) \mid x \in X\} \subseteq N \\ &= \{y \in N \mid \text{es gibt ein } x \in \cancel{M}\, X \text{ mit } y = f(x)\}. \end{aligned}$$

  Bild von X unter f.

- $f(M)$: *Bild* von f.
- $Y \subseteq N$:

$$f^{-1}(Y) := \{x \in M \mid f(x) \in Y\}$$

  Urbild von Y unter f.

- $f^{-1}(\{y\})$ mit $y \in N$: die *Fasern von f*.

  Urbild von y unter f

Bild und Urbild (Forts.)

Beispiele

$f\colon \{1,2,3,4\} \to \{5,6,7,8,9\}$, $1 \mapsto 5$, $2 \mapsto 8$, $3 \mapsto 5$, $4 \mapsto 9$

- $f(\{1,2,3\}) = \{5,8\}$
- Bild von $f = \{5,8,9\}$
- $f^{-1}(\{5,9\}) = \{1,3,4\}$
- $f^{-1}(\{5\}) = \{1,3\}$ Faser von 5
- Sei A die Menge der jetzt in diesem Hörsaal anwesenden Personen.
  Setzte $J := A \to \mathbb{Z}$, $p \mapsto$ Geburtsjahr von p.
  Die Faser $J^{-1}(\{2000\})$ ist die Menge der Personen aus A, die im Jahr 2000 geboren sind.

Bild und Urbild (Forts.)

Bemerkung

Es sei $f : M \to N$ eine Abbildung.
Die nicht-leeren Fasern von f bilden eine Partition von M.

Bew.: Sei $y \in N$. Faser von $y = f^{-1}(\{y\}) \neq \emptyset \Leftrightarrow y \in \text{Bild}(f)$

Beh.: $M = \dot{\bigcup}_{y \in \text{Bild} f} f^{-1}(\{y\})$ ist disjunkte Vereinigung

(also $\{f^{-1}(\{y\}) \mid y \in \text{Bild} f\}$ ist Partition von M.)

- zu jedem $x \in M$ gibt es ein $y \in N$ mit $f(x) = y$, also $x \in f^{-1}(\{y\})$
- sei nun $x \in M$, $x \in f^{-1}(\{y\})$ und $x \in f^{-1}(\{y'\})$ für $y, y' \in N$, dann $f(x) = y$ und $f(x) = y'$, also $y = y'$ (da $f(x)$ eindeutig)

Injektive, surjektive und bijektive Abbbildungen

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

Definition

- f heißt *surjektiv*, falls $f(M) = N$.
- f heißt *injektiv*, falls für alle $x, x' \in M$ gilt:
  $f(x) = f(x') \Rightarrow x = x'$. [oder: $x \neq x' \Rightarrow f(x) \neq f(x')$]
- f heißt *bijektiv*, falls f injektiv und surjektiv ist.

Injektive, surjektive und bijektive Abbbildungen (Forts.)

Beispiel

- $\{1,2,3\} \to \{4,5\}$, $1 \mapsto 4$, $2 \mapsto 4$, $3 \mapsto 5$ surj, $\neg$ inj,
- $\{1,2\} \to \{4,5,6\}$, $1 \mapsto 4$, $2 \mapsto 5$ $\neg$ surj, inj
- $\{1,2,3\} \to \{4,5,6\}$, $1 \mapsto 5$, $2 \mapsto 6$, $3 \mapsto 4$ inj, surj $\Rightarrow$ bij
- $\{1,2,3\} \to \{4,5,6\}$, $1 \mapsto 5$, $2 \mapsto 6$, $3 \mapsto 5$ $\neg$ inj, $\neg$ surj

Injektive, surjektive und bijektive Abbbildungen (Forts.)

Beispiel

$f: \mathbb{Q} \to \mathbb{Q}$, $x \mapsto -2x + 3$ ist bijektiv.

Bew: injektiv: Seien $x, x' \in \mathbb{Q}$ mit $f(x) = f(x')$ $\Leftrightarrow$

$$-2x+3 = -2x'+3 \Leftrightarrow -2x = -2x' \Leftrightarrow x = x'$$

surjektiv: Sei $y \in \mathbb{Q}$. Dann gilt für $x = \frac{3-y}{2}$, dass

$f(x) = -2 \cdot \left(\frac{3-y}{2}\right) + 3 = y$ ist, also $y \in \text{Bild}(f)$.

Injektive, surjektive und bijektive Abbbildungen (Forts.)

Beispiel

$$
\begin{aligned}
&\mathrm{Abb}_{\mathrm{inj}}(\{1,2\},\{3,4,5\})\\
&=\{(1\mapsto 3, 2\mapsto 4),(1\mapsto 3, 2\mapsto 5),(1\mapsto 4, 2\mapsto 3),\\
&\qquad(1\mapsto 4, 2\mapsto 5),(1\mapsto 5, 2\mapsto 3),(1\mapsto 5, 2\mapsto 4)\}\\
&\mathrm{Abb}_{\mathrm{surj}}(\{1,2,3\},\{4,5\})\\
&=\{(1\mapsto 4, 2\mapsto 4, 3\mapsto 5),(1\mapsto 4, 2\mapsto 5, 3\mapsto 4),\\
&\qquad(1\mapsto 4, 2\mapsto 5, 3\mapsto 5),(1\mapsto 5, 2\mapsto 4, 3\mapsto 4),\\
&\qquad(1\mapsto 5, 2\mapsto 4, 3\mapsto 5),(1\mapsto 5, 2\mapsto 5, 3\mapsto 4)\}\\
&\mathrm{Abb}_{\mathrm{bij}}(\{1,2,3\},\{4,5,6\})\\
&=\{(1\mapsto 4, 2\mapsto 5, 3\mapsto 6),(1\mapsto 4, 2\mapsto 6, 3\mapsto 5),\\
&\qquad(1\mapsto 5, 2\mapsto 4, 3\mapsto 6),(1\mapsto 5, 2\mapsto 6, 3\mapsto 4),\\
&\qquad(1\mapsto 6, 2\mapsto 4, 3\mapsto 5),(1\mapsto 6, 2\mapsto 5, 3\mapsto 4)\}
\end{aligned}
$$

Injektive, surjektive und bijektive Abbbildungen (Forts.)

Beispiele

- $f : \mathbb{Z} \to \mathbb{Z}, z \mapsto 2z$ ist inj, ¬ surj
- $f : \mathbb{R} \to \mathbb{R}, x \mapsto 2x$ ist inj, surj
- $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ ist ¬ inj, ¬ surj
- Hashfunktionen, z.B. md5 : $\{\text{Texte}\} \to \{0,1\}^{128}$

  ¬ inj, surj, Fasern für Texte gleicher Länge ungefähr gleich mächtig.

- Verschlüsselungsfunktionen, z.B. crypt : $\{0,1\}^k \to \{0,1\}^k$, sind injektiv, also auch surjektiv!