UNIVERSITÄT LEIPZIG

Vorlesung 7 - Funktionen und Ordnungsrelationen

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

- Sei $\equiv$ eine Äquivalenzrelation auf M, dann ist $M/\equiv$ eine Zerlegung von M. Umgekehrt, wenn wir eine Zerlegung $\mathcal{K}$ von M haben, dann können wir eine Äquivalenzrelation definieren, sodass die Äquivalenzklassen gleich zu $\mathcal{K}$ sind.
- Funktionen sind spezielle Relationen. Nähmlich, $f \subset M \times N$ ist eine Funktion gdw für jedes $m \in M$ existiert genau ein Element $n \in M$ so dass $(m, n) \in f$. Wir schreiben $f(m) = n$, oder $m \mapsto n$.
- $f : M \to N$ ist injektiv gdw $\forall x, y \in M : \; x \neq y \to f(x) \neq f(y)$
- $f : M \to N$ ist surjektiv gdw $\forall b \in N \exists a \in M \mid f(a) = b$
- $f : M \to N$ ist bijektive gdw f ist injektiv und surjektiv.

- Funktionen sind Relationen, und Relation können wir komponieren. Deswegen können wir auch Funktionen komponieren. Wir haben bewiesen dass wenn $f\colon M \to N, g\colon N \to P$ sind zwei Funktionen dann $f;g\colon M \to P$ ist auch eine Funktion.
- Es gilt $f;g(x) = g(f(x))$.
- Komposition ist assoziativ: $(f;g);h = f;(g;h)$.
- Wenn f, g beide injektiv (bzw. surjektiv oder bijektiv) sind, dann hat auch $f;g$ die entsprechende Eigenschaft.

- Eine Funktion $f\colon M \to N$ ist invertierbar gdw. eine Funktion $g\colon N \to M$ existiert, so dass
$$f \mathbin{;} g = \mathrm{id}_M$$
und
$$g \mathbin{;} f = \mathrm{id}_N.$$
- Äquivalent gesagt: für alle $m \in M$ gilt $g(f(m)) = m$ und für alle $n \in N$ gilt $f(g(n)) = n$.

- Kandidat für die inverse Funktion: Die inverse Relation f^{-1}

Lemma. Sei $f : M \to N$ eine Funktion. Für alle $m \in M$ und $n \in N$ gelten

- $(m, m) \in f; f^{-1}$
- $(f^{-1}; f \subset \mathrm{id}_N$. Wenn f surjektiv ist, dann $(f^{-1}; f = \mathrm{id}_N$.

Beweis.

- $(m, f(m)) \in f$, $(f(m), m) \in f^{-1}$. Deswegen $(m, m) \in f; f^{-1}$.
- Sei $(n, x) \in f^{-1}; f$. Dann $(n, a) \in f^{-1}$, $(a, x) = (a, f(a)) \in f$. Weil $(n, a) \in f^{-1}$, schließen wir $f(a) = n$. Das zeigt dass $f^{-1}; f \subset \mathrm{id}_N$.

  Wenn f surjektiv ist und $n \in N$, dann existiert $m \in M$ mit $(m, n) \in f$. Dann auch $(n, m) \in f^{-1}$, und deswegen $(n, n) \in f^{-1}; f$. Das zeigt dass $\mathrm{id}_N \subset f^{-1}; f$.

Satz. Eine Funktion $f\colon M \to N$ ist invertierbar gdw. sie bijektiv ist.

Beweis. ($\to$) Sei f invertierbar. Dann existiert eine Funktion $g\colon N \to M$, so dass $f\,;g = \mathrm{id}_M$ und $g\,;f = \mathrm{id}_N$.

- Injektivität von f: Seien $x, y \in M$ mit $f(x) = f(y)$. Zu zeigen: $x = y$. Es gilt

$$x = g(f(x)) = g(f(y)) = y.$$

- Surjektivität von f. Sei $n \in N$ beliebig. Dann ist $f(g(n)) = n$. Also existiert ein $m \in M$, so dass $f(m) = n$, nämlich $m := g(n)$.

Satz. Eine Funktion $f: M \to N$ ist invertierbar gdw. sie bijektiv ist.

$\leftarrow$ Sei f bijektiv. Wir zeigen, dass f^{-1} eine Funktion ist.

- Totalität von f^{-1}: Sei $n \in N$ beliebig. Da f surjektiv ist, existiert $m \in M$ mit $f(m) = n$. Also $(n, m) \in f^{-1}$.
- Eindeutigkeit. Seien $(n, x) \in f^{-1}$ und $(n, y) \in f^{-1}$. Folglich gilt $f(x) = n = f(y)$. Da f injektiv ist, folgt $x = y$.

Aus dem Lemma wissen wir $f^{-1}; f = \mathrm{id}_N$, und $\mathrm{id}_N \subset f; f^{-1}$. Da $f; f^{-1}$ ist eine Funktion, folgt aus der Eindeutigkeit $\mathrm{id}_N = f; f^{-1}$.

$\square$

Satz. (Eindeutigkeit der inversen Funktion) Sei $f\colon M \to N$ und seien $g, g'\colon N \to M$ mit

$$f \,;\, g = \mathrm{id}_M, \quad g \,;\, f = \mathrm{id}_N,$$

und

$$f \,;\, g' = \mathrm{id}_M, \quad g' \,;\, f = \mathrm{id}_N.$$

Dann gilt $g = g'$.

Beweis. Wegen der Assoziativität der Komposition gilt

$$g = g \,;\, \mathrm{id}_M = g \,;\, (f \,;\, g') = (g \,;\, f) \,;\, g' = \mathrm{id}_N \,;\, g' = g'.$$

$\square$

In Anwendungen wie zum Beispiel die Verschlüsselung sind die Funktionen, mit denen wir arbeiten, häufig nicht bijektiv, sondern nur injektiv. In diesem Fall spricht man von einer einseitigen Inverse.

Satz. Für jede injektive Funktion $f\colon M \to N$ existiert eine Funktion $g\colon N \to M$, so dass $f;g = \mathrm{id}_M$.

Beweis. Die Relation f^{-1} ist eindeutig (doch generell nicht total, also keine Funktion). Wir zeigen es wie früher: Seien $(n,x) \in f^{-1}$ und $(n,y) \in f^{-1}$. Folglich gilt $f(x) = n = f(y)$ und da f ist injektiv, folgt $x = y$.

Sei $m_0 \in M$ beliebig. Wir definieren $g\colon N \to M$ wie folgt: wenn $n \in f(M)$ dann $g(n) := f^{-1}(n)$, und sonst $g(n) := m_0$.

Zu zeigen: wenn $m \in m$ dann $f;g(m) = g(f(m)) = m$, Da $f(m) \in f(M)$, folgt $g(f(m)) = f^{-1}(f(m)) = m$. □

Einseitige Inversen haben wir auch für surjektive Funtionen (doch zu bemerken ist dass die Inverse “auf der anderen Seite” ist, im Vergleich zu surjektiven Funtionen)

Satz. Für jede surjektive Funktion $f\colon M \to N$ existiert eine Funktion $g\colon N \to M$, so dass $g\,;f = \mathrm{id}_N$.

- Da die Funktion f nicht immer injektiv ist, ist unser Kandidat f^{-1} im Allgemeinen nicht eindeutig, also auch keine Funktion.
- Der Beweis folgt nun einer simplen Idee: Wir wählen für jedes Element $n \in N$ ein beliebiges Urbild $m_n \in f^{-1}(\{n\})$, und bauen so aus f^{-1} die gesuchte Funktion g.

Satz. Für jede surjektive Funktion $f\colon M \to N$ existiert eine Funktion $g\colon N \to M$, so dass $g\,;f = \mathrm{id}_N$.

Beweis. (nutzt “Auswahlaxiom”) Sei $n \in N$ beliebig. Da f surjektiv ist, existiert $m \in M$ mit $f(m) = n$. Also $f^{-1}(\{n\}) \neq \emptyset$.

Wähle ein $m_n \in f^{-1}(\{n\})$ für jedes $n \in N$. Wir definieren die Funktion $g\colon N \to M$ durch $g(n) := m_n$.

Zu zeigen: $g\,;f = \mathrm{id}_N$. Für alle $n \in N$ gilt

$$f(g(n)) = f(m_n) = n.$$

$\square$

Im Allgemeinen ist es nicht möglich, die Funktion g im vorherigen Beweis explizit ("algorithmish") zu definieren. Die Urbilde von Elementen können "ununterscheidbar" sein.

- In vielen konkreten Situationen ist dies möglich - zum Beispiel können wir eine surjektive Funktion $f\colon \mathbb{N} \to \mathbb{N}$ haben. In diesem Fall könnten wir die einseitige Inverse $g\colon \mathbb{N} \to \mathbb{N}$ definieren, indem wir das kleinste Element im Vorbild wählen.

- Aber im Allgemeinen, wenn wir die gesamte Mathematik aufbauen würden, indem wir alle "ersten Prinzipien" (so-genannte "Axiome"), die wir verwenden, sorgfältig angeben, müssten wir auch das Auswahlaxiom explizit aufnehmen.

> (Auswahlaxiom, Zermelo 1904) Für jede Menge $\mathcal{X}$ von nicht-leeren Mengen gibt es eine Auswahlfunktion, d.h. Funktion $c\colon \mathcal{X} \to \bigcup \mathcal{X}$ mit $c(M) \in M$ für alle $M \in \mathcal{X}$.

- In der Konstruktion der einseitigen Inverse, nehmen wir $\mathcal{X} := \{f^{-1}(n)\colon n \in N\}$

Wir haben die Relationen $\leq$ auf $\mathbb{Z}$ und $\subseteq$ auf $\mathcal{P}(M)$, wo M eine beliebige Menge ist. Diese sind Beispiele von Ordnungsrelationen. Die algemeine Definition ist wie folgt.

Eine Relation $\preceq$ auf M ist eine Ordnungsrelation gdw. sie reflexiv, antisymmetrisch und transitiv ist.

- Das Paar $(M, \preceq)$ heißt dann eine geordnete Menge, oder auch eine teilweise geordnete Menge.
- Ist $\preceq$ auch vollständig, dann heißt $(M, \preceq)$ auch total geordnete Menge, linear geordnete Menge oder eine Kette.
- Die Schreibweise $(M, \preceq)$ bedeutet dass wir uns die Menge M nun geordnet vorstellen. Das ist ein Beispiel von einer mathematischen Struktur

Beispiele

- Die Identität id_M ist eine Ordnungsrelation, aber nicht vollständig.
- $(\mathbb{N}, \leq)$ ist eine total geordnete Menge.
- Für jede Menge M ist $(\mathcal{P}(M), \subseteq)$ eine teilweise geordnete Menge.
- Die Teilbarkeitsrelation $| = \{(n, n') \in \mathbb{N}_+ \times \mathbb{N}_+ \mid n$ teilt $n'\}$ ist eine Ordnungsrelation.
  - **Reflexivität:** Für alle $x \in \mathbb{N}_+$ teilt x sich selbst, also $x \mid x$.
  - **Antisymmetrie:** Seien $x \mid y$ und $y \mid x$. Dann gelten $x \leq y$ und $y \leq x$, womit $x = y$.
  - **Transitivität:** Seien $x \mid y$ und $y \mid z$. D. h. es existieren $k, n \in \mathbb{N}_+$, so dass $kx = y$ und $ny = z$. Also $z = ny = n(kx) = (nk)x$, womit auch $x \mid z$ gilt.

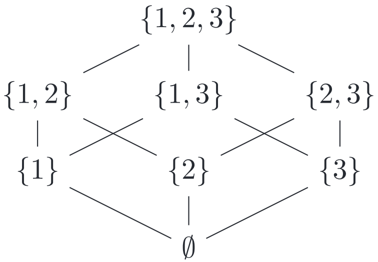
Teilweise geordnete Mengen lassen sich durch Hasse-Diagramme visualisieren.

Hasse-Diagramm für $(\mathbb{N}, \leq)$:

$$\begin{tikzcd}
\vdots \arrow[d, dash, dotted] \\
3 \arrow[d, dash] \\
2 \arrow[d, dash] \\
1 \arrow[d, dash] \\
0
\end{tikzcd}$$

- Alle Kanten sind per Konvention nach oben gerichtet.
- Eine Kante von x nach y bedeutet dass (x, y) ist in der Ordnungsrelation also $x \preceq x$.
- Kanten aus id_M (Schleifen) werden nicht dargestellt
- Ebenso Kanten, die sich vermittels Transitivität aus anderen Kanten ergeben.

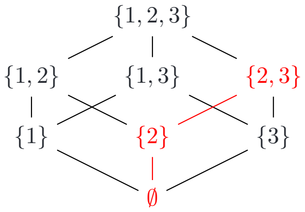
Hasse-Digramm für $(\mathcal{P}(\{1,2,3\}), \subseteq)$:



Sei $(M, \preceq)$ eine teilweise geordnete Menge. Eine Teilmenge $X \subseteq M$ ist eine Teilkette von $(M, \preceq)$ gdw. $x \preceq y$ oder $y \preceq x$ für alle $x, y \in X$.

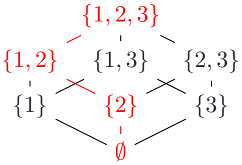
Beispiele

- Die Menge $\mathbb{N}$ ist eine Teilkette von $(\mathbb{Z}, \leq)$
- Die Menge $\{\emptyset,\ \{2\},\ \{2,\ 3\}\}$ ist eine Teilkette von $(\mathcal{P}(\{1,\ 2,\ 3\}), \subseteq)$

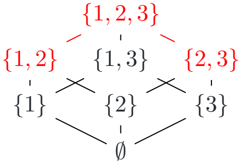


Beispiele

- Die Menge $\{\emptyset, \{2\}, \{1, 2\}, \{1, 2, 3\}\}$ ist eine Teilkette von $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$



- Die Menge $\{\{1, 2\}, \{1, 2, 3\}, \{2, 3\}\}$ ist keine Teilkette von $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$.



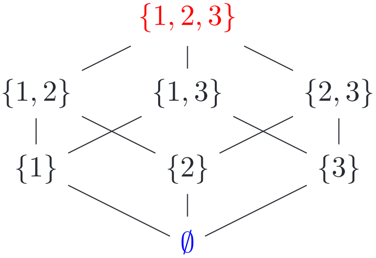
- Wir dürfen jedoch die geordnete Menge $(\{\{1, 2\}, \{1, 2, 3\}, \{2, 3\}\}, \subseteq)$ betrachten.

Sei $(M, \preceq)$ eine teilweise geordnete Menge. Ein Element $x \in M$ ist

- maximal gdw. $x \not\preceq m$ für alle $m \in M$ mit $m \neq x$; d. h. es gibt keine echt größeren Elemente,
- minimal gdw. $m \not\preceq x$ für alle $m \in M$ mit $m \neq x$; d. h. es gibt keine echt kleineren Elemente.

Beispiele

- In $(\mathbb{N}, \leq)$ haben wir 0 als einziges minimales Element und keine maximalen Elemente.
- $(\mathcal{P}(\{1,\ 2,\ 3\}), \subseteq)$



maximale Elemente: $\{1,\ 2,\ 3\}$ minimale Elemente: $\emptyset$

Beispiele

- $(\mathcal{P}(\{1, 2, 3\}) \setminus \{\emptyset, \{1, 2, 3\}\}, \subseteq)$

$$\begin{tikzcd}
\{1,2\} \arrow[d, dash] \arrow[dr, dash] & \{1,3\} \arrow[dl, dash] \arrow[dr, dash] & \{2,3\} \arrow[dl, dash] \arrow[d, dash] \\
\{1\} & \{2\} & \{3\}
\end{tikzcd}$$

maximale Elemente: $\{1, 2\}$, $\{1, 3\}$ und $\{2, 3\}$, minimale Elemente: $\{1\}$, $\{2\}$ und $\{3\}$

Sei $(M, \preceq)$ eine teilweise geordnete Menge und $X \subseteq M$. Ein Element $m \in M$ ist

- eine obere Schranke für X gdw. $x \preceq m$ für alle $x \in X$; d. h. größer als alle Elemente aus X,
- das größte Element von X gdw. $m \in X$ und m obere Schranke für X ist;
- Die Begriffe untere Schranke und kleinstes Element werden analog definiert. Ein element m ist eine untere Schranke falls $\forall x \in X$ gilt $m \preceq m$. Und m ist das kleinste Element von X wenn $m \in X$ und m ist eine untere Schranke.
- Es gibt höchstens ein größtes (bzw. kleinstes) Element von X. Wenn m, n sind beide die größten Elemente, dann $m \preceq n$ und $n \preceq m$, also $m = n$.
- Wir bezeichnen mit $\uparrow X$ und $\downarrow X$ jeweils die Menge der oberen und unteren Schranken. Mit $\max X$ und $\min X$ bezeichnen wir jeweils das größte and das kleinste Element von X (wenn sie existieren).

Beispiele

- In $(\mathbb{Z}, \leq)$ hat die Mengen $\mathbb{N}$
  - obere Schranken: keine
  - größtes Element: keins
- In $(\mathbb{Z}, \leq)$ hat $\{-1, 2\}$
  - obere Schranken: $\{z \in \mathbb{Z} \mid z \geq 2\}$
  - größtes Element: 2
- In $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$ hat $\{\{1\}, \{2\}\}$
  - obere Schranken: $\{1, 2\}$ und $\{1, 2, 3\}$
  - größtes Element: keins, maximale Elemente $\{1\}, \{2\}$.

- Sei $(M, \preceq)$ eine teilweise geordnete Menge und $X \subseteq M$.
- Das Supremum $\sup X$ von X ist das kleinste Element von $\uparrow X$. Also die kleinste obere Schranke für X.
- Das Infimum $\inf X$ von X ist das größte Element von $\downarrow X$. Also die größte untere Schranke für X.

- Wir betrachten $(\mathcal{P}(\{1,2,3\}), \subseteq)$.
    - Das Supremum von $\{\{2\}\}$ ist $\{2\}$, es gilt $\sup\{\{2\}\} = \{2\}$.
    - Es gilt $\sup\{\{1\},\ \{2\}\} = \{1,\ 2\}$.
- Suprema/Infima existieren nicht immer. Als Beispiel betrachten wir $\mathbb{R}$ mit üblicher Ordnungsrelation. Dann $\mathbb{R}$ selbst hat kein Supremum und kein Infimum.
- Supremum von $[0,1)$ in $(\mathbb{R}, \leq)$ ist 1.
- Sei $M \subseteq \mathcal{P}(\mathbb{N})$ die Menge von allen endlichen Teilmengen von $\mathbb{N}$, mit der Teilmengerelation $\subseteq$. Dann hat M kein Supremum in M. Jedoch M hat ein Supremum als eine Teilmenge von $\mathcal{P}(\mathbb{N})$.

Satz. Sei M eine Menge, und sei $X \subset \mathcal{P}(\mathcal{M})$. Dann X hat Supremum und Infimum in $\mathcal{P}(M)$, und es gilt $\sup X = \bigcup X$, $\inf X = \bigcap X$.

Beweis. Z.B. zeigen wir $\sup X = \bigcup X$. Wir zeigen zunächst, dass $\bigcup X$ eine obere Schranke für X ist. Sei $Y \in X$ beliebig. Dann gilt $Y \subseteq \bigcup X$, womit $\bigcup X$ obere Schranke ist.

Jetzt zeigen wir das $\bigcup X$ die kleinste obere Schranke ist. Sei S irgenwelche andere obere Schranke. Dann für jede $Y \in X$ gilt $Y \subset S$, wobei auch $\bigcup X \subset X$. □

- Dieser Satz motiviert die folgende Notation: Sei $(M, \subseteq)$ eine geordnete Menge, und $x, y \in M$. Dann schreiben wir $x \vee y := \sup(\{x, y\})$, $x \wedge y := \inf(\{x, y\})$.
- $(M, \subseteq)$ heißt Verband gdw. für alle $x, y \in M$ wir haben dass $x \vee y$ und $x \wedge y$ existieren.
- $(M, \subseteq)$ heißt vollständiger Verband gdw. für alle $X \subseteq M$ wir haben dass $\sup X$ und $\inf X$ existieren.

UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski
Mathematisches Institut

grabowski@math.uni-leipzig.de