Diskrete Strukturen

WiSe 2012/13 in Trier

Henning Fernau
Universität Trier
fernau@uni-trier.de

17. Dezember 2012

$\boxed{\textbf{Diskrete Strukturen}}$ Gesamtübersicht

- Organisatorisches und Einführung
- Mengenlehre
- Relationen und Funktionen
- Kombinatorik: Die Kunst des Zählens
- Grundbegriffe (algebraischer) Strukturen
- Graphen

Organisatorische Besonderheiten in den nächsten Wochen

- 30.11.: Da Herr Meister nicht da ist, werde ich die Übungen betreuen.
  Es wird ausnahmeweise dabei nur ZWEI Übungsgruppen geben:
  a) 9.00 Beginn im H 11
  b) 10.05 Beginn im K 101 (Kapelle)
  Aufgrund der Kapazitäten der Hörsäle würde ich diejenigen, die es einrichten können, bitten, in die Kapelle zu kommen.

- 14.12.: 10.05 Vorlesungsbeginn in der Kapelle (K 101)
  14.05 Zwischenklausur im HS 13 (ohne Unterlagen)

- 21.12.: Da Herr Meister nicht da ist, werde ich die Übungen betreuen.
  Der Ablauf ist wie am 30.11.

Spezielle Relationen

- Äquivalenzrelationen
- Halbordnungen
- Funktionen

Äquivalenzrelationen

Def.: Eine *Äquivalenzrelation* (auf M) ist eine Binärrelation über M, die reflexiv, symmetrisch und transitiv ist.
Üblich zumeist Infixschreibweise.

Beispiel: Allrelation und Diagonale sind Äquivalenzrelationen.

Beispiel: $R = \{(a,b),(b,a)\} \cup \Delta_{\{a,b,c,d\}}$ ist eine Äquivalenzrelation auf $\{a,b,c,d\}$.

Beispiel: Betrachte das Warenangebot eines Supermarktes. Die Preisgleichheit liefert eine Äquivalenzrelation auf der Menge der angebotenen Waren.

Beispiel: $R_m = \{(a,b) \in \mathbb{Z}^2 : m \mid (a-b)\}$. Eigenschaften nachrechnen!
Schreibweise: $a \equiv b \pmod{m}$ statt aR_mb.

Partitionen

Def.: Es sei M eine Menge, $M \neq \emptyset$. Eine *Zerlegung*, *Klasseneinteilung* oder *Partition* von M ist eine *Mengenfamilie* $Z \subseteq 2^M$ mit:

1. $M = \bigcup_{A \in Z} A$.

2. $\emptyset \notin Z$.

3. $\forall A, B \in Z : A \cap B \neq \emptyset \implies A = B$.

Die Elemente von Z heißen auch *Klassen*.

Beispiel: Die Klassen von R_m heißen auch *Restklassen* (modulo m).

Partitionen und Äquivalenzrelationen 1

Satz 1: Eine Klasseneinteilung Z von M induziert eine Äquivalenzrelation $\sim_Z$ über M durch $a \sim_Z b \iff$ a und b liegen in derselben Z-Klasse.

Beweis: 0. Klar: $\sim_Z \subseteq M \times M$.

1. Reflexivität: Wegen $M = \bigcup_{A \in Z} A$ folgt für jedes a: $a \sim_Z a$.

2. Symmetrie: trivial

3. Transitivität: Betrachte a, b, c mit $a \sim_Z b$ und $b \sim_Z c$.

Also gibt es Klassen J und K mit $a, b \in J$ und $b, c \in K$.

Daher ist: $J \cap K \neq \emptyset$.

Da Z Zerlegung, folgt $J = K$, woraus sich ergibt,

dass a und c in derselben Z-Klasse liegen, also $a \sim_Z c$ gilt. $\square$

Partitionen und Äquivalenzrelationen 2

Def.: Es sei R eine Äquivalenzrelation über M.
$[b]_R := \{a \in M \mid aRb\}$ bezeichnet die *Äquivalenzklasse* von b.
b heißt auch *Repräsentant* oder *Vertreter* von $[b]_R$.
$M/R := Z_R := \{[b]_R \mid b \in M\}$ ist die *Quotientenmenge* von R.

Satz 2: Ist R eine Äquivalenzrelation über M, so ist Z_R eine Zerlegung von M.

Genauer gilt: Lemma: Ist R ÄR, so gilt $R = (\sim_{Z_R})$.

Ein Hilfssatz: Ist $R \subseteq M \times M$ eine Äquivalenzrelation, dann gilt für beliebige Äquivalenzklassen $[b]_R$ und beliebige $x, y \in M$:
Falls $\{x, y\} \subseteq [b]_R$, so $\{(x, y), (y, x)\} \subseteq R$.

Beweis: Betrachte $x, y \in M$ mit $\{x, y\} \subseteq [b]_R$.

Nach Def. bedeutet das: $\{(x, b), (y, b)\} \subseteq R$.

Da R symmetrisch, gilt auch: $(b, y) \in R$.

Da R transitiv, folgt aus $\{(x, b), (b, y)\} \subseteq R$: $(x, y) \in R$.

Da R symmetrisch, folgt weiter: $(y, x) \in R$. $\square$

Zum Beweis von Satz 2

1. Jedes Element ist in einer ÄK von Z_R enthalten.

Betrachte $a \in M$. Wegen $(a, a) \in R$ gilt: $[a]_R \neq \emptyset$.

2. $\emptyset \notin Z_R$.

Dies folgt mit dem vorigen Argument, da ÄK nur von der Gestalt $[a]_R$ sind.

3. Gilt $[a]_R \cap [b]_R \neq \emptyset$, so ist $[a]_R = [b]_R$.

Vorüberlegung: Da $[a]_R \cap [b]_R \neq \emptyset$, gibt es ein $y \in [a]_R \cap [b]_R$.

Betrachte irgendein $x \in [a]_R$. Da $\{x, y\} \subseteq [a]_R$, gilt $(x, y) \in R$ (HS).

Für $z \in [b]_R$ ist $\{y, z\} \subseteq [b]_R$ und daher $(y, z) \in R$ (HS).

Da R transitiv, gilt $(x, z) \in R$.

Mithin ist $x \in [b]_R$ und $z \in [a]_R$.

Nach Def. der Quotientenmengen und da x, z bel., folgt $[a]_R = [b]_R$. $\square$

Partitionen und Äquivalenzrelationen: Beispiele

Beispiel: Allrelation: $[x]_{M\times M} = M$ für alle $x \in M$.

Beispiel: Diagonale: $[x]_{\Delta_M} = \{x\}$ für alle $x \in M$.

Beispiel: $R_m \subset \mathbb{Z} \times \mathbb{Z}$: Äquivalenzklassen sind $[0], [1], \ldots, [m-1]$.

Hinweis: Zwei ganze Zahlen sind äquivalent gdw. sie lassen beim Teilen durch m denselben Rest. Schreibweise: (für die Menge der Restklassen) $\mathbb{Z}_m := \mathbb{Z}/R_m$.

Partitionen und Äquivalenzrelationen: $\mathbb{Q}$ als Beispiel

Wir hatten bislang (verschiedentlich) $\mathbb{N}$ *axiomatisch* eingeführt.
Daraus könnte man $\mathbb{Z}$ einführen als Quotientenmenge auf $\{+,-\} \times \mathbb{N}$ mit der Äquivalenzrelation $(v, n) \sim (v', n')$ gdw. $n = n' \wedge (v = v' \vee n = 0)$.

Über $M = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ definiere: $(a, b) \sim (a', b') \iff ab' = ba'$.
Dann ist die Menge der rationalen Zahlen $\mathbb{Q}$ definiert als $\mathbb{Q} = M/\sim$.
Statt $[(a, b)] \in M/\sim$ schreiben wir auch $\frac{a}{b}$.
(a, b) und (a', b') liegen in derselben Äquivalenzklasse gdw.
$\frac{a}{b} = \frac{a'}{b'}$ gdw. $ab' = ba'$.

Ergänzung zu Satz 1

Es sei Z eine Zerlegung von M. Es sei $R =\sim_Z$ die induzierte Äquivalenzrelation.

Lemma: $Z = \{[a]_R \mid a \in M\}$, also $Z_R = Z$.

Beweis: Es sei $X \in Z$. Fixiere $x \in X$. Wir zeigen: $y \in X$ gdw. $y \in [x]_R$.

Falls $y \in X$, so $x \sim_Z y$ nach Def., also $y \in [x]_R$.

Falls $y \in [x]_R$, so $x \sim_Z y$ nach Def., also $y \in X$. $\square$

Lemma: Ist P eine bel. Äquivalenzrelation auf M mit $Z = \{[a]_P \mid a \in M\}$, so gilt $P = R$ (Eindeutigkeit).

Beweis: $(x, y) \in P \implies x \in [y]_P \implies \exists z \in M : x, y \in [z]_R \implies \exists z \in M : \{(x, z), (y, z)\} \subseteq R$ $\implies \exists z \in M : \{(x, z), (z, y)\} \subseteq R$ (Symmetrie) $\implies (x, y) \in R$ (Transitivität).

Die andere Richtung sieht man genauso. $\square$

Weitere Sätze und Begriffe

Satz: Sind R und S ÄR über M, so auch $R \cap S$.
(Übungsaufgabe)

Satz: Es seien R und S ÄR über M. $R \circ S$ und $S \circ R$ ist ÄR gdw. $R \circ S$ ist ÄR gdw. es gilt $R \circ S = S \circ R$.
(Übungsaufgabe)

Die *Äquivalenzhülle* von einer binären Relation R ist die kleinste R umfassende Relation, die sowohl reflexiv, transitiv, als auch symmetrisch ist; geschrieben R_E^*.

Äquivalenzhülle—ein Beispiel

Sei $M = \{a, b, c, e, d, f\}$ und
$R = \{(a, b), (c, b), (d, e), (e, f)\}$.
Konstruiere Äquivalenzhülle R_E^* von R.
R_E^* ist reflexiv $\leadsto \Delta_M \subseteq R_E^*$.
R_E^* ist symmetrisch $\leadsto R^- \subseteq R_E^*$.
Transitivität liefert vier weitere Paare (welche?)
Die Äquivalenzklassen von R_E^* sind:
$[a] = \{a, b, c\}$ und $[d] = \{d, e, f\}$.

Äquivalenzhülle—ein Satz

Satz 3: Für $R \subseteq M \times M$ gilt:

$$R_E^* = \underbrace{(R \cup R^- \cup \Delta_M)^+}_{=:S} = \underbrace{(R \cup R^-)^+ \cup \Delta_M}_{=:T}.$$

In Worten:

R_E^* ist die reflexive Hülle der transitiven Hülle der symmetrischen Hülle von R.

Äquivalenzhülle—ein Satz

Satz: Für $R \subseteq M \times M$ gilt:

$$R_E^* = \underbrace{(R \cup R^- \cup \Delta_M)^+}_{=:S} = \underbrace{(R \cup R^-)^+ \cup \Delta_M}_{=:T}.$$

<u>Beweis:</u> Wegen $\Delta_M \cup R^- \subseteq S \cap T$ sind S und T reflexiv und symmetrisch; S und T sind per def. transitiv. $\leadsto$ S und T sind ÄR, d.h., $R \subseteq R_E^* \subseteq T \subseteq S$.
Angenommen, es gäbe $(x, y) \in S$, $(x, y) \notin R_E^*$.
Es gibt eine kleinste natürliche Zahl n, sodass es irgendwelche $(s, u) \in (R \cup R^- \cup \Delta_M)^n$ gibt mit $(s, u) \notin R_E^*$.
Klar: $n > 1$, denn $R_E^* \supseteq (R \cup R^- \cup \Delta_M) = (R \cup R^- \cup \Delta_M)^1$
$\leadsto \exists t (s, t) \in (R \cup R^- \cup \Delta_M)^{n-1} \wedge (t, u) \in (R \cup R^- \cup \Delta_M)$
n minimal $\leadsto$ $(s, t) \in R_E^*$; “klar”: $(t, u) \in R_E^*$; also: $(s, u) \in R_E^*$, da R_E^* transitiv.
<u>Hinweis:</u> Alternative: Induktionsbeweis

Starker Zusammenhang

Satz: Für $R \subseteq M \times M$ gilt: $R' := R^* \cap (R^-)^*$ ist eine ÄR.

(Übungsaufgabe)

Noch zwei Beispiele

Beispiel: Es sei M die Menge aller Menschen.
R sei gegeben durch: $(x, y) \in R$ gdw. x ist Elternteil von y.
Was bedeutet $x R_E^* y$ (in Worten) ?
Beschreibe R' (wie soeben definiert).

Quasiordnung

Def.: Eine reflexive und transitive Relation R über M heißt auch *Quasiordnung*.

Beispiel: Jede Äquivalenzrelation ist eine Quasiordnung.
Genauer gilt: Eine Quasiordnung ist genau dann eine Äquivalenzrelation, wenn sie symmetrisch ist.

Beispiel: Betrachte über der Menge $\mathbb{C}$ der komplexen Zahlen die Relation $y \prec z \iff |y| \leq |z|$.
Beobachte: $\prec$ ist weder symmetrisch noch antisymmetrisch.

Satz: Ist R eine Relation über M, so ist R^* die kleinste R umfassende Quasiordnung.

Halbordnungen

Def.: Eine antisymmetrische Quasiordnung R über M heißt auch *Halbordnung* (auf der gegebenen Grundmenge). Gilt $(x, y) \in R$, so heißt x auch *Vorgänger* von y und y *Nachfolger* von x.

Beispiel: $\leq$ oder $\geq$ auf $\mathbb{R}$ sind Halbordnungen.

Beispiel: $\prec$ auf $\mathbb{C}$ ist keine Halbordnung.

Beispiel: Die Teilerrelation ist eine Halbordnung auf $\mathbb{N}$, aber nicht auf $\mathbb{Z}$.

Beispiel: Auf der Potenzmenge von M ist $\subseteq$ oder auch $\supseteq$ eine Halbordnung.

Lineare Ordnungen

Def.: Eine Halbordnung $\leq$ auf M heißt *linear* (*total*) gdw. $\forall x, y \in M(x \leq y \vee y \leq x)$. Zwei Elemente $x, y \in M$ heißen *vergleichbar* gdw. $(x \leq y \vee y \leq x)$; andernfalls heißen sie *unvergleichbar*. Die HO $\leq$ ist also linear gdw. alle Elemente von M untereinander paarweise vergleichbar sind.

Satz: Ist Vergleichbarkeit transitiv, so ist sie eine Äquivalenzrelation.
Dann gilt: Eine HO ist linear gdw. die von ihr induzierte Vergleichbarkeitsrelation hat nur eine Äquivalenzklasse.

Beispiel: Lexikalische Ordnung in einem Wörterbuch

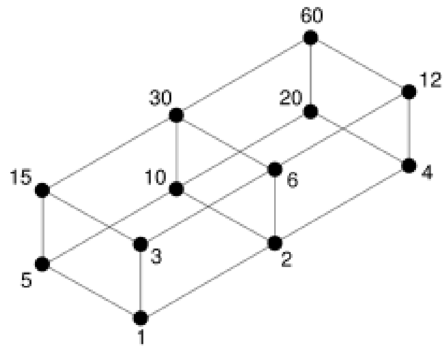
Lineare Ordnungen sind eminent wichtig für unser Leben (als Informatiker)

Bezeichnungen für “Computer”: ordinateur / ordenador

“Ordnen” (Sortieren) ist die “Rechnertätigkeit”, die am meisten Rechenzeit weltweit benötigt.

Für manche “gutartige” Sortierverfahren ist es entscheidend für ihre Laufzeit, wie “wenig linear” die Eingangsreihenfolge ist.

Halbordungsrelationen: ein Beispiel zum Hasse-Diagramm



Bei diesem *Hasse-Diagramm* werden “passende” unvergleichbare Elemente auf einer Ebene dargestellt.
Ein Element x wird “unter” einem anderen y dargestellt und durch eine ungerichtete Kante verbunden, wenn x unmittelbarer Nachfolger von y ist (Def. folgt).
Das obige Diagramm zeigt die Teiler von 60, angeordnet für die Halbordnung $|$ “ist Teiler von”.
1 ist hierbei unmittelbarer Nachfolger aller Primteiler von 60.

Erinnerung: Hasse-Diagramme für Inklusionen sind Spezialfall, da $(2^M, \subseteq)$ Halbordnung.

echte und unmittelbare Nachfolger / Hasse-Diagramme

Es sei $\leq$ eine Halbordnung auf M. $z \in M$ heißt *unmittelbarer Nachfolger* von $x \in M$, falls (1) $x \leq z$, (2) $x \neq z$ und (3) falls aus $x \leq y \leq z$ folgt: $y = x$ oder $y = z$. Gelten nur (1) und (2), so heißt z *echter Nachfolger* von x, i.Z. $x < z$.

Hinweis: Im Hasse-Diagramm werden genau die Kanten dargestellt, die zur Relation "unmittelbarer Nachfolger" gehören.

Hinweis: Entsprechend definierbar: *echter Vorgänger*, *unmittelbarer Vorgänger*

Satz: Ist R die zu der Halbordnung $\leq$ auf M gehörige Relation des echten Nachfolgers, so ist $\leq$ gerade die reflexive Hülle von R.

Satz: Ist R die zu der Halbordnung $\leq$ auf M gehörige Relation des unmittelbaren Nachfolgers und ist M endlich, so ist $\leq$ gerade die reflexive transitive Hülle von R.

Beispiel: Teilmengenhalbordnung von $\{a, b, c\}$.

Restriktionen

Ist R eine Relation über M und ist $N \subseteq M$, so heißt $R_N := (R \cap N \times N)$ *Restriktion* oder *Einschränkung* von R auf N.

Satz: Mit R ist auch R_N Quasiordnung bzw. Halbordnung bzw. lineare Ordnung.

Dahinter steckt ein Prinzip:
Über Allaussagen definierte Eigenschaften übertragen sich durch Restriktion.

In einer Halbordnung $(M, \leq)$ heißt $K \subseteq M$ *Kette* gdw. die Restriktion von $\leq$ auf K eine lineare Ordnung ist.
Eine Kette K heißt *maximal*, wenn es keine K umfassende Kette gibt.

Maximalkettenprinzip von Hausdorff / Birkhoff:
In jeder halbgeordneten Menge gibt es maximale Ketten.

Sortieren—formal

Es sei $(M, \leq)$ eine totale Ordnung (z.B.: lexikalische Ordnung oder gewöhnliche Anordnung der ganzen Zahlen) und $N \subseteq M$ eine endliche Menge mit totaler Ordnung $\mathtt{Mem}$ (z.B.: (reflexive Hülle der) Anordnung im Speicher).
N heißt *sortiert* bzgl. $\leq$ gdw. $\mathtt{Mem} = \leq_N$.

$\leadsto$ einfacher Sortieralgorithmus:

Solange $\exists x, y \in N, x \neq y : (x, y) \in \mathtt{Mem} \wedge y \leq x$: $\mathtt{Mem} := (\mathtt{Mem} \setminus \{(x, y)\}) \cup \{(y, x)\}$.

$\leadsto$ Iterative Variante: *Blasensortieren* (Bubblesort)
Es werden immer nur Nachbarn (bzgl. $\mathtt{Mem}$) verglichen, also $x, y \in N$, sodass x echter Vorgänger von y ist (bzgl. $\mathtt{Mem}$).

Solange $\exists x, y \in N, x \neq y : (x, y) \in \mathtt{Mem} \wedge y \leq x$**:** $\mathtt{Mem} := (\mathtt{Mem} \setminus \{(x, y)\}) \cup \{(y, x)\}$

Warum stimmt der Algorithmus?

Wenn der Algorithmus anhält, (*partielle Korrektheit*)
so gibt es keine $x, y \in N, x \neq y : (x, y) \in \mathtt{Mem} \wedge y \leq x$.
Also gilt für alle $x, y \in N, x \neq y$: Wenn $(x, y) \in \mathtt{Mem}$, dann gilt $y \leq x$ <u>nicht</u>.
Da $(M, \leq)$ eine totale Ordnung ist, muss dann also $x \leq y$ gelten.
Die Anordnung im Speicher spiegelt also die lineare Ordnung $\leq$ wieder.
Formal bedeutet das gerade: $\mathtt{Mem} = \leq_N$.
Daher liefert der Algorithmus eine Sortierung, sofern er hält.

Solange $\exists x, y \in N, x \neq y : (x, y) \in \texttt{Mem} \wedge y \leq x$: $\texttt{Mem} := (\texttt{Mem} \setminus \{(x, y)\}) \cup \{(y, x)\}$

Warum hält der Algorithmus immer? (*Terminierung*)

Hierzu ist folgende Überlegung hilfreich:
Lemma: Es sei m eine natürliche Zahl.
Nach dem m-ten Durchlauf der Schleife gilt (so es diesen überhaupt gibt): es gibt wenigstens m Paare $(x, y) \in N \times N$, $x \neq y$, für die gilt: $(x, y) \in \texttt{Mem}$ und $x \leq y$.

Wenn die Menge N nun n verschiedene Elemente enthält (Genaueres zu Mächtigkeiten später in der Vorlesung), so gibt es in $N \times N$ höchstens n^2 viele Paare.
Mit dem Lemma folgt:
Folgerung: Der Algorithmus hält nach höchstens n^2 vielen Schleifendurchläufen.

Zum Beweis des Lemmas mit Induktion

Nach dem m-ten Durchlauf der Schleife gilt (so es diesen überhaupt gibt): es gibt $\geq m$ Paare $(x, y) \in N \times N$, $x \neq y$, mit $(x, y) \in \texttt{Mem}$ und $x \leq y$.

Beweis: IA: Die Aussage gilt trivialerweise für $m = 0$.

IV: Nach dem j-ten Durchlauf gilt: es ex. $\geq j$ Paare $(x, y) \notin \Delta_N$ mit $(x, y) \in \texttt{Mem}$ und $x \leq y$.

IB: Nach dem $(j+1)$-sten Durchlauf der Schleife gilt (falls es diesen gibt): es gibt $\geq (j+1)$ Paare $(x, y) \in N \times N$, $x \neq y$, für die gilt: $(x, y) \in \texttt{Mem}$ und $x \leq y$.

IS: Betrachten wir die Situation unmittelbar vor dem $(j+1)$-sten Durchlauf der Schleife.

Diese entspricht genau derjenigen nach dem j-ten Durchlauf der Schleife.

Also gibt es j Paare $(x_i, y_i) \in N \times N$, $x_i \neq y_i$, $1 \leq i \leq j$ für die gilt: $(x_i, y_i) \in \texttt{Mem}$ und $x_i \leq y_i$.

Falls $(j+1)$-ster Durchlauf stattfindet, ex. ein Paar (x, y), $x \neq y$, mit $(x, y) \in \texttt{Mem} \wedge y \leq x$.

Würde $(x, y) = (x_i, y_i)$ gelten für ein $1 \leq i \leq j$, so wäre $x \leq y$ und $y \leq x$ gültig.

Da $\leq$ antisymmetrisch, folgt $x = y$, Widerspruch.

Also gibt es nach dem $(j+1)$-sten Durchlauf der Schleife $(j+1)$ Paare $(x, y) \in N \times N$, $x \neq y$, für die gilt: $(x, y) \in \texttt{Mem}$ und $x \leq y$. $\square$

Programmtexte als Formalismen—ein Weg zur Informatik

```
procedure BS(A)
  for each i from 1 to length(A) do:
       for each j from length(A) downto i + 1 do:
         if A[ j ] < A[ j-1 ] then
           swap( A[ j ], A[ j-1 ] )
         end if
       end for
  end for
end procedure
```

Ein Beispiel:

```
7 5 3 8
7 5 3 8
7 3 5 8
3 7 5 8
3 7 5 8
3 5 7 8
```

Ausgangslage: $M = \mathbb{N}$, $N = \{7, 5, 3, 8\}$, $\leq$ ist das übliche Kleiner-Gleich auf $\mathbb{N}$.

`Mem` ist die reflexiv-transitive Hülle der Relation $\{(7, 5), (5, 3), (3, 8)\}$.

Es gilt daher: $(A[i], A[j]) \in$ `Mem` gdw. $i \leq j$.

Der `swap` verändert also in unserer Lesart `Mem` wie gewünscht.

`BS` systematisiert die Suche nach falsch angeordneten Paaren.

Programmtexte als Formalismen—ein Weg zur Informatik

Hier verstecken sich zwei Induktionsbeweise!

```
procedure BS(A)
//Die Eingabe A ist eine Liste zu sortierender Gegenstände
  for each i from 1 to length(A) do:
       for each j from length(A) downto i + 1 do:
         if A[ j ] < A[ j-1 ] then
           swap( A[ j ], A[ j-1 ] )
         end if
//A[j-1] ist ein kleinstes Element von A[j-1],...,A[length(A)]
       end for
//A[i] ist ein kleinstes Element von A[i],...,A[length(A)]
//Die Liste A[1],..,A[i] ist aufsteigend sortiert
  end for
end procedure
```

Programmtexte als Formalismen—ein Weg zur Informatik

Hier versteckt sich ein Induktionsbeweis!

```
procedure BS(A)
//Die Eingabe A ist eine Liste von n zu sortierenden Gegenständen
  for each i from 1 to n do:
       for each j from n downto i + 1 do:
         if A[ j ] < A[ j-1 ] then
           swap( A[ j ], A[ j-1 ] )
         end if
       end for
//swap wird höchstens n−i mal ausgeführt
  end for
//(Die äußere Schleife wird n mal ausgeführt.)
//Also wird swap insgesamt höchstens (n−1)+(n−2)+···+1 = n(n−1)/2 mal ausgeführt
end procedure
```

Aufgabe: Welche Teile müssten Sie noch beweisen ?!

klein und groß...

Es sei $(M, \leq)$ eine Halbordnung und $\emptyset \neq N \subseteq M$.
$x \in N$ heißt *größtes Element* von N, wenn $\forall y \in N : y \leq x$.
$x \in N$ heißt *kleinstes Element* von N, wenn $\forall y \in N : x \leq y$.
$x \in N$ heißt *maximales Element* in N, wenn $\forall y \in N : x \leq y \implies y = x$.
$x \in N$ heißt *minimales Element* in N, wenn $\forall y \in N : y \leq x \implies y = x$.
$x \in M$ heißt *obere Schranke* von N, wenn $\forall y \in N : y \leq x$.
$x \in M$ heißt *untere Schranke* von N, wenn $\forall y \in N : x \leq y$.
Eine kleinste obere Schranke heißt auch *obere Grenze* oder *Supremum*.
Eine größte untere Schranke heißt auch *untere Grenze* oder *Infimum*.

Satz: Eine Menge N besitzt ein größtes Element
gdw. eine obere Grenze liegt in N
gdw. eine obere Schranke liegt in N.
Größte Elemente und obere Schranken einer Menge sind eindeutig bestimmt.

Beispiel: Teilmengenhalbordnung von $\{a, b, c\}$.
Beispiel: $0 \prec 2 \prec 4 \prec \cdots \prec 1 \prec 3 \prec 5 \prec \cdots$ auf $\mathbb{N}$.

oh wie wohl... (ein ergänzender Ausblick)

Eine *Wohlordnung* auf einer Menge M ist eine totale Ordnung mit der Eigenschaft, dass jede nichtleere Teilmenge von M ein bzgl. dieser Ordnung kleinstes Element hat. Die Menge M zusammen mit der Wohlordnung heißt eine wohlgeordnete Menge.

Beispiel: Die $(\mathbb{N}, \leq)$ ist eine Wohlordnung, aber weder die gewöhnliche Anordnung der ganzen Zahlen noch die der positiven reellen Zahlen ist eine Wohlordnung.

Für die Algorithmik wichtig: noch allgemeinerer Begriff der *Wohlquasiordnung*.

Wohlordnungssatz / Wohlordnungsprinzip: Jede Menge kann wohlgeordnet werden.
Hinweis: Äquivalent zum Maximalkettenprinzip und zum Auswahlaxiom.

Transfinite Induktion verallgemeinert die uns bekannte Induktion auf beliebige wohlgeordnete Mengen: Sei $(M, \leq)$ eine Wohlordnung und 0 bezeichne das kleinstes Element.
Will man beweisen, dass die Eigenschaft P für alle Elemente von M zutrifft, dann beweist man bei transfiniter Induktion folgendes:
– $P(0)$ ist wahr.
– Wenn $0 \leq a$, $a \neq 0$ und $P(b)$ ist wahr ist für alle $b \leq a$, $b \neq a$, dann ist auch $P(a)$ wahr.

Wohlordnungsprinzip $\rightsquigarrow$ Induktion ist potentiell immer anwendbar.

Definitionen mit transfiniter Induktion erstmals von J. von Neumann (1928).

Erinnerung: Wir hatten für Relationen R über M definiert:

R heiße *nacheindeutig* (oder *rechtseindeutig*) gdw.

$$\forall x, y, z \in M(((x, y) \in R \land (x, z) \in R) \implies y = z).$$

R heiße *vortotal* (oder *linkstotal*) gdw. $\forall x \in M \exists y \in M((x, y) \in R)$.

Wir wollen dies im Folgenden etwas allgemeiner für Relationen R zwischen A und B verstehen.

Kleine Übertragungsaufgabe: Was bedeutet dies formal?

Funktionen

Def.: Eine *partielle Funktion* F ist eine nacheindeutige binäre Relation zwischen A und B.
Eine partielle Funktion F heißt *total* oder einfach *Funktion* oder *Abbildung* gdw. F ist linkstotal.

Hinweis: Für Mathematiker sind Funktionen total, für Informatiker sind Funktionen partiell.

Schreibweise: $f : A \to B, a \mapsto f(a)$
$f(a)$ *Bild* von a bei f; a *Urbild*;
A: *Definitionsbereich*,
B: *Wertebereich*
$f^{-}(B) = \{a \in A \mid \exists b \in B : f(a) = b\}$ *Urbildbereich*
$f(A) = \{b \in B \mid \exists a \in A : f(a) = b\}$ *Bildbereich*
Satz: Eine partielle Funktion ist total gdw. ihr Definitions- und Urbildbereich stimmen überein.

Funktionen: Beispiele

Beispiel: Die Diagonale ist eine totale Funktion.
Beispiel: Die Vorschrift, die jedem Studenten der Universität Trier seine DSL-Note zuordnet, ist eine partielle Funktion.
Beispiel: Die Relation, die sämtlichen Elementen aus A stets dasselbe Element aus B zuordnet, ist eine totale Funktion, genannt *konstante Funktion*.
Beispiel: Ist $A \subseteq B$, so kann man die Diagonale Δ_A auch als Abbildung $\iota : A \to B$ auffassen: diese heißt auch *natürliche Einbettung* oder *Inklusionsabbildung*.
Für $A = \emptyset$ spricht man von der *leeren Abbildung*.

Projektionen

Ist $M = M_1 \times M_2 \times \cdots \times M_n$, so definiert für $1 \leq i \leq n$

$$\mathrm{pr}_i : M \to M_i, (x_1, x_2, \ldots, x_i, \ldots, x_n) \mapsto x_i$$

die *Projektion* von M auf M_i.

Lemma: Jede Projektion ist eine Abbildung.

Projektionen lassen sich auch mit Relationen als Definitionsbereich etwas allgemeiner auffassen.

Funktionen und Äquivalenzrelationen

Satz 4: Es sei $f : A \to B$ eine Abbildung. Dann definiert $x \sim_f y$ gdw. $f(x) = f(y)$ eine Äquivalenzrelation auf A. Diese nennt man auch *Kern* von f.

Satz 5: Es sei $\sim$ eine Äquivalenzrelation auf A. Es bezeichne $[a]$ die $\sim$-Äquivalenzklasse von A. $f_\sim : A \to A/\sim, a \mapsto [a]$ ist eine Abbildung.
Diese heißt auch *kanonische Abbildung* von $\sim$.

Folgerung: Mit den Bezeichnungen der voranstehenden Sätze gilt:

$$\sim = \sim_{f_\sim} \quad \text{und} \quad f = f_{\sim_f}$$

Beispiele an der Tafel.

Funktionen und Verknüpfungen

Eine (n-stellige) *Verknüpfung* oder *Operation* auf einer Grundmenge M ist eine Abbildung $f : M^n \longrightarrow M$.

Hinweis: $M^n = M \times \cdots \times M$ bezeichnet das $(n-1)$-fache kartesische Produkt von M mit sich selbst.

Speziell: zweistellige Verknüpfungen schreibt man meist in Infixnotation, die Operatorensymbole stehen also zwischen den beiden Operanden.

Beispiel: (für Logiker) Auf der Menge $B = \{w, f\}$ sind die Junktoren $\vee$, $\wedge$ zweistellige Verknüpfungen.

Einstellige Verknüpfungen sind "normale" Abbildungen $M \longrightarrow M$.
Nullstellige Verknüpfungen bezeichnen Konstanten in M.

Mengenfunktionen

Es sei $R \subseteq A \times B$ eine Relation (z.B. auch eine (partielle) Funktion).
Diese kann man auch als Mengenfunktionen deuten:
$R_1 : 2^A \to 2^B,\ X \mapsto \{y \in B \mid \exists x \in X (x,y) \in R\}$
$R_2 : 2^B \to 2^A,\ Y \mapsto \{x \in A \mid \exists y \in Y (x,y) \in R\}$

Satz: $R_1(A_1 \cup A_2) = R_1(A_1) \cup R_1(A_2)$. (entsprechend für R_2)

Beweis: Sei $y \in R_1(A_1 \cup A_2)$. Dann gibt es $x \in A_1 \cup A_2$ mit $(x,y) \in R$. Also: $x \in A_1$ oder $x \in A_2$. Im ersten Fall ist $y \in R_1(A_1)$, im zweiten $y \in R_1(A_2)$. Die Rückrichtung sieht man analog. $\square$

Satz: $R_1(A_1 \cap A_2) \subseteq R_1(A_1) \cap R_1(A_2)$. (entsprechend für R_2)

Beweis: Die Inklusion sieht man wie bei $\cup$. Gleichheit gilt im Allg. nicht, z.B.: $A = \{a, a'\}, B = \{1\}$, $R = \{(a,1),(a',1)\}$, $A_1 = \{a\}, A_2 = \{a'\}$. $R_1(A_1 \cap A_2) = R_1(\emptyset) = \emptyset \subsetneq \{1\} = R_1(A_1) \cap R_1(A_2)$. $\square$

Ist R durch eine Funktion $f : A \to B$ gegeben, schreibt man auch $f(X)$ statt $R_1(X)$, und $f^-(Y)$ statt $R_2(Y)$.
Satz: $f^-(B_1 \cap B_2) = f^-(B_1) \cap f^-(B_2)$.

Komposition von Funktionen

Satz: Sind R und S nacheindeutige Relationen über M, so auch $R \circ S$.

Satz: Sind R und S vortotale Relationen über M, so auch $R \circ S$.

Das Relationenprodukt wird im Falle (partieller) Funktionen auch oft als *Komposition* oder *Hintereinanderausführung* angesprochen.

Vom Relationenprodukt erben wir die folgende Eigenschaft:
Satz: Die Komposition von (partiellen) Funktionen ist assoziativ.
ACHTUNG: Veränderte Reihenfolge bei Komposition von Funktionen gegenüber Meinel/Mundhenk, d.h.: $(f \circ g)(x) = g(f(x))$.

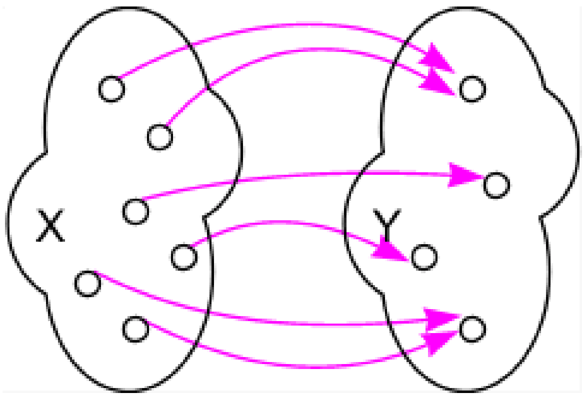
Funktionen: Eigenschaften I

Def.: Eine Abbildung $f : X \to Y$ heißt *surjektiv* oder eine *Surjektion* oder eine Abbildung von X *auf* Y gdw. ihr Bild- und Wertebereich übereinstimmen, d.h., wenn sie nachtotal ist.

Surjektionen sind also vor- und nachtotale, rechtseindeutige Relationen.

Beispiel: $f : \mathbb{Z} \to \mathbb{Z}_m, n \mapsto n \pmod m$ ist surjektiv; ebenso jede Projektion.

Im Bild:



Surjektive Abbildungen

Satz 6: Es sei $f : A \longrightarrow B$ eine Abbildung.
Die folgenden Aussagen sind logisch äquivalent:
(1) f ist surjektiv.
(2) $\forall b \in B : f^{-}(\{b\}) \neq \emptyset$.
(3) $\exists g : B \longrightarrow A : g \circ f = \Delta_B$.
(4) Es sei C eine weitere Menge und $r, s : B \longrightarrow C$ beliebige Abbildungen, so gilt die folgende Kürzungsregel: $f \circ r = f \circ s \Rightarrow r = s$.

Surjektive Abbildungen—Anmerkungen zum Beweis:

Beweisstrategie: Statt (1) $\iff$ (2), (1) $\iff$ (3) und (1) $\iff$ (4) beweisen wir im *Ringschluss*:
(1) $\implies$ (2), (2) $\implies$ (3), (3) $\implies$ (4), (4) $\implies$ (1).
Die "fehlenden" Implikationen liefert die "Transitivität" der Implikation.

Bei der Implikation (2) $\implies$ (3) machen wir Gebrauch vom *Auswahlaxiom von Zermelo*: Zu jeder Menge $\mathcal{M}$ von nichtleeren Mengen eines Universums $\mathfrak{U}$ gibt es eine Abbildung $f : \mathcal{M} \to \mathfrak{U}$ mit $f(A) \in A$.
Das Auswahlaxiom ist zum Maximalkettenprinzip äquivalent.

Einzelheiten zum Beweis

(1) $\Rightarrow$ (2): f surj. $\rightsquigarrow f(A) = B$, d.h., für $b \in B$ gibt es ein $a \in A$ mit $f(a) = b$, also $f^{-}(\{b\}) \neq \emptyset$.
(2) $\Rightarrow$ (3): Mit dem Auswahlaxiom können wir uns wegen $f^{-}(\{b\}) \neq \emptyset$ zu jedem $b \in B$ ein $g(b) \in f^{-}(\{b\})$ auswählen; es gilt nach Def.: $f(g(b)) = b$.
Damit gilt: $(g \circ f)(b) = f(g(b)) = b$ für alle $b \in B$.
(3) $\Rightarrow$ (4): Betrachte zwei bel. Abb. $r, s : B \to C$ mit $f \circ r = f \circ s$.
Wegen (3) gibt es $g : B \to A : g \circ f = \Delta_B$. Mit der Assoziativität der Komposition folgt:

$$r = \Delta_B \circ r = (g \circ f) \circ r = g \circ (f \circ r) = g \circ (f \circ s) = (g \circ f) \circ s = \Delta_B \circ s = s.$$

(4) $\Rightarrow$ (1) mit Kontraposition: Annahme, f ist nicht surjektiv, d.h., es gibt ein $b_0 \in B \setminus f(A)$.
Für $C = \{0, 1\}$ betrachte Abbildungen $r, s : B \to \{0, 1\}$ mit $r(b) = s(b) = 0$ für alle $b \neq b_0$ und $r(b_0) = 0$ und $s(b_0) = 1$.
Offenbar gilt $r \neq s$, aber sehr wohl $f \circ r = f \circ s$, da der Unterschied außerhalb von $f(A)$ auftritt. $\square$

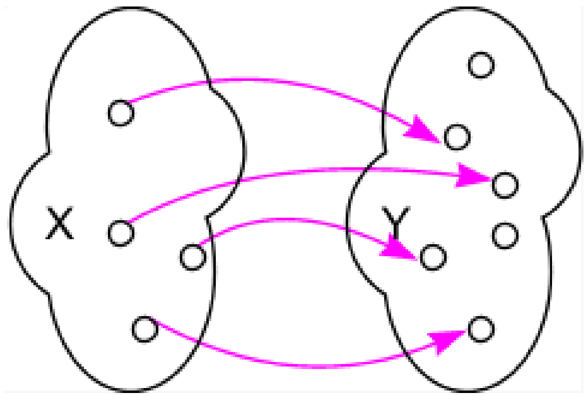
Funktionen: Eigenschaften II

Def.: Eine Abbildung $f : X \to Y$ heißt *injektiv* oder eine *Injektion* oder *eineindeutig* gdw. die zugehörige Relation voreindeutig ist.

Injektionen sind also vortotale, links- und rechtseindeutige Relationen.

Bsp.: $f : \mathbb{Z} \to \mathbb{Z}, n \mapsto 2 \cdot n$ ist injektiv, ebenso jede Inklusionsabbildung.

Im Bild:

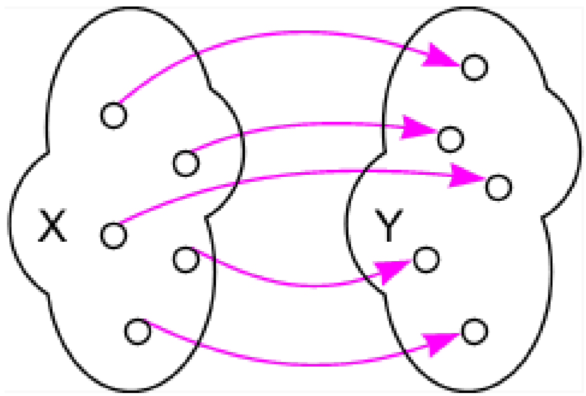


Injektive Abbildungen

Satz 7: Es sei $f : A \to B$ eine Abbildung.
Die folgenden Aussagen sind logisch äquivalent:
(1) f ist injektiv.
(2) $\forall b \in B : f^{-}(\{b\})$ enthält höchstens ein Element.
(3) $\exists g : B \to A : f \circ g = \Delta_A$.
(4) Es sei C eine weitere Menge und $r, s : C \to A$ beliebige Abbildungen, so gilt die folgende Kürzungsregel: $r \circ f = s \circ f \Rightarrow r = s$.
Beweis ähnlich zur Surjektivität.

Funktionen: Eigenschaften III

Def.: Eine Abbildung $f : X \to Y$ heißt *bijektiv* oder eine *Bijektion* gdw. die zugehörige Relation voreindeutig und rechtstotal ist.
Bijektionen sind also vor- und nachtotale, links- und rechtseindeutige Relationen.
Im Bild:



Bijektive Abbildungen

Satz 8: Es sei $f : A \to B$ eine Abbildung.
Die folgenden Aussagen sind logisch äquivalent:
(1) f ist bijektiv.
(2) $\forall b \in B : f^{-}(\{b\})$ enthält genau ein Element.
(3) $\exists g : B \to A : g \circ f = \Delta_B$ und $f \circ g = \Delta_A$.

Die in (3) beschriebene Inverse heißt auch die *Umkehrabbildung* von f, geschrieben f^{-1}.
Lemma: Mit f ist auch f^{-1} bijektiv, und es gilt: $(f^{-1})^{-1} = f$.

Bijektive Abbildungen—Weitere Aussagen

Satz 9: (1) Die Komposition von Surjektionen ist surjektiv.
(2) Die Komposition von Injektionen ist injektiv.
(3) Die Komposition von Bijektionen ist bijektiv.

Satz: Ist A endlich und $f : A \to A$, so sind gleichwertig:
(1) f ist surjektiv, (2) f ist injektiv, (3) f ist bijektiv.
Den Beweis hierzu “vertagen” wir.

Der Satz von Schröder und Bernstein

Der im Folgenden formulierte Sachverhalt erscheint auf den ersten Blick völlig einleuchtend, erfordert aber einen nicht-trivialen Beweis.

Etwas zur Historie:

Der erste Beweis hierzu wurde von Felix Bernstein vorgestellt, damals war F.B. ein Student bei Georg Cantor.

Einige Jahre zuvor haben den Satz wohl Richard Dedekind und Ernst Schröder bewiesen, und Cantor hat den Sachverhalt wohl auch schon erkannt.

Unser Beweis folgt der Darstellung von Julius König.

Satz 10: Gibt es injektive Abbildungen $f : A \longrightarrow B$ und $g : B \longrightarrow A$, so gibt es auch eine Bijektion zwischen A und B.

Beweis: Es seien $f : A \to B$ und $g : B \to A$ injektiv. O.E. gehen wir davon aus, dass $A \cap B = \emptyset$. Für jedes $a \in A$ betrachte die Folge

$$\cdots \mapsto f^{-}(g^{-}(a)) \mapsto g^{-}(a) \mapsto a \mapsto f(a) \mapsto g(f(a)) \mapsto \cdots$$

(und entsprechend für $b \in B$); diese Folgen wechseln zwischen A und B hin und her.

Für gewisse $n \geq 1$ könnte $(f \circ g)^n(a) = a$ gelten. Dann bildet $a, f(a), g(f(a)), \ldots, (g \circ f)^{n-1}(f(a))$ einen “Kreis.”

Andernfalls setzt sich die Folge “nach rechts” unendlich lang fort.

Man muss dann “nach links” drei Fälle unterscheiden:

(a) Die Folge endet in A; (b) sie endet in B; (c) sie setzt sich unendlich fort.

Beobachtung: Jedes Element aus A und auch aus B kommt in genau einer dieser Folgen vor.

Satz 1 zeigt: Die Relation R mit “$(x, y) \in R$ gdw. x und y liegen in derselben Folge” ist also eine Äquivalenzrelation auf $A \cup B$.

Wir definieren eine Bijektion $h : A \to B$ für jede Äquivalenzklasse getrennt:

Liegt $a \in A$ in einer Folge vom Typ (a) oder (c) oder in einem Kreis, so setze $h(a) = f(a)$.

Liegt $a \in A$ in einer Folge vom Typ (b), so setze $h(a) = g^{-}(a)$.

Zu zeigen bleibt: h ist tatsächlich eine Bijektion. $\square$

Eine Illustration des Beweises

Es sei $A \subseteq \mathbb{N}$ die Menge der geraden Zahlen und $B \subseteq \mathbb{N}$ die Menge der ungeraden Zahlen. Die Abbildungen $f : A \to B, n \mapsto n + 3$ und $g : B \to A, n \mapsto 3n - 1$ sind beide injektiv. Folgen in $A \cup B$ sind:

$$0 \mapsto 3 \mapsto 8 \mapsto 11 \mapsto 32 \mapsto \cdots$$

$$1 \mapsto 2 \mapsto 5 \mapsto 14 \mapsto 17 \mapsto \cdots$$

$$4 \mapsto 7 \mapsto 20 \mapsto 23 \mapsto 68 \mapsto \cdots$$

$$6 \mapsto 9 \mapsto 26 \mapsto 29 \mapsto 86 \mapsto \cdots$$

$$\vdots$$

$$h : 0 \mapsto 3, 2 \mapsto 1, 4 \mapsto 7, 6 \mapsto 9, 8 \mapsto 11, 10 \mapsto 13, 12 \mapsto 15, 14 \mapsto 5, \ldots$$

Definiert man (Relationenschreibweise) $f' := (f \setminus \{(2,5)\}) \cup \{(2,1)\}$ und $g' = (g \setminus \{(1,2),(3,8)\}) \cup \{(1,0),(3,2)\}$, so erhält man Kreisfall.

Eine Ergänzung des Beweises

Klar: $h \subseteq A \times B$ (Relationenschreibweise).
h ist vortotal: Mit der Beobachtung genügt die folgende Bemerkung: Insbesondere wird $h(a) = g^{-}(a)$ nur im Fall (b) gesetzt, wenn Urbilder von g stets existieren.
h ist links- und rechtseindeutig: Das ergibt sich mit der Beobachtung aus der Rechtseindeutigkeit von f und der Linkseindeutigkeit von g.
h ist nachtotal: Betrachte ein $b \in B$. Nach der Beobachtung liegt b in einer Folge, die sich (im Ausschnitt) als

$$\cdots f^{-}(b) \mapsto b \mapsto g(b) \mapsto \cdots$$

darstellt. Je nach Fall ist somit $h(f^{-}(b)) = b$ oder $h(g(b)) = b$. Also gilt $b \in h(A)$.

Warum stimmt also die Beobachtung?
Würde $a \in A$ in zwei solcher Folgen vorkommen, so wären beide Folgen “nach rechts” ab a identisch aufgrund der Rechtseindeutigkeit von f und von g, und sie stimmten auch “nach links” überein ab a wegen der Linkseindeutigkeit von f und von g.

Ferner gilt: Da f (und g) vortotal, enthält jede Folge mit $a \in A$ auch $f(a) \in B$ und umgekehrt; also enthält jede Folge mindestens zwei Elemente.

Das gilt insbesondere für mögliche Kreise.

Folgerung: Gilt $A \subseteq B$ und gibt es eine injektive Abbildung $B \to A$, so gibt es auch eine Bijektion zwischen A und B.

Beweis: Beachte: Die natürliche Einbettung $\iota : A \to B$ ist injektiv. $\square$

Diese Beobachtungen erleichtern die Angabe von Bijektionen, da Injektionen meistens ausreichend sind.

Im Folgenden werden wir aber dennoch meist direkt Bijektionen angeben.

Das ist aber nicht immer so einfach; versuchen Sie, eine Bijektion $f : [0,1] \to [0,1)$ zu finden.
$[0,1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$;
$[0,1) = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$.

Folgen sind spezielle Funktionen

Erinnerung: $\mathbb{N}$: Menge der natürlichen Zahlen; $[n] := \{m \in \mathbb{N} \mid m < n\}$.

Def.: Eine *unendliche Folge* f mit *Gliedern* aus einer Menge M ist eine Abbildung $f : \mathbb{N} \to M$.

Def.: Eine *endliche Folge* f mit *Gliedern* aus einer Menge M ist eine Abbildung $f : [n] \to M$ für ein $n \in \mathbb{N}$.

Folgen dienen zum *Auflisten*, *Abzählen* oder *Nummerieren* von (einigen) Elementen einer Menge. Eine surjektive Folge liefert also eine *vollständige Auflistung* des Wertebereichs.

Folgen: Beispiele

Beispiel: *Listenschreibweise*:

$$\left(1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \dots, \frac{1}{2^m}, \dots\right)$$

beschreibt die Folge $f : \mathbb{N} \to \mathbb{Q},\ i \mapsto 2^{-i}$.

Beispiel: Die ganzen Zahlen lassen sich vollständig auflisten. Betrachte

$$f : \mathbb{N} \to \mathbb{Z},\ n \mapsto \begin{cases} -\frac{n}{2}, & \text{falls } n \text{ gerade} \\ \frac{n+1}{2}, & \text{sonst} \end{cases}$$

Das Cantorsche Abzählungsschema I

Satz 11: Es gibt eine vollständige Auflistung von $\mathbb{N} \times \mathbb{N}$.

Beweis: Betrachte das folgende Schema:

```
/ 0 1 2 3 4 5 ...
0 0 2 5 9 14 20 ...
1 1 4 8 13 19 26 ...
2 3 7 12 18 25 33 ...
3 6 11 17 24 32 41 ...
4 10 16 23 31 40 50 ...
5 15 22 30 39 49 60 ...
| | | | | | | ...
```

Das Cantorsche Abzählungsschema I

Das Schema lässt sich auch formal notieren als *Cantorsche Paarfunktion*:

$$\langle i, j \rangle = (i + j)(i + j + 1)/2 + j$$

Also:
$\langle 0, 0 \rangle = 0$, $\langle 1, 0 \rangle = 1$, $\langle 0, 1 \rangle = 2$, $\langle 2, 0 \rangle = 3$, $\ldots$

Folgerung: Für jedes n ist $\mathbb{N}^n = \underbrace{\mathbb{N} \times \cdots \times \mathbb{N}}_{n \text{ mal}}$ vollständig auflistbar.

Beispiel: $n = 3$ (Tripel): $\langle i, j, k \rangle = \langle \langle i, j \rangle, k \rangle$.

Das Cantorsche Abzählungsschema II

Satz 12: Die rationalen Zahlen lassen sich vollständig auflisten.

Beweis: Dies lässt sich zeigen, indem man die Brüche folgendermaßen in einem zweidimensionalen Schema anordnet und dann den vorigen Satz anwendet:

```
1/1 1/2 1/3 1/4 1/5 ...
2/1 2/2 2/3 2/4 2/5 ...
3/1 3/2 3/3 3/4 3/5 ...
4/1 4/2 4/3 ...
5/1 5/2 ...
...
```

Erinnerung: Äquivalenzklassendefinition der rationalen Zahlen

Rekursiv definierte Folgen

Beispiel: Die Folge $(a_0, a_1, a_2, \dots) = (a_n)_{n \in \mathbb{N}}$ ist gegeben durch:

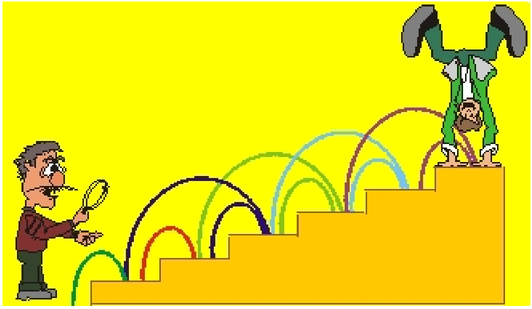
$$\begin{aligned} a_0 &= 1, \\ a_n &= a_{n-1} \cdot n, \text{ für } n > 0. \end{aligned}$$

Schreibweise: $\prod_{j \in [n]} b_j$ bezeichnet das Produkt aller Zahlen der endlichen Folge $(b_0, \dots, b_{n-1})$. Das leere Produkt wird als Eins interpretiert.

Satz: Für die oben definierte Folge a_n gilt: $a_n = \prod_{j \in [n] \setminus \{0\}} j$. $f(n) = a_n$ heißt auch *Fakultätsfunktion*; Schreibweise: $n!$

Beweis: eine leicht Induktion

Rekursiv definierte Folgen: Treppensteigen



Bei jeder Stufe kann man sich die Frage stellen:
Nehme ich eine Stufe oder überspringe ich eine Stufe?
Die erste Stufe muss auf jeden Fall betreten werden.
Frage: Auf wieviel verschiedene Arten f_n kann man nun eine n-stufige Treppe heraufgehen?

Versuchen wir (an der Tafel), eine Tabelle dafür aufzustellen.

Rekursiv definierte Folgen: Treppensteigen

Finden wir ein *Bildungsgesetz* ?

Für $n \geq 2$ gibt es zwei Möglichkeiten, eine n-stufige Treppe zu erklimmen:
– entweder hatten wir einen Schritt von einer $(n-1)$-stufigen Treppe aus gemacht
– oder zwei Stufen auf einmal von einer $(n-2)$-stufigen Treppe aus genommen.

$\rightsquigarrow$ $f_n = f_{n-1} + f_{n-2}$; Sonderfälle: $f(0) = 0$ und $f(1) = 1$.

Diese Folge kommt sehr häufig in der Natur und Kultur vor und wird gemeinhin die Folge der *Fibonacci-Zahlen* genannt !
Mehr über Leonardo Fibonacci bei einem virtuellen Museumsbesuch.

Der Goldene Schnitt

ist die Teilung einer Strecke so, dass die gesamte Strecke X sich zu dem größerem Teilstück der Länge 1 verhält wie das größere Teilstück zum kleineren.

Das Teilverhältnis lässt sich nun einfach ausrechnen. Es gilt:

$$X : 1 = 1 : (X - 1), \quad \text{also:} \quad X^2 - X = 1$$

mit den beiden Lösungen ϕ und $\hat{\phi} = 1 - \phi$, wobei

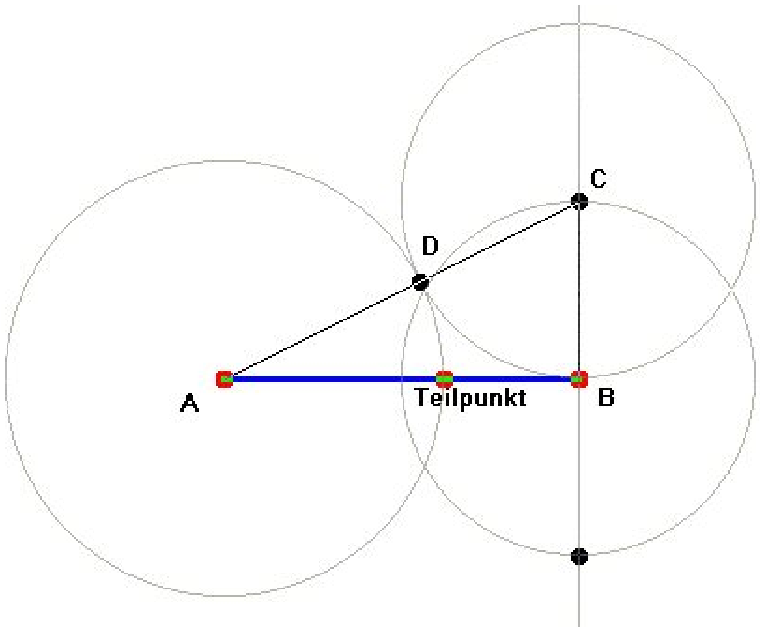
$$\phi = \frac{1 + \sqrt{5}}{2} \approx 1.6181\ldots$$

die *goldene Schnittzahl* ist.

Ein architektonischer Exkurs

Beim Parthenontempel in Athen bildet der Säuleneingang hierbei ein goldenes Rechteck, also ein Rechteck, dessen Seiten sich genau wie der goldene Schnitt verhalten. Auch verhält sich die Höhe bis zum Dach zur Höhe der Säulen wie der goldene Schnitt.

Konstruktion des Goldenen Schnitts



Im Endpunkt der Strecke AB wird die Senkrechte errichtet. Auf ihr trägt man die Hälfte von AB ab. Es ergibt sich Punkt C. Der Kreis um C mit dem Radius CB schneidet AC bei D. Überträgt man den Abstand AD auf die Strecke AB, so ergibt sich der Teilpunkt T. T teilt AB im Verhältnis des Goldenen Schnittes.

Fibonacci-Zahlen: Eine Philatelistische Annäherung

Diese Schweizer Briefmarke wurde zum 150-jährigen Bestehen des Schweizerischen Ingenieur- und Architektenvereins SIA herausgegeben und enthält eine interessante mathematische Konstruktion.

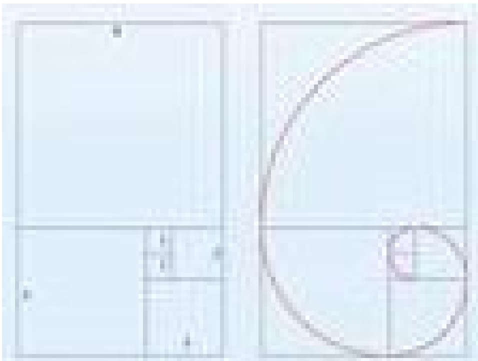
Die Briefmarke zeigt den Zusammenhang des Goldenen Schnitts mit der Logarithmischen Spirale, auch Fibonacci-Spirale genannt.

Nähere Erläuterungen finden Sie hier

Ein **geometrisches Problem**, das zu den Fibonacci-Zahlen führt:

Konstruktion aneinanderliegender Quadrate.

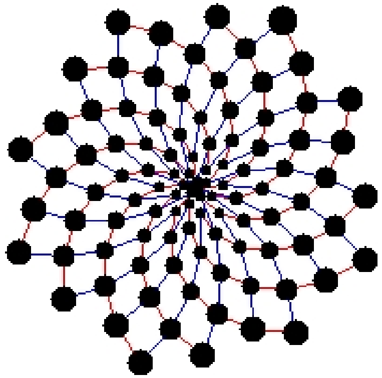
Wird in jedem Quadrat ein Viertel eines Kreises gezogen wie in der Abbildung, erhält man die sogenannte *Fibonacci-Spirale*, eine Form, die bei gewissen Muscheln beobachtet werden kann.



Die Muscheln sind lediglich ein Beispiel für ein verbreitetes Phänomen: das
Vorkommen der Fibonacci-Zahlen in der Natur.

Die Fibonacci-Zahlen finden sich in der Position der Blätter und der Blumenblätter von Blumen, in den Verzweigungen einiger Pflanzen, in der Anordnung der Samen der Sonnenblumen oder der Schuppen der Tannzapfen.
Letztere sind so angeordnet, dass sie zwei Serien von entgegengesetzten Spiralen bilden, die im Zentrum zusammenfließen.
Im selben Tannzapfen oder derselben Sonnenblume sind die Zahlen der Spiralen, die sich in beide Richtungen winden, aufeinanderfolgende Fibonacci-Zahlen.

Konkretes Naturbeispiel: Die Sonnenblume



Bei der Sonnenblume sind die Samen bogenförmig angeordnet. Das heißt, wenn man die Anzahl der Bögen gegen den Uhrzeigersinn und die der Bögen im Uhrzeigersinn betrachtet, erhält man zwei aufeinanderfolgende Fibonacci-Zahlen.

Begründung: Die Sonnenblumenkerne wachsen kreisförmig um den Mittelpunkt der Sonnenblume. Zwei in ihrer Entwicklung aufeinander folgende Kerne teilen den Umfang dabei im Verhältnis des Goldenen Schnitts. Der Winkel zwischen ihnen beträgt also $360^o - 360^o/\phi \approx 137,518\ldots^o$.

Mehr finden Sie bei matheprisma.

Satz: (Formel von Binet) $f_n = \frac{\phi^n - (1-\phi)^n}{\sqrt{5}}$.

Beweis: $n = 0$ und $n = 1$ elementar. Für den IS beobachten wir:

$$\phi^2 = 1 + \phi = 1 + \frac{1+\sqrt{5}}{2}; \qquad (1-\phi)^2 = 1 + (1-\phi) = 1 + \frac{1-\sqrt{5}}{2}$$

Also:

$$\begin{aligned} \frac{\phi^{n+2} - (1-\phi)^{n+2}}{\sqrt{5}} &= \frac{\phi^n(1+\phi) - (1-\phi)^n(1+(1-\phi))}{\sqrt{5}} \\ &= \frac{\phi^n + \phi^{n+1} - (1-\phi)^n - (1-\phi)^{n+1}}{\sqrt{5}} \\ &= f_{n+1} + f_n = f_{n+2} \end{aligned}$$

Ein weiterer Zusammenhang zwischen Goldenem Schnitt und Fibonacci-Zahlen:

$$\lim_{n\to\infty} \frac{f_n}{f_{n-1}} = \phi.$$

Zur Anwendung injektiver Folgen

Es gibt Injektionen $f : \mathbb{N} \to [0, 1]$ mit $f(0) = 1$, z.B.: $i \mapsto 2^{-i}$.
Dies gestattet die Konstruktion einer Bijektion $h : [0, 1] \to [0, 1)$.
Setze nämlich:

$$h(x) = \begin{cases} x, & \text{falls } x \notin f(\mathbb{N}) \\ f(n+1), & \text{falls } x = f(n) \end{cases}$$

Insbesondere ist also: $h(1) = f(1) = \frac{1}{2}$, $h(\frac{1}{2}) = \frac{1}{4}$.
Überlegen Sie, wo die Injektivität von f eingeht.