Mathematik I für Studierende der Informatik und Wirtschaftsinformatik (Diskrete Mathematik) im Wintersemester 2017/18

2. November 2017

Vollständige Induktion mit mehreren Vorgängern. Wieder sei $A(n)$ eine Aussageform.
Dann gilt $A(n)$ genau dann für alle natürlichen Zahlen n, wenn $A(1)$ wahr ist und für alle $n \in \mathbb{N}$ die folgende Implikation gilt: $A(1) \wedge \cdots \wedge A(n) \Rightarrow A(n+1)$.

Bei dieser Variante ist die Induktionsannahme die Annahme, dass $A(1), \ldots, A(n)$ wahr sind.

Eng mit der vollständigen Induktion verwandt sind *rekursive Definitionen*.

Beispiel 2.6

Wir definieren einen Folge natürlicher Zahlen a_n wie folgt:

1. $a_1 = 1$
2. $a_{n+1} = 2a_n + 1$

Definition 2.7 (Fibonacci-Zahlen)

Es sei $f_0 = 0$ und $f_1 = 1$. Für alle $n \geq 1$ sei $f_{n+1} = f_{n-1} + f_n$.

Satz 2.8

Für alle $n \in \mathbb{N}_0$ gilt

$$f_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Beweis. Wir beweisen den Satz durch vollständige Induktion, wobei wir Induktion mit mehreren Vorgängern anwenden.
Es seien

$$\varphi := \frac{1+\sqrt{5}}{2} \text{ und } \psi := \frac{1-\sqrt{5}}{2}.$$

Sei $A(n)$ die Aussageform $f_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}$.

Induktionsanfang. Es gilt

$$\frac{\varphi^0 - \psi^0}{\sqrt{5}} = \frac{1-1}{\sqrt{5}} = 0 = f_0$$

sowie

$$\frac{\varphi^1 - \psi^1}{\sqrt{5}} = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2} \right) = \frac{1}{\sqrt{5}} \cdot \frac{2\sqrt{5}}{2} = 1 = f_1.$$

Induktionsschritt. Wir zeigen $A(n-1) \wedge A(n) \Rightarrow A(n+1)$ für alle $n \geq 1$.

Dazu nehmen wir an, dass für ein gewisses $n \geq 1$ die Aussage $A(n-1) \wedge A(n)$ gilt (Induktionssannahme).

Dann ist

$$f_{n+1} = f_{n-1} + f_n = \frac{\varphi^{n-1} - \psi^{n-1} + \varphi^n - \psi^n}{\sqrt{5}}$$
$$= \frac{\varphi^n \left(1 + \frac{1}{\varphi}\right) - \psi^n \left(1 + \frac{1}{\psi}\right)}{\sqrt{5}}.$$

Es gilt

$$1 + \frac{1}{\varphi} = 1 + \frac{2}{1+\sqrt{5}} = \frac{1+\sqrt{5}+2}{1+\sqrt{5}}$$
$$= \frac{(3+\sqrt{5})(1-\sqrt{5})}{(1+\sqrt{5})(1-\sqrt{5})} = \frac{-2-2\sqrt{5}}{1-5} = \frac{1+\sqrt{5}}{2} = \varphi.$$

Analog gilt

$$1 + \frac{1}{\psi} = \psi.$$

Damit ergibt sich

$$f_{n+1} = \frac{\varphi^{n+1} - \psi^{n+1}}{\sqrt{5}},$$

also $A(n+1)$. $\square$

Ist $A(n)$ eine Aussageform und gelten $A(1)$ und $\forall n \in \mathbb{N}(A(n) \Rightarrow A(n+1))$, so können wir die Menge $S = \{n \in \mathbb{N} : A(n) \text{ ist wahr}\}$ betrachten und stellen Folgendes fest:

1. $1 \in S$
2. $n \in S \Rightarrow n + 1 \in S$

Eine Menge mit den Eigenschaften (1) und (2) nennen wir *induktiv*.

Wir können also bei 1 anfangen, in Einerschritten zu zählen, ohne jemals die Menge S zu verlassen.
Nach unserer Intuition über die natürlichen Zahlen erreichen wir dabei alle natürlichen Zahlen.
Also gilt $\mathbb{N} \subseteq S$. Andererseits ist $S \subseteq \mathbb{N}$.

Es folgt $S = \mathbb{N}$. Also gilt $A(n)$ für alle $n \in \mathbb{N}$.

Die folgende Axiome präzisieren unsere Intuition über die natürlichen Zahlen.
Hierbei steht n' für den Nachfolger von n in den natürlichen Zahlen, also für $n+1$.

Definition 2.11

Die folgenden Axiome sind die *Peano-Axiome* für die natürlichen Zahlen.

1. $1 \in \mathbb{N}$
2. $n \in \mathbb{N} \Rightarrow n' \in \mathbb{N}$
3. $n \in \mathbb{N} \Rightarrow n' \neq 1$
4. $m, n \in \mathbb{N} \Rightarrow (m' = n' \Rightarrow m = n)$
5. $(1 \in S \wedge \forall n \in \mathbb{N}(n \in S \Rightarrow n' \in S)) \Rightarrow \mathbb{N} \subseteq S$

Das Axiom (5) ist das *Induktionsaxiom*, welches garantiert, dass wir Sätze mittels vollständiger Induktion beweisen können.

Normalsprachlich lauten die Axiome wie folgt:

1. 1 ist eine natürliche Zahl.
2. Der Nachfolger einer natürlichen Zahl ist wieder eine natürliche Zahl.
3. 1 ist nicht Nachfolger einer natürlichen Zahl.
4. Die Nachfolgerfunktion $n \mapsto n'$ ist injektiv.
5. Jede induktive Menge enthält alle natürlichen Zahlen.

Satz 2.12

Jede nichtleere Menge natürlicher Zahlen hat ein kleinstes Element.

Ganze und rationale Zahlen

Die Menge $\mathbb{Q}$ der *rationalen Zahlen* ist die Menge aller Brüche $\frac{m}{n}$ mit $m, n \in \mathbb{Z}$ und $n \neq 0$.

Da wir jede ganzen Zahl m mit dem Bruch $\frac{m}{1}$ identifzieren können, fassen wir $\mathbb{Z}$ als eine Teilmenge von $\mathbb{Q}$ auf.

Wir erinnern uns kurz daran, wie man Brüche addiert und multipliziert:

$$\frac{m}{n} + \frac{m'}{n'} = \frac{m \cdot n' + m'n}{n \cdot n'}$$

$$\frac{m}{n} \cdot \frac{m'}{n'} = \frac{m \cdot m'}{n \cdot n'}$$

Die folgenden Rechenregeln für rationale Zahlen a, b, c setzen wir als bekannt voraus:

(K1) Assoziativgesetze

- $a + (b + c) = (a + b) + c$
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) Kommutativgesetze

- $a + b = b + a$
- $a \cdot b = b \cdot a$

(K3) Distributivgesetz

- $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) Existenz neutraler Elemente bezüglich der Addition und der Multiplikation

- $a + 0 = a$
- $1 \cdot a = a$

(K5) Existenz inverser Elemente bezüglich der Addition und der Multiplikation

- Es gibt ein Element $-a$ mit $a + (-a) = 0$.
- Falls $a \neq 0$ ist, so gibt es ein Element a^{-1} mit $a \cdot a^{-1} = 1$.

Definition 3.15

Sei K eine Menge, 0 und 1 zwei verschiedene Elemente von K und $+ : K \times K \to K$ und $\cdot : K \times K \to K$ Abbildungen.
Dann heißt K zusammen mit 0, 1, $+$ und $\cdot$ ein *Körper*, falls die Axiome (K1)–(K5) erfüllt sind.

Wie oben schon bemerkt, erfüllt $\mathbb{Q}$ mit der üblichen Addition und Multiplikation und mit den bekannten Konstanten 0 und 1 die Körperaxiome (K1)–(K5).

Die ganzen Zahlen $\mathbb{Z}$ mit den üblichen Rechenoperationen erfüllen zwar (K1)–(K4), aber sie bilden keinen Körper, da zum Beispiel 2 in $\mathbb{Z}$ kein multiplikatives Inverses besitzt:
Es gibt keine ganze Zahl n mit $2 \cdot n = 1$.

Neben der Struktur eines Körpers, haben die rationalen Zahlen noch eine weitere wichtige Eigenschaft. Sie werden durch die Kleiner-Beziehung $<$ *angeordnet*.

Für je zwei verschiedene rationale Zahlen a und b gilt entweder $a < b$ ("a kleiner b") oder $a > b$ ("a größer b").

Es gelten folgende Regeln (Seite 29 im Skript):

1. $a < b \wedge b < c \Rightarrow a < c$
2. $a < b \Rightarrow a + c < b + c$
3. $a < b \Rightarrow a \cdot c < b \cdot c$, falls $c > 0$.
4. $a < b \Rightarrow a \cdot c > b \cdot c$, falls $c < 0$.

Wir schreiben $a \leq b$ für $(a < b \vee a = b)$ und lesen $\leq$ als "kleiner-gleich" und $\geq$ als "größer-gleich".

Für $\leq$ gelten ähnliche Regeln wie für $<$.

1. $a \leq b \wedge b \leq c \Rightarrow a \leq c$
2. $a \leq b \Rightarrow a + c \leq b + c$
3. $a \leq b \Rightarrow a \cdot c \leq b \cdot c$, falls $c \geq 0$.
4. $a \leq b \Rightarrow a \cdot c \geq b \cdot c$, falls $c \leq 0$.

Relationen

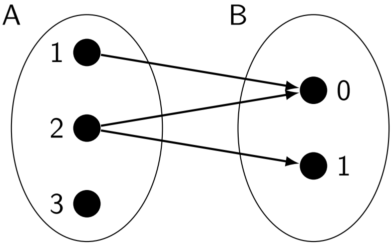
Definition 3.1

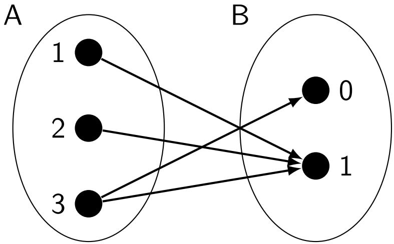
Eine *Relation* von A nach B ist eine Teilmenge R von $A \times B$. Eine Relation auf A ist eine Teilmenge von $A \times A$. Für $(a, b) \in R$ schreiben wir auch aRb.

Beispiel 3.2

1. Sei $A = \{1, 2, 3\}$ und $B = \{0, 1\}$. Dann sind $R_1, \ldots, R_4$ Relationen von A nach B:
   1.1 $R_1 = \{(1, 0), (2, 0), (2, 1)\}$.
   1.2 $R_2 = \{(1, 1), (2, 1), (3, 0), (3, 1)\}$
   1.3 $R_3 = A \times B$
   1.4 $R_4 = \emptyset$.
2. $R = \{(a, b) : a, b \in \mathbb{N} \wedge a < b\}$,
   $S = \{(a, b) : a, b \in \mathbb{N} \wedge a \leq b\}$ und
   $T = \{(a, b) : a, b \in \mathbb{N} \wedge a = b\}$ sind Relationen auf $\mathbb{N}$.

Wir können Relationen ähnlich wie Funktionen mit Hilfe von Pfeildiagrammen notieren. Hier sind zwei Diagramme für die Relationen $R_1 = \{(1,0),(2,0),(2,1)\}$ und $R_2 = \{(1,1),(2,1),(3,0),(3,1)\}$.





Definition 3.3

Sei A eine Menge und sei R eine Relation auf A.

1. R heißt *reflexiv*, falls für alle $a \in A$ das Paar (a, a) in R ist.
2. R heißt *irreflexiv*, falls R kein Paar der Form (a, a) enthält.
3. R heißt *symmetrisch*, falls für alle $(a, b) \in R$ auch $(b, a) \in R$ gilt.
4. R heißt *antisymmetrisch*, falls aus $(a, b) \in R$ und $a \neq b$ stets $(b, a) \notin R$ folgt.
5. R heißt *transitiv*, falls aus $(a, b) \in R$ und $(b, c) \in R$ stets $(a, c) \in R$ folgt.

Man beachte, dass irreflexiv nicht dasselbe ist wie nicht reflexiv.
Ebenso ist antisymmetrisch nicht dasselbe wie nicht symmetrisch.

Partitionen und Äquivalenzrelationen

Definition 3.4

Eine Relation R auf einer Menge A heißt Äquivalenzrelation, falls R reflexiv, transitiv und symmetrisch ist.
Ist R eine Äquivalenzrelation auf A so bezeichnen wir für jedes $a \in A$ mit $[a]_R$ die Menge $\{b \in A : (a, b) \in R\}$ und nennen diese Menge die *Äquivalenzklasse* von a.

Satz 3.5

Sei A eine Menge und R eine Äquivalenzrelation auf A.Dann gilt für alle $a, b \in A$ entweder $[a]_R \cap [b]_R = \emptyset$ oder $[a]_R = [b]_R$. Der zweite Fall tritt genau dann ein, wenn aRb gilt.

Für eine Äquivalenzrelation R auf einer Menge A ist $\{[a]_R : a \in A\}$ eine *Partition* von A.

Definition 3.6

Sei A eine Menge, I eine Indexmenge und für alle $i \in I$ sei $K_i \subseteq A.P = \{K_i : i \in I\}$ ist eine *Partition* von A, falls gilt:

1. Für alle $i, j \in I$ mit $i \neq j$ ist $K_i \cap K_j = \emptyset$.
2. Es gilt $\bigcup_{i \in I} K_i = A$.

Dabei ist $\bigcup_{i \in I} K_i$ die Menge $\{x : \exists i \in I(x \in K_i)\}$.

Korollar 3.7

Es sei A eine Menge. Für jede Äquivalenzrelation auf A bilden die Äquivalenzklassen eine Partition von A.Umgekehrt gibt es für jede Partition von A eine Äquivalenzrelation, deren Äquivalenzklassen genau die Mengen in der Partition sind.

Beispiel 3.8

Sei $m \in \mathbb{N}$ und $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b (\text{mod } m)\}$. Dann ist R eine Äquivalenzrelation auf $\mathbb{Z}$, deren Äquivalenzklassen *Restklassen modulo m* genannt werden.

Die Anzahl der Restklassen modulo m ist genau m. Die verschiedenen Restklassen sind die Mengen $\{m \cdot q + 0 : q \in \mathbb{Z}\}$, $\{m \cdot q + 1 : q \in \mathbb{Z}\}, \ldots, \{m \cdot q + (m - 1) : q \in \mathbb{Z}\}$.