Repetitorium WiSe 2013/14

16.10.2013

elementare Beweismethoden, vollständige Induktion

Logische Grundlagen: Sind A, B Aussagen, so auch $A \wedge B$, $A \vee B$, $A \Rightarrow B$, $A \Leftarrow B$, $A \Leftrightarrow B$, $\neg A$

Es gilt: $(A \Rightarrow B) \Leftrightarrow \neg A \vee B$

Beweismethoden: (Satz: $A \Rightarrow B$) — A: Vor., B: Beh.

- direkt (Angabe einer Schlusskette), vollst. Induktion
  ⌜$A \Rightarrow B$ wird bewiesen durch Schlusskette $A \Rightarrow C_1 \Rightarrow C_2 \Rightarrow \dots \Rightarrow C_n \Rightarrow B$⌟
- indirekt (Widerspruchsbeweis, Kontraposition)
  ⌜Zeigen: $A \wedge \neg B \Rightarrow$ falsche Aussage, z.B. $0 = 1$,
  denn: $\neg(A \wedge \neg B) \Leftrightarrow \neg A \vee B \Leftrightarrow (A \Rightarrow B)$
  bzw.: $\underbrace{\neg B \Rightarrow \neg A}_{\Leftrightarrow (A \Rightarrow B)}$ beim Kontrapositionsbeweis⌟

Vollständige Induktion: Beweis einer Beh. der Form: $\forall n \in \mathbb{N}, n \geq n_0 : A(n)$

Induktionsprinzip:
- Induktionsanfang: $A(n_0)$ ist richtig
- Induktionsschritt: Für alle $n \in \mathbb{N}$ mit $n \geq n_0$ gilt die Implikation $A(n) \Rightarrow A(n+1)$.

Der Beweis einer Aussage mittels vollst. Induktion besteht aus diesen beiden (Teil-)beweisen!

Bsp.: Beweis von $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ ⌜K.F. Gauß⌟

2. Fassung der vollständigen Induktion:

1.) Zeigen, dass $A(n_0)$ gilt.

2.) Unter der Vor., dass $A(n)$ für alle n mit $n_0 \leq n < k$ gilt, zeigt man die Gültigkeit von $A(k)$.

setzt Gültigkeit von $A(n-1), A(n-2)$ voraus → Bsp.: Beweis von $F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$ für die Fibonaccizahlen ($F_n = F_{n-1} + F_{n-2}$)
$1, 1, 2, 3, 5, 8, 13, \dots$

Aufbau des Zahlensystems

$\mathbb{N}$ natürliche Zahlen: $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ ev. $\rightsquigarrow$ vollst. Induktion

$\cap$

$\mathbb{Z}$ ganze Zahlen: $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$

$\cap$

$\mathbb{Q}$ Körper, Körperaxiome: Relationen $+, \cdot$,
Rechnen mit Zahlen: assoziativ, Ex. des neutralen El., Ex. des Inversen (außer mult. Inv. der 0, ex. nicht)
kommutativ, distributiv

$\cap$

$\mathbb{R}$ reelle Zahlen: Körperaxiome, Anordnungsaxiome, Vollständigkeitsaxiom

$\cap$

$\mathbb{C}$ Komplexe Zahlen: $\mathbb{C} = \mathbb{R} + i\mathbb{R} := \{\underset{\text{Realteil}}{a} + i\underset{\text{Imaginärteil}}{b} \mid a, b \in \mathbb{R}\}$
mit $i^2 = -1$, nicht anordenbar! (aber vollst.)

Körperaxiome: Eine Menge K mit zwei Verknüpfungen $+$ und $\cdot$ heißt Körper, falls gilt:

$\boxed{1}$ $(K, +)$ ist abelsche Gruppe,

$\boxed{2}$ $(K \setminus \{0\}, \cdot)$ ist abelsche Gruppe,

$\boxed{3}$ $\forall a, b, c \in K: \; a \cdot (b + c) = a \cdot b + a \cdot c$ (Distributivgesetz)

Gruppenaxiome: Eine Menge G mit einer Operation $\circ$ (d.h. einer Abbildung $\circ: G \times G \to G$, wir schreiben $a \circ b := \circ(a, b)$ für $a, b \in G$) heißt Gruppe, falls gilt:

1. $\forall a, b, c \in G: \; (a \circ b) \circ c = a \circ (b \circ c)$ (Assoziativ)
2. $\exists 0 \in G \; \forall a \in G: \; 0 \circ a = a \circ 0 = a$ (Ex. neutr. El.)
3. $\forall a \in G \; \exists b \in G: \; a \circ b = b \circ a = 0$ (Ex. inv. El.)

G heißt abelsch, falls $\forall a, b \in G: \; a \circ b = b \circ a$ (Kommutativ)

<u>Grundregeln für Gruppen:</u> Sei $(G,\cdot)$ multipl. geschriebene Gruppe.

- Kürzungsregel: $ax = ay \Rightarrow x = y$
  $xa = ya \Rightarrow x = y$
- Jede der Glgn. $ax = b$ und $ya = b$ besitzt genau eine Lösung $x \in G$ bzw. $y \in G$
- Es gilt $(ab)^{-1} = b^{-1}a^{-1}$ $\ulcorner (ab)\cdot(b^{-1}a^{-1}) = abb^{-1}a^{-1} = \underbrace{aa^{-1}}_{=1} \lrcorner$

Es gilt: Der Körper $\mathbb{R}$ der reellen Zahlen ist "der" bis auf Isomorphie eindeutig bestimmte <u>vollständige angeordnete Körper.</u>

<u>Anordnungen:</u>
Eine Relation "<" auf einer Menge M heißt (totale oder lineare) Ordnung auf M, wenn gilt:

(1) Transitivität: $\forall x,y,z \in M: \; x<y \wedge y<z \Rightarrow x<z$
(2) Trichotomie: $\forall x,y \in M: \; x<y \;\dot\vee\; y<x \;\dot\vee\; x=y$

Def.: Ein angeordneter Körper K ist ein Körper zusammen mit einer Ordnung auf K, wenn gilt:

(1) Monotonie der Addition: $\forall x,y,z \in K: x<y \Rightarrow x+z < y+z$
(2) Monotonie der Multiplikation: $\forall x,y,z \in K: x<y \wedge z>0 \Rightarrow xz < yz$

- Ein Körper heißt vollständig, wenn die Vollständigkeitsbedingung darin gilt (vgl. nächste Sitzung).

- Der Körper $\mathbb{C}$ der Komplexen Zahlen wird erklärt durch

$$\mathbb{C} := \{x+iy \mid x,y \in \mathbb{R}\}$$

und $(x+iy)+(u+iv) := (x+u)+i(y+v)$ Komponentenweise

sowie $(x+iy)\cdot(u+iv) := (xu-yv)+i(xv+yu)$

Darin gilt $i^2 = (0+i\cdot 1)\cdot(0+i\cdot 1) = (0\cdot 0 - 1\cdot 1) + i(0\cdot 1 + 1\cdot 0) = -1$.
<u>Wichtig:</u> $\mathbb{C}$ ist nicht anordenbar!

Summen, Produkte, Potenzen:

Für reelle Zahlen a_k setzt man

$$\sum_{k=1}^{1} a_k := a_1, \quad \sum_{k=1}^{n+1} a_k := \left(\sum_{k=1}^{n} a_k\right) + a_{n+1} \quad \rightsquigarrow \quad \text{Summe: } \sum_{k=1}^{n} a_k$$

$$\prod_{k=1}^{1} a_k := a_1, \quad \prod_{k=1}^{n+1} a_k := \left(\prod_{k=1}^{n} a_k\right) \cdot a_{n+1} \quad \rightsquigarrow \quad \text{Produkt: } \prod_{k=1}^{n} a_k$$

und für reelles a auch $a^0 := 1,\ a^1 := a,\ a^{n+1} := a^n \cdot a$. $\rightarrow$ Potenz a^n

$\rightsquigarrow$ $\boxed{\text{Anhang: Potenzen, Exponenten, Wurzeln}}$

Indexverschiebung: $\displaystyle\sum_{k=m}^{n} a_k = \sum_{k=m+p}^{n+p} a_{k-p}$, ebenso für $\prod$

Teleskopsumme: $\displaystyle\sum_{k=m}^{n} (a_k - a_{k-1}) = a_n - a_{m-1}$

Doppelsumme: $\displaystyle\sum_{k=1}^{n}\left(\sum_{j=1}^{m} a_{kj}\right) = \sum_{j=1}^{m}\left(\sum_{k=1}^{n} a_{kj}\right)$

Produkt von Summen: $\displaystyle\left(\sum_{k=1}^{n} a_k\right)\cdot\left(\sum_{j=1}^{m} b_j\right) = \sum_{k=1}^{n}\left(\sum_{j=1}^{m} a_k b_j\right)$

$$= \sum_{j=1}^{m}\left(\sum_{k=1}^{n} a_k b_j\right)$$

Summenformeln:

1) (Endliche) Geometrische Summe:

Für $x \neq 1$ und $n, m \in \mathbb{N}$, $n \geq m$, gilt:

$$\sum_{k=0}^{n} x^k = \frac{1 - x^{n+1}}{1 - x}, \quad \sum_{k=m}^{n} x^k = x^m \sum_{k=0}^{n-m} x^k = \frac{x^m - x^{n+1}}{1 - x}$$

2) Potenzsummen: $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$, $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$,

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

3) Binomischer Satz: $a,b \in \mathbb{R}, n \in \mathbb{N}_0 \Rightarrow (a+b)^n = \sum_{k=0}^{n} \underbrace{\binom{n}{k}}_{\text{Binomialkoeff.}} a^k b^{n-k}$

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$,

$n! = 1 \cdot 2 \cdot \ldots \cdot n$ Fakultät

Ungleichungen:

1) Bernoulli-Unglg.: $x \in \mathbb{R}, x \geq -1, n \in \mathbb{N}_0 \Rightarrow (1+x)^n \geq 1+nx$

2) Unglg. vom harmonischen, geometrischen und arithmetischen Mittel:

$$n \in \mathbb{N}, a_k \in \mathbb{R}, a_k > 0 \Rightarrow \frac{n}{\frac{1}{a_1} + \ldots + \frac{1}{a_n}} \leq \sqrt[n]{a_1 \cdots a_n} \leq \frac{a_1 + \ldots + a_n}{n}$$

3) Cauchy-Schwarz-Unglg.:

$$n \in \mathbb{N}, x_k, y_k \in \mathbb{R} \Rightarrow \left(\sum_{k=1}^{n} x_k y_k\right)^2 \leq \left(\sum_{k=1}^{n} x_k^2\right) \cdot \left(\sum_{k=1}^{n} y_k^2\right)$$

[Insb. für das Skalarprodukt von Vektoren $\underline{x}, \underline{y}$ in $\mathbb{R}^n$:

$$|\langle \underline{x}, \underline{y} \rangle| \leq \|\underline{x}\| \cdot \|\underline{y}\|,$$

"=" gilt $\Leftrightarrow$ $\underline{x}, \underline{y}$ lin. abh.]

4) Hölder-Unglg. (Verallg. der CS-Unglg.):

$$p,q > 1, \frac{1}{p} + \frac{1}{q} = 1, x_k, y_k \in \mathbb{R} \Rightarrow \sum_{k=1}^{n} |x_k y_k| \leq \left(\sum_{k=1}^{n} |x_k|^p\right)^{\frac{1}{p}} \cdot \left(\sum_{k=1}^{n} |y_k|^q\right)^{\frac{1}{q}}$$

Mengensysteme: 1. aus endl. vielen Mengen: $M_1, M_2, \dots, M_k$
2. aus abzählbar ∞ vielen Mengen: $M_1, M_2, \dots$
3. allgemeiner Art: $(M_i \mid i \in I)$,
I heißt Indexmenge
(bei $I = \mathbb{N}$ liegt Fall 2. vor ("Folge"))

Ein Mengensystem $(M_i \mid i \in I)$
heißt Familie von Mengen. Schreibweise auch: $(M_i)_{i \in I}$

$\rightsquigarrow$ Durchschnitt / Vereinigung von Mengenfamilien: $\bigcap_{i \in I} M_i$, $\bigcup_{i \in I} M_i$

Kartesisches Produkt: $\bigtimes_{i \in I} M_i$, bei endl. vielen: $\underbrace{M_1 \times M_2 \times \dots \times M_k}_{\text{Menge aller } k\text{-Tupel } (m_1, \dots, m_k), \text{ die } m_i \in M_i}$

$M \times N := \{ \underbrace{(m,n)}_{\text{Paar, 1. Eintrag} = m, \text{ 2. Eintrag} = n} \mid m \in M, n \in N \}$

beachten:
$$\{m, n\} = \{n, m\}, \quad \text{aber } (m,n) \neq (n,m)$$

Formal: $(m,n) := \{ \{m\}, \{m,n\} \}$,
erfüllt $(m,n) = (x,y) \Leftrightarrow m = x \wedge n = y$

Relationen: Sind A, B Mengen, heißt eine Teilmenge $R \subseteq A \times B$ Relation.

Sei $R \subseteq A \times A$ eine Relation auf A.

R heißt reflexiv $:\Leftrightarrow \forall x \in A: (x,x) \in R$

" symmetrisch $:\Leftrightarrow \forall x,y \in A: (x,y) \in R \Rightarrow (y,x) \in R$

" antisymmetrisch $:\Leftrightarrow \forall x,y \in A: (x,y) \in R \wedge (y,x) \in R \Rightarrow x = y$

" transitiv $:\Leftrightarrow \forall x,y,z \in A: (x,y) \in R \wedge (y,z) \in R \Rightarrow (x,z) \in R$

" konnex/linear $:\Leftrightarrow \forall x,y \in A: (x,y) \in R \vee (y,x) \in R$ [je zwei El. aus A sind vergleichbar]

Eine Relation R auf A, also $R \subseteq A \times A$, heißt

Äquivalenzrelation $\Leftrightarrow$ R ist reflexiv, symmetrisch und transitiv

Halbordnung $\Leftrightarrow$ R ist reflexiv, antisymmetrisch und transitiv

Ordnung $\Leftrightarrow$ R ist Halbordnung und konnex/linear
($\rightsquigarrow$ Trichotomie, vgl. oben)

Bsp. Halbordnung: $A = \{\emptyset, \{2\}, \{2,3\}, \{1,2\}\}$, $\subseteq$

$$\begin{array}{ccc} \{2,3\} & & \{1,2\} \\ \cup\!\shortmid & & \not\subseteq \\ & \{2\} & \\ & \cup\!\shortmid & \\ & \emptyset & \end{array}$$

Bsp. Ordnung: $A = \{\emptyset, \{2\}, \{1,2\}\}$

$$\begin{array}{c} \{1,2\} \\ \cup\!\shortmid \\ \{2\} \\ \cup\!\shortmid \\ \emptyset \end{array}$$

Bei Ä-Relationen üblich: schreibe xRy statt $(x,y) \in R$,
auch meist mit $\sim$ statt R, also in der Form $x \sim y$ für $(x,y) \in \sim$.

Äquivalenzklassen: $\sim$ Ä-Rel. $\Rightarrow$ $a/\!\sim \; := \{b \in A \mid b \sim a\} \subseteq A$ für $a \in A$
heißen **Äquivalenzklassen** von $\sim$.

Bsp.: Auf $\mathbb{Z}$ ist durch $x \sim y \Leftrightarrow 5 \mid x - y$ eine Ä-Rel. erklärt.
Die Ä-Klassen sind $\underline{0} = \{x \in \mathbb{Z};\ 5 \mid x\}$, $\underline{1} = \{x \in \mathbb{Z};\ 5 \mid x-1\}$,
$\ldots$, $\underline{4} = \{x \in \mathbb{Z};\ 5 \mid x-4\}$. $\rightsquigarrow$ $\mathbb{Z} = \underline{0} \,\dot\cup\, \underline{1} \,\dot\cup \ldots \dot\cup\, \underline{4}$

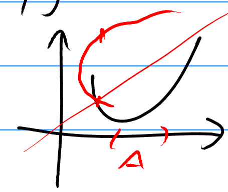
Abbildungen/Funktionen:

Eine Relation f zwischen X und Y (d.h. $f \subseteq X \times Y$) heißt **Abbildung**,
falls gilt: $\forall x \in X\ \exists! y \in Y:\ (x,y) \in f$
die Eindeutigkeit hier nennt man "**Rechtseindeutigkeit**":
$(x,y) \in f \wedge (x,z) \in f \Rightarrow y = z$

Schreibweise für eine Abb.: $f: \begin{cases} X \to Y \\ x \mapsto y = f(x) \end{cases}$

Bild von f: $f(X) := \{f(x) \mid x \in X\} = \{y \in Y \mid \exists x \in X : f(x) = y\} \subseteq Y$

Umkehrrelation: $f^{-1} := \{(y,x) \mid (x,y) \in f\} \subseteq Y \times X$



Seien $A \subseteq X$, $B \subseteq Y$.

Bildmenge von A: $f(A) := \{f(x) \mid x \in A\}$

Urbildmenge von B: $f^{-1}(B) := \{x \in X \mid f(x) \in B\}$

Spezielle Funktionen: $f: X \to Y$ heißt

injektiv $\Leftrightarrow$ $(x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)) \Leftrightarrow (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$

surjektiv $\Leftrightarrow$ $\forall y \in Y \; \exists x \in X : y = f(x)$

bijektiv $\Leftrightarrow$ f inj. $\wedge$ f surj.

Abzählbare Mengen: Eine Menge M heißt abzählbar ∞, falls eine Abb. $f: \mathbb{N} \to M$ ex., die bijektiv ist.

Bsp.: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, aber $\mathbb{R}$ ist überabzählbar (Cantorsches Diag.-verfahren)

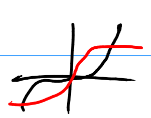
Die abzählbare Vereinigung abzählbarer Mengen ist abzählbar.

Anhang: Potenzen, Exponenten, Wurzeln

Für $a \in \mathbb{R}$, $n \in \mathbb{N}_0$: $a^0 := 1$, $a^1 := a$, $a^{n+1} := a^n \cdot a$. $\to$ Potenz a^n

$\rightsquigarrow$ Für $r, s \in \mathbb{N}_0$, $a, b \in \mathbb{R}$: $a^r \cdot a^s = a^{r+s}$, $(a^r)^s = a^{r \cdot s}$, $(a \cdot b)^r = a^r \cdot b^s$

$a^{\sqrt{2}}$?



Erweiterung auf rationale Exponenten $r = \frac{z}{m}$ mit $z \in \mathbb{Z}$, $m \in \mathbb{N}$

nur möglich, wenn $a \geq 0$ ist: $(-2)^{\frac{1}{2}}$ ex. nicht, $\ulcorner ((-2)^{\frac{1}{2}})^2 = -2$ ↯

und $(-8)^{\frac{1}{3}}$ auch nicht def., sonst: $-2 = (-8)^{\frac{1}{3}} = (-8)^{\frac{2}{6}} = ((-8)^2)^{\frac{1}{6}} = 64^{\frac{1}{6}} = 2$ ↯.

Für $a \geq 0$ ist $a^{\frac{1}{n}}$ definiert als diejenige reelle Zahl $y \geq 0$ mit $y^n = a$ (damit $(a^{\frac{1}{n}})^n = a^{\frac{1}{n} \cdot n} = a^{\frac{n}{n}} = a^1 = a$ gilt), die Existenz dieser Zahl ist gesichert mit dem Vollständigkeitsaxiom. (s. nächstes Mal)

Bem.: $\sqrt[n]{a}$ ist eine andere Schreibweise für $a^{\frac{1}{n}}$

$\sqrt[m]{a^z}$ 〃 〃 〃 $a^{z/m}$