

Vorkurs Theoretische Informatik

Induktion, Prädikatenlogik und Grundlagen der modularen
Arithmetik

reloading 0 % complete...

Arbeitskreis Theo-Vorkurs

Donnerstag, 2. Oktober 2025

Fachgruppe Informatik Universität Stuttgart

1. Vollständige Induktion

Funktionsweise

Formalere Definition

2. Prädikatenlogik

Grundlagen + Beispiel

Generisch

3. Modulare Arithmetik

4. Wiederholung

5. Wiederholungsaufgaben

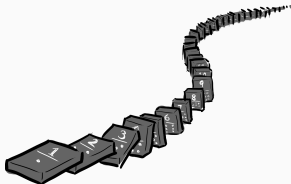
Vollständige Induktion

reloading 1.41 % complete...

Zeige Aussagen der Form:

Für alle $n \in \mathbb{N}$ gilt...

1. Zeige Aussage für das kleinste Element
2. Zeige, dass Aussage auch für das folgende Element gilt.
3. Zeige, dass Aussage auch für das folgende Element gilt.
4. Zeige, dass Aussage auch für das folgende Element gilt.
5. Zeige, dass Aussage auch für das folgende Element gilt.
6. Zeige, dass Aussage auch für das folgende Element gilt.
7. ...



Vollständige Induktion

reloading 2.82 % complete...

Funktionsweise

Zeige Aussagen der Form:

Für alle $n \in \mathbb{N}$ gilt...

1. Induktionsanfang

Zeige Aussage für das kleinste Element

2. Induktionsvoraussetzung

Zeige, unter der Voraussetzung:

die Aussage gelte für beliebiges n ,...

3. Induktionsschritt

...dann gilt die Aussage auch für dessen Nachfolger $n + 1$.

4. $\leadsto$ Aussage gilt für alle $n \in \mathbb{N}$.

$$\sum_{i=0}^n (2i + 1) = (n + 1)^2, \quad \forall n \in \mathbb{N}.$$



Zeigen Sie $\sum_{i=0}^n (2i + 1) = (n + 1)^2, \quad \forall n \in \mathbb{N}.$

Induktionsanfang (IA)

Zeige Aussage gilt für $n := 0$:

$$\begin{array}{lll} \sum_{i=0}^0 (2i + 1) & \stackrel{!}{=} & (0 + 1)^2 \\ \iff 2 \cdot 0 + 1 & \stackrel{!}{=} & 1^2 \\ \iff 1 & = & 1 \quad \checkmark \end{array}$$

Zeigen Sie $\sum_{i=0}^n (2i + 1) = (n + 1)^2, \quad \forall n \in \mathbb{N}.$

Induktionsanfang (IA)

Aussage gilt für $n := 0$, da $\sum_{i=0}^0 (2i + 1) = (0 + 1)^2.$

Induktionsvoraussetzung (IV)

Ang. Aussage gilt für (ein beliebiges aber festes) $n \in \mathbb{N}.$

Induktionsschritt (IS)

Zeige Aussage gilt für alle $n + 1$ unter Nutzung der (IV):

$$\sum_{i=0}^{n+1} (2i + 1) \stackrel{!}{=} ((n + 1) + 1)^2$$

Induktionsschritt

Zeige Aussage gilt für alle $n + 1$ unter Nutzung der IV:

$$\begin{aligned} & \sum_{i=0}^{n+1} (2i + 1) && \stackrel{!}{=} && ((n + 1) + 1)^2 \\ \Leftrightarrow & \sum_{i=0}^n (2i + 1) + \sum_{i=n+1}^{n+1} (2i + 1) && \stackrel{!}{=} && (n + 2)^2 \\ \Leftrightarrow & \sum_{i=0}^n (2i + 1) + (2(n + 1) + 1) && \stackrel{!}{=} && n^2 + 2 \cdot 2n + 2^2 \\ \stackrel{IV}{\Leftrightarrow} & (n + 1)^2 + (2(n + 1) + 1) && \stackrel{!}{=} && n^2 + 4n + 4 \\ \Leftrightarrow & n^2 + 2n + 1^2 + 2n + 2 + 1 && \stackrel{!}{=} && n^2 + 4n + 4 \\ \Leftrightarrow & n^2 + 4n + 4 && = && n^2 + 4n + 4 \end{aligned}$$

Zeigen Sie $\sum_{i=0}^n (2i + 1) = (n + 1)^2, \quad \forall n \in \mathbb{N}.$

Induktionsanfang (IA)

Aussage gilt für $n := 0$, da $\sum_{i=0}^0 (2i + 1) = 1^2.$

Induktionsvoraussetzung (IV)

Ang. Aussage gilt für (ein beliebiges aber festes) $n \in \mathbb{N}.$

Induktionsschritt (IS)

Aussage gilt für alle $n + 1$ unter Nutzung der IV, da

$$\sum_{i=0}^{n+1} (2i + 1) = ((n + 1) + 1)^2$$

↪ Aussage gilt für alle $n.$



Aufgaben

Versuche dich an den folgenden Induktionsbeweisen.

Normal

$$\sum_{i=0}^n i = \frac{n(n+1)}{2}, \quad \forall n \in \mathbb{N}$$

Schwerer

$$\prod_{i=1}^n 4^i = 2^{n(n+1)}, \quad \forall n \in \mathbb{N} \setminus \{0\}$$

Vollständige Induktion



reloading 21.13 % complete...

Formalere Definition

Definition nochmal formaler

$$(\forall n \in \mathbb{N}_{n_0} : P(n)) \iff (\underbrace{P(n_0)}_{\text{IA}} \wedge \overbrace{\forall n \in \mathbb{N}_{n_0} : (\underbrace{P(n)}_{\text{IV}} \implies P(n+1)))}^{\text{IS}})$$

1. **IA:** $n = n_0$
2. **IS:** Sei $n \in \mathbb{N}_{n_0}$ beliebig. Ang. es gilt $P(n)$. _(IV)
3. Zeigen, dass $P(n+1)$ gilt, unter Verwendung von $P(n)$ _(IV)

Die folgende Induktion zeigt eine seltsame Aussage.

Ist der Beweis korrekt geführt? Was ist passiert?

Sei $A(n) :=$ In einem Wald aus n Bäumen haben alle die selbe Größe.

Zu zeigen: $A(n)$ gilt für alle $n \in \mathbb{N} \setminus \{0\}$.

Induktionsanfang (IA)

$A(1)$: Aussage gilt für $n := 1$, da ein Baum nur eine Größe haben kann.

Induktionsvoraussetzung (IV)

Ang. $A(n)$ gilt für $n \in \mathbb{N}$ mit $n \geq 1$.

Induktionsschritt (IS)

Zeige Aussage gilt für alle $n + 1$ unter Nutzung der IV:

D.h. wir zeigen $A(n + 1) =$ In einem Wald aus $n + 1$ Bäumen haben alle die selbe Größe.

Induktionsschritt (IS)

Wir betrachten einen Wald aus $n + 1$ Bäumen:



Wir sondern einen Baum aus und betrachten den Rest. Nach I.V. haben diese alle die selbe Größe.



Jetzt sondern wir einen anderen Baum aus.



Die übrigen n Bäume haben nach I.V. wieder die selbe Größe.



Also haben alle $n + 1$ Bäume die selbe Größe. $\leadsto A(n)$ gilt für alle n .

Prädikatenlogik

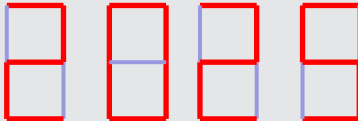


reloading 26.76 % complete...

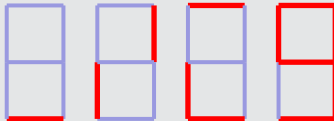
Grundlagen + Beispiel

7-Segment Anzeigen

Können Zahlen zeigen



Zeigen manchmal wirres Zeug



Wir brauchen einen *Checker*:

$$P_{\text{Zahl}} \left(\begin{array}{|c|} \hline \text{ } \\ \hline \end{array} \right) P_{\text{Zahl}} \left(\begin{array}{|c|} \hline \text{ } \\ \hline \end{array} \right)$$

Wenn wir in diesen *Checker* (genannt Prädikat) eine Anzeige einsetzen, haben wir eine logische Aussage

Wahr, wenn eine Zahl zu sehen ist

Falsch, wenn keine Zahl zu sehen ist

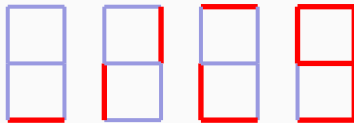
Eigentlich ist es die Lückentext-Aussage:
In der Anzeige __ kann man eine Zahl sehen.

Sind die folgenden Aussagen wahr oder falsch?

Normal

- $A_1: P_{\text{ZAHL}}(\text{E})$
- $A_2: P_{\text{ZAHL}}(\text{F})$
- $A_3: P_{\text{ZAHL}}(\text{H})$
- $A_4: P_{\text{ZAHL}}(\text{H})$

Wie reparieren wir die Anzeige?



Wir brauchen eine Funktion, die Segmente einschaltet

$$f_{\text{ON}} \left(\begin{array}{|c|c|} \hline \text{red} & \text{blue} \\ \hline \text{red} & \text{blue} \\ \hline \end{array}, \begin{array}{|c|c|} \hline \text{blue} & \text{red} \\ \hline \text{blue} & \text{red} \\ \hline \end{array} \right) = \begin{array}{|c|c|} \hline \text{red} & \text{red} \\ \hline \text{red} & \text{red} \\ \hline \end{array}$$

- $f_{\text{ON}}(\text{8}, \text{2}) = \text{2}$
- $f_{\text{ON}}(\text{8}, \text{9}) = \text{0}$
- $f_{\text{ON}}(\text{8}, \text{8}) = \text{2}$
- $f_{\text{ON}}(\text{9}, \text{X}) = \text{5}$

$$f_{\text{Off}} \left(\begin{array}{|c|c|} \hline \text{red} & \text{blue} \\ \hline \text{red} & \text{red} \\ \hline \end{array}, \begin{array}{|c|} \hline \text{blue} \\ \hline \end{array} \right) = \begin{array}{|c|} \hline \text{red} \\ \hline \text{red} \\ \hline \end{array}$$

Kombiniert mit unserem Prädikat:

$$P_{\text{ZAHL}} \left(f_{\text{ON}} \left(\begin{array}{|c|c|} \hline \text{red} & \text{red} \\ \hline \text{blue} & \text{blue} \\ \hline \end{array}, \begin{array}{|c|c|} \hline \text{blue} & \text{blue} \\ \hline \text{red} & \text{red} \\ \hline \end{array} \right) \right)$$

Diese Aussage ist wahr

Allgemeiner:

$$U = \{ \begin{array}{|c|c|} \hline \text{red} & \text{red} \\ \hline \text{blue} & \text{blue} \\ \hline \end{array}, \begin{array}{|c|c|} \hline \text{blue} & \text{blue} \\ \hline \text{red} & \text{red} \\ \hline \end{array}, \dots \}$$

$$\forall x \in U : \exists y \in U : P_{\text{ZAHL}}(f_{\text{ON}}(x, y))$$

Das **Universum** U ist die Menge aller Werte, die in unsere Formel eingesetzt werden können. Es darf **nicht** leer sein!

Finde Anzeigen für die Variablen X, Y , für die die Aussage stimmt

Normal

- $P_{\text{ZAHL}} (f_{\text{ON}} (\text{B}, x_1))$
- $P_{\text{ZAHL}} (f_{\text{OFF}} (x_2, y_2))$
- $P_{\text{ZAHL}} (f_{\text{OFF}} (x_3, \text{B})) \wedge P_{\text{Zahl}} (f_{\text{ON}} (x_3, \text{B}))$
- $\neg P_{\text{ZAHL}} (f_{\text{ON}} (f_{\text{ON}} (\text{B}, x_4), \text{B}))$

Beweise, ob die folgenden Aussagen wahr oder falsch sind

Etwas schwerer

- $A_5: \forall X : P_{\text{ZAHL}} (f_{\text{ON}} (x, \text{B}))$
- $A_6: \forall X \exists y : P_{\text{ZAHL}} (X) \implies \neg P_{\text{ZAHL}} (f_{\text{ON}} (x, y))$

Fällt euch ein Prädikat $P_?$ ein, für das die folgende Aussage wahr ist:

Mit $U_{80} = \{\text{8}, \text{0}\} \subseteq U$

$$\forall x \in U_{80} : P_?(x)$$

- Prädikatenlogische Formeln haben ihre Prädikate und Funktionen nicht unbedingt festgelegt
- Sie können auch aus Prädikatymbolen und Funktionssymbole bestehen
- Unsere Aufgabe ist dann, sie zu interpretieren

Prädikate

- $P_{ZAHL}(x)$: Die Anzeige x zeigt eine Zahl.
- $P_{<7}(x)$: Die Anzeige x hat maximal 6 leuchtende Segmente.
- $P_{=}(x, y)$: Die Anzeigen x und y sind gleich.
- $P_{>}(x, y)$: Die Anzeige x hat mehr leuchtende Segmente als die Anzeige y.

Funktionen

- $f_{ON}(x, y)$: Schalte alle Segmente an, welche in x oder y an sind.
- $f_{OFF}(x, y)$: Schalte alle Segmente an, welche in x and sind aber nicht in y .
- $f_{INV}(x)$: Schalte alle Segmente an, welche in x aus sind.
- $f_{COUNT}(x)$: Zeige die Zahl an, die angibt wie viele Segmente in x an sind.

Das Universum

$$U = \{0, 0, 5, 0, 0, 0, 6, 9, \dots\}$$

Nun wollen wir für die folgende prädikantenlogische Formel eine Interpretation erstellen:

$$\forall x \exists y : P_0(f_0(x), f_1(y)) \wedge P_1(a)$$

- $I(P_0) = P_{=}$

- $I(f_0) = f_{COUNT}$

- $I(f_1) = f_{INV}$

- $I(P_1) = P_{ZAHL}$

- $I(a) = 4$

- $I(P_0) = P_{=}$

- $I(f_0) = f_{COUNT}$

- $I(f_1) = f_{COUNT}$

- $I(P_1) = P_{<7}$

- $I(a) = 6$

Finde Interpretationen, für die die Aussagen stimmen

Normal

- $A_1: \neg P_0(f_0(a, b), f_1(b, a))$
- $A_2: \forall x \exists y : \neg P_0(f_0(x, y), f_1(y, x))$
- $A_3: \forall x : P_0(f_0(x, a), x)$
- $A_4: \forall x, y : P_0(x, y) \implies P_0(y, x)$

Etwas schwerer

- $A_5: \forall x \exists y : P_0(f_0(x), f_0(y)) \implies P_1(y)$
- $A_6: \forall x, y : P_0(f_0(x), y) \implies P_1(y)$
- $A_7: (\forall x : P_0(x, x) \wedge P_0(x, f_0(a))) \wedge (\forall y : \neg P_0(y, f_0(a)) \wedge \neg P_0(y, y))$

Prädikatenlogik



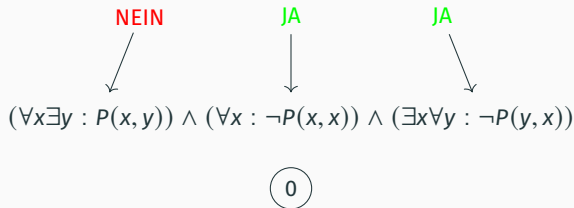
Generisch

- Eigentlich haben wir kein Universum, keine Prädikate und keine Funktionen vorgegeben
- Gegeben ist nur eine Prädikatenlogische Formel
- Wir müssen bestimmen ob diese irgendwie erfüllbar ist

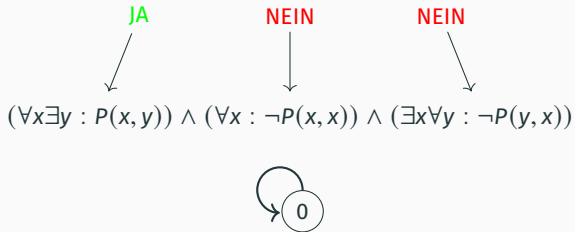
$$(\forall x \exists y : P(x, y)) \wedge (\forall x : \neg P(x, x)) \wedge (\exists x \forall y : \neg P(y, x))$$

$U = \emptyset$ müssen wir nicht testen, da das Universum nicht leer sein darf.

Dieses Beispiel wurde aus der Ergänzung für Theo II 2018 von Carlos Carmino übernommen.



Was ist mit dem Universum, das ein Element hat. Nennen wir das Element mal 0

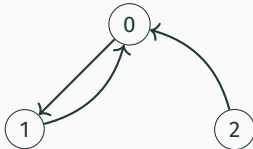


Was ist mit dem Universum, das ein Element hat. Nennen wir das Element mal 0

JA JA JA

↓ ↓ ↓

$$(\forall x \exists y : P(x, y)) \wedge (\forall x : \neg P(x, x)) \wedge (\exists x \forall y : \neg P(y, x))$$



Lasst es uns mal mit $U = \{0, 1, 2\}$ probieren

Achtung: Wir müssen das Ergebnis formal aufschreiben!

Das Universum

$$U = \{0, 1, 2\}$$

$$I(P) = \{(0, 1), (1, 0), (2, 1)\}$$

$$I(f) = \{0 \mapsto 1, 1 \mapsto 2, 2 \mapsto 0\}$$

$$I(a) = 0$$

alle Kombinationen für die das Prädikat zu einer wahren Aussage wird

Wenn eine Konstante enthalten wäre, wird sie so angegeben

Wenn eine Funktion enthalten wäre, wird diese so angegeben

Finde Interpretationen, für die die Aussagen stimmen

Normal

- $\forall x : P_1(x, f_1(x))$
- $(\forall x \forall y : P_2(x, y)) \wedge (\forall x : \neg P_2(a_2, x))$ mit a_2 Konstante
- $\forall x : (P_{3a}(x, f_3(x)) \wedge P_{3b}(f_3(x), x))$ mit $U = \mathbb{N}$

Schwer

- $(\forall x \forall y \forall z : (P_4(x, y) \wedge P_4(y, z)) \implies P_4(x, z)) \wedge$
 $(\forall x \forall y : P_4(x, y) \implies P_4(y, x)) \wedge (\forall x : \neg P_4(a_4, x) \wedge \neg P_4(x, a_4))$ mit a_4
Konstante
- $(\forall x \exists y \forall z \in U \setminus \{y\} : P_5(x, y) \wedge \neg P_5(x, z)) \wedge$
 $(\forall x, y \exists n \in \mathbb{N} \exists z_0, \dots, z_{n-1} : P_5(x, z_0) \wedge (\bigwedge_{i=0}^{n-2} P_5(z_i, z_{i+1})) \wedge P_5(z_{n-1}, y))$

Anmerkung: $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$

- $F_1 = \forall x \exists y : P_0(x, y)$
- $F_2 = \forall x : \neg P_0(x, x)$
- $F_3 = \exists y \forall x : \neg P_0(x, y)$
- $F_4 = \forall x : \neg P_0(x, f(x))$
- $F_5 = \forall x \forall y : (P_0(x, f(y)) \implies P_0(y, x))$
- $F_6 = P(a, f(f(a)))$
- $F_7 = \forall x (\exists y : P_0(y, x) \implies P_1(x))$
- $F_8 = \neg P_1(f(f(b)))$
- $F_9 = P(f(c), c)$

Gib eine Interpretation für $F = \bigwedge_{i=1}^9 F_i$ an

Modulare Arithmetik

reloading 60.56 % complete...

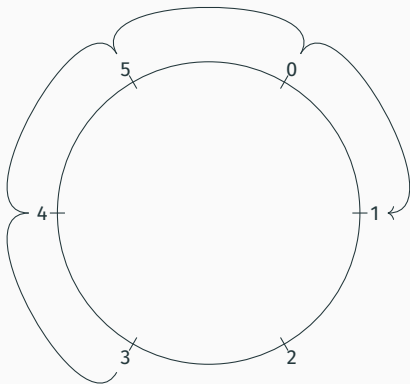
Rechnen mit unendlich vielen Zahlen ist hart



Wir können einfach nur mit den Zahlen 0 bis 5 rechnen



Was ist jetzt $3 + 4$?



$$3 + 4 \equiv 1 \pmod{6}$$

Das bedeutet so viel wie:

$$(3 + 4) \% 6 = 1 \% 6$$

- Wir nennen so einen begrenzten Zahlenraum **Restklassenring**
- Die mathematische Schreibweise für einen Restklassenring mit m Zahlen aus $\mathbb{Z}$ ist:

$$\mathbb{Z}/m\mathbb{Z}$$

Aufgaben

löst die folgenden Rechenaufgaben im $\mathbb{Z}/12\mathbb{Z}$

• $10 + 2$

• $3 \cdot 4 - 1$

• $(2 - 4) \cdot 2$

löst die folgenden Rechenaufgaben im $\mathbb{Z}/7\mathbb{Z}$

• $5 + 1$

• $(2 - 4) \cdot 2 + 5$

• $0 \cdot 4$

• $3 \cdot 4 - 1$

• 5^2

• $5!$

Was ist m ?

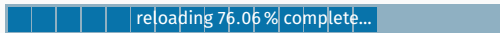
• $4 \equiv 6 \pmod{m}$

• $3 \equiv 9 \pmod{m}$

• $4 \equiv 11 \pmod{m}$

- Computer sind nicht unendlich groß
 - Variablen verbrauchen eine fixe Menge Platz
 - Was machen wenn die Zahl zu groß wird für diesen Platz?
 - Z.B. der `unsigned integer` ist im $\mathbb{Z}/2^{32}\mathbb{Z}$
- Hashing / Checksums
 - Wie stelle ich sicher ob eine Datei die Datei ist, die ich haben will?
- Verschlüsselung
 - Moderne Kryptographie verwendet die modulare Arithmetik

Wiederholung



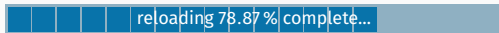
Prädikatenlogik

- Was sind Prädikate, Funktionen, Variable und Konstanten?
- Wie interpretieren wir Prädikaten- und Funktionssymbole?
- Wie funktionieren generische prädikatenlogische Aussagen?
- Wie schreiben wir Lösungen von prädikatenlogischen Aussagen formal auf?

Modulare Arithmetik

- Was macht der Modulo Operator?
- Wie rechnen wir in einem Restklassenring?
- Warum ist die Modulare Arithmetik in der Informatik so wichtig?

Wiederholungsaufgaben



Aufgaben

Welche der folgenden Aussagen ist korrekt?

Normal bis etwas Schwerer

- $a \in \{a, b, c\}$
- $a \subseteq \{a, b, c\}$
- $\{a, b\} \in \{a, b, \{a, b\}, c\}$
- $\{a, b\} \subseteq \{a, b, \{a, b\}, c\}$
- $\{\{a, b\}\} \subseteq \{a, b, \{a, b\}, c\}$

Nenne jeweils 5 Elemente aus den folgenden Mengen

Normal bis etwas Schwerer

- $M_1 = \{n + m \mid n, m \in \mathbb{N}\}$
- $M_2 = \{n + n \mid n \in \mathbb{N}\}$
- $M_3 = M_2 \setminus L_1$
- $M_4 = \{m \mid m \subseteq \mathbb{N} \wedge |m| \equiv 3 \pmod{4}\}$

Aufgaben

Bestimme den Wahrheitswert der folgenden Aussagen

Normal

- $\neg(42 = 11) \wedge (0 \in \mathbb{N} \vee 0 = |\mathbb{N}|)$
- $\forall x \in \mathbb{Q} \exists p, q \in \mathbb{Z} : \left(\left(x = \frac{p}{q} \wedge q = 1 \right) \implies \frac{p}{q} \in \mathbb{Z} \right)$
- $\exists n \in \mathbb{N} : (n \equiv 13 \pmod{2025} \implies n < 2025) \iff 14 \in \mathbb{N}$
- $(\exists n \in (\mathbb{N} \cap \emptyset) : |n| \geq 0) \iff (A \cap B = B \cap A)$

Schwer

- $\forall x \in \mathbb{Z} : x \equiv 0 \pmod{2} \vee x \equiv 1 \pmod{4}$

Abk.	Bedeutung	Was?!
$\mathbb{N}$	natürliche Zahlen (mit 0)	In der theoretischen Informatik enthält $\mathbb{N}$ die 0: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ (Auch $\mathbb{N}_0$)
$\mathbb{Z}$	ganze Zahlen	$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
$\mathbb{R}$	reelle Zahlen	$\mathbb{R} = \{\text{z.B. } 2, -3, \sqrt{17}, \pi, \text{ usw.}\}$
$\emptyset$	$\{\}$	leere Menge
$a b$	teilt	a ist Teiler von b , d.h. a teilt b ohne Rest
:	sodass	z.B. $\forall a, b \in \mathbb{Z} : a b$

Glossar – Mengenoperationen

Abk.	Bedeutung	Was?!
$A \subseteq B$	Teilmenge	Alle Elemente aus A sind auch in B enthalten. Dabei können die Mengen auch gleich sein.
$A \subsetneq B$	echte Teilmenge	$A \subseteq B$. Und zusätzlich enthält B Elemente, die nicht in A enthalten sind. $\implies$ Mengen sind nicht gleich!
$A \subset B$	Teilmenge <u>oder</u> echte Teilmenge	Bei manchen Leuten $\subseteq$, bei manchen $\subsetneq$. Mehrdeutig, lieber nicht verwenden!
$A \cap B$	Schnitt	Enthält alle Elemente, die in A <i>und</i> in B enthalten sind
$A \cup B$	Vereinigung	Enthält alle Elemente, die in A , B oder beiden enthalten sind
$A \setminus B$	Komplement, gespr. "A ohne B"	Enthält alle Elemente aus A , die <i>nicht</i> in B enthalten sind
$\overline{B}$	B Komplement	Enthält alle Elemente aus einer geg. Obermenge, die <i>nicht</i> in B enthalten sind

Abk.	Bedeutung	Was?!
$A \wedge B$	<i>A und B</i>	A und B müssen wahr sein, damit die Gesamtaussage wahr ist
$A \vee B$	<i>A oder B</i>	Es müssen mindestens A, B oder beide wahr sein
$\neg A$	<i>nicht A</i>	A muss falsch sein, damit $\neg A$ wahr ist
$B \implies A$	A ist notwendig für B	A muss wahr sein, wenn B wahr ist
$A \implies B$	A ist hinreichend für / impliziert B	B muss wahr sein, wenn A wahr ist
$A \iff B$	notwendig und hinreichend	genau dann, wenn

Abk.	Bedeutung	Was?!
$A \text{ gdw. } B$	genau dann, wenn	Äquivalenz zwischen Aussagen
$A \text{ ist notwendig für } B$	$B \implies A$	A muss wahr sein, wenn B wahr ist
$A \text{ ist hinreichend für } B$	$A \implies B$	B muss wahr sein, wenn A wahr ist
notwendig und hinreichend	$A \iff B$	genau dann, wenn

Abk.	Bedeutung	Was?!
$\forall x \in M : A(x)$	Für alle x aus M gilt $A(x)$	Die Aussage A muss für alle Elemente der Menge M wahr sein
$\exists x \in M : A(x)$	Es existiert ein x in M für das $A(x)$ gilt	Die Aussage $A(x)$ muss für mind. 1 (oder mehr) Elemente wahr sein
$\forall x, y \in M : A(x, y)$	Für alle x und alle y gilt $A(x, y)$	Äquivalent zu $\forall x \forall y : A(x, y)$

Abk.	Bedeutung	Was?!
z.z. Sei	zu zeigen	Was zu beweisen ist bereits bekannte Objekte werden eingeführt und benannt
$\exists$	es gibt ein	
$\exists!$	es gibt genau ein	
x ist genau y	$x = y$	<u>genau</u> wird verwendet bei Äquiva- lenz
x ist eindeutig	$\exists!x$	

Abk.	Bedeutung	Was?!
œ	ohne Einschränkung	die Allgemeinheit der Aussage wird nicht durch getroffene Aussagen eingeschränkt
o.B.d.A.	ohne Beschränkung der Allgemeinheit	wie œ
trivial	offensichtlich	Beweisschritte, welche keine weitere Begründung brauchen. (nicht verwenden!)
□	Mic Drop	Kommt am Ende eines erfolgreichen Beweises
q.e.d.	quod erat demonstrandum	Was zu beweisen war

Gestalt	mögliches Vorgehen
nicht F	Zeige, dass F nicht gilt.
F und G	Zeige F und G in zwei getrennten Beweisen.
$F \implies G$	Füge F in die Menge der Annahmen hinzu und zeige G.
F oder G	Zeige: nicht $F \implies G$. (Alternativ zeige: nicht $G \implies F$)
$F \iff G$	Zeige: $F \implies G$ und $G \implies F$.
$\forall x \in A : F$	Sei x ein beliebiges Element aus A. Zeige dann F.
$\exists x \in A : F$	Sei x ein konkretes Element aus A. Zeige dann F.

Abk.	Bedeutung	Was?!
U	Universum	Menge aller Elemente die in der prädikatenlogischen Formel zum Einsatz kommen
$P(x)$	Prädikatsymbol	Abbildung, die in Abhängigkeit von einem (oder mehreren Elementen) aus dem Universum wahr oder falsch ist
$I(P), I(f), I(a)$	Interpretation von P, f , und a	Tatsächliche Prädikate, Funktionen und konstanten, die für die entsprechenden Symbole eingesetzt werden für welche die prädikatenlogische Formel ausgewertet wird

Abk.	Bedeutung	Was?!
$n \equiv m \pmod{x}$	n ist kongruent m modulo x	Der Rest der Division n/x und m/x ist gleich. Wenn $m < x$ gilt $n = k \cdot x + m$ Es gilt: $a \equiv b \pmod{n} \iff n (a-b)$
$\mathbb{Z}/m\mathbb{Z}$	Restklassenring mit m Zahlen	

- Unsere Folien sind frei!
- Jeder darf die Folien unter den Bedingungen der **GNU General Public License v3** (oder jeder späteren Version) weiterverwenden.
- Ihr findet den Quelltext unter
<https://www.github.com/FIUS/theo-vorkurs-folien>