

# Mathematik und Logik

## 6. Übungsaufgaben

bis 2008-11-18, Lösungen

1. Seien  $d, a, b \in \mathbb{Z}$ . Dann gilt:

$$d \mid a \wedge d \mid b \implies d \mid ab \wedge d \mid (a - b).$$

Formulieren Sie diesen Satz formal mit Quantoren und beweisen Sie ihn. Achten Sie dabei besonders darauf, welche Schlußregeln jeweils verwendet werden. Achten Sie insbesondere auf die korrekte Verwendung der Definition:

$$a \mid b \iff \exists_{q \in \mathbb{Z}} b = q \cdot a.$$

*Lösung:* Zu zeigen ist

$$\forall_{a \in \mathbb{Z}} \forall_{b \in \mathbb{Z}} \forall_{d \in \mathbb{Z}} d \mid a \wedge d \mid b \implies d \mid a \cdot b \wedge d \mid (a - b)$$

Dreifache Anwendung einer  $\forall\mathcal{E}$  führt zu:

Annahmen:  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$ ,  $d \in \mathbb{Z}$ ;

Zu zeigen:  $d \mid a \wedge d \mid b \implies d \mid a \cdot b \wedge d \mid (a - b)$ .

Nun verwenden wir in der üblichen Weise eine Einführung für die Implikation:

Zusätzliche Annahme:  $d \mid a \wedge d \mid b$ ;

Nur noch zu zeigen:  $d \mid a \cdot b \wedge d \mid (a - b)$ .

Dieses Beweisziel ist eine Konjunktion, und wir haben beide Teile zu zeigen.

Gemäß Definition gilt:

$$\forall_{a \in \mathbb{Z}} \forall_{b \in \mathbb{Z}} a \mid b \iff \exists_{q \in \mathbb{Z}} b = q \cdot a.$$

Wir verwenden zweimalige  $\forall$ -Elimination, wobei wir  $d$  für  $a$  und  $a \cdot b$  für  $b$  einsetzen. Dies ergibt zunächst:

$$d \mid a \cdot b \iff \exists_{q \in \mathbb{Z}} a \cdot b = q \cdot d.$$

Die linke Seite ist hier unser erstes Beweisziel. Wir benötigen somit die Richtung von rechts nach links ( $\wedge\mathcal{E}_1$ ), sodaß wir mit einer  $\implies$ -Elimination erhalten:

Es reicht zu zeigen:

$$\exists_{q \in \mathbb{Z}} a \cdot b = q \cdot d.$$

Nun setzen wir für  $d \mid a$  die Definition ein:

$$d \mid a \iff \exists_{q \in \mathbb{Z}} a = q \cdot d.$$

Da  $d \mid a$  eine Annahme ist (zumindest nach Anwendung einer  $\wedge \mathcal{E}_0$ ), benötigen wir hier die Richtung von links nach rechts ( $\wedge \mathcal{E}_1$ ). Aus unseren Annahmen folgt somit:

$$\exists_{q \in \mathbb{Z}} a = q \cdot d.$$

Eine  $\exists \mathcal{E}$  erlaubt es uns nun, ein neues Symbol einzuführen und von diesem eben diese Eigenschaft anzunehmen. Als neues Symbol können wir hier einfach  $q$  verwenden, da dieses sonst noch nirgends verwendet wird (gebundene Vorkommen zählen nicht). Also: Annahme:  $a = q \cdot d$ .

Wegen der Wohldefiniertheit der Multiplikation dürfen wir beide Seiten mit  $b$  multiplizieren, was zuerst zu  $a \cdot b = (q \cdot d) \cdot b$  führt, und mit den üblichen Rechenregeln (Kommutativgesetz und Assoziativgesetz) zu

$$a \cdot b = (b \cdot q) \cdot d.$$

Daraus schließen wir nun mit der  $\exists$ -Introduktionsregel:

$$\exists_{q \in \mathbb{Z}} a \cdot b = q \cdot d,$$

wobei  $b \cdot q$  für das im Existenzquantor gebundene  $q$  einzusetzen ist.

Für die zweite Behauptung ( $d \mid (a - b)$ ) gehen wir ähnlich vor. Einsetzen der Definition besagt, daß wir

$$\exists_{q \in \mathbb{Z}} a - b = q \cdot d$$

zu zeigen haben. Wie oben ausgeführt, dürfen wir dazu voraussetzen:  $a = q \cdot d$ . Diesesmal verwenden wir aber auch die zweite Annahme, welche zu  $\exists_{q \in \mathbb{Z}} b = q \cdot d$  führt. Auch für diese verwenden wir eine  $\exists$ -Elimination. Die neue Variable darf aber nicht wieder  $q$  heißen. Wir verwenden deshalb  $r$  (welches noch nirgends vorkommt):

Annahme:  $b = r \cdot d$ ,

Diesesmal subtrahieren wir die beiden Gleichungen (eine Anwendung der Wohldefiniertheit der Subtraktion), sodaß sich ergibt:

$$a - b = q \cdot d - r \cdot d,$$

und das Distributivgesetz liefert schließlich

$$a - b = (q - r) \cdot d,$$

woraus eine  $\exists \mathcal{E}$  wiederum

$$\exists_{q \in \mathbb{Z}} a - b = q \cdot d$$

ergibt.

## 2. Zeigen oder widerlegen Sie:

$$\left( \forall_{x \in X} \forall_{y \in Y} A(x) \vee B(x) \right) \implies \left( \forall_{x \in X} A(x) \right) \vee \left( \forall_{y \in Y} B(x) \right)$$

*Lösung:* Sei  $X = Y = \mathbb{N}$ , und  $A(x)$  die Aussage „ $x$  ist gerade“ sowie  $B(x)$  die Aussage „ $x$  ist ungerade“. Die Voraussetzung in der obigen Implikation besagt dann, daß jede natürliche Zahl gerade oder ungerade ist, während die Konklusion besagt, daß entweder jede natürliche Zahl gerade ist oder jede Zahl ungerade, was natürlich Unsinn ist und insbesondere nicht aus der (gültigen) Voraussetzung folgt.

## 3. Welche der beiden Richtungen in

$$\overline{\forall_{x \in X} A(x)} \iff \overline{\exists_{x \in X} A(x)}$$

können Sie beweisen?

*Lösung:*

- Wir beginnen mit der Richtung von links nach rechts. Nach einer  $\implies$ -Introduktion liegt die folgende Beweissituation vor:

Annahme:  $\left( \forall_{x \in X} A(x) \right) \implies \perp$ ;

Zu zeigen:  $\overline{\exists_{x \in X} A(x)}$ .

Um die Existenzaussage mit Introduktion zu beweisen, benötigen wir einen konkreten Term vom Typ  $X$ . Die Annahme ermöglicht keine Konstruktion eines solchen. Die einzige Schlußregel, die hier überhaupt noch möglich erscheint, ist  $\implies$ -Elimination der Annahme, d.h.

Es reicht zu zeigen:  $\forall_{x \in X} A(x)$ .

(Da in diesem Fall  $\perp$  gelten würde, und somit auch das obige Beweisziel.) Klarerweise ist dies aber nicht allgemein möglich. (Die Existenzaussage im Beweisziel ist dafür ja nicht verwendbar.)

Somit gerät dieser Teil des Beweises endgültig ins Stocken. Tatsächlich ist diese Richtung mit der besprochenen Regeln nicht beweisbar.

- Auch die Umkehrung beginnt natürlich mit einer  $\implies$ -Introduktion, was aber nun zu dieser Beweissituation führt:

Annahme:  $\overline{\exists_{x \in X} A(x)}$ ;

zu zeigen:  $\left( \forall_{x \in X} A(x) \right) \implies \perp$ ;

Hier läßt sich erstens  $\implies$ -Introduktion verwenden, d.h.

Annahme:  $\forall_{x \in X} A(x)$ ;

zu zeigen:  $\perp$ .

Und zweitens können wir den Existenzquantor eliminieren. Wir führen also ein neues Symbol ein, z.B.  $x$ , und nehmen somit zusätzlich an:

$x \in X$  und  $A(x) \implies \perp$ .

Dieses  $x$  setzen wir nun für das gebundene  $x$  bei der  $\forall$ -Elimination der Annahme ein:

Es gilt somit:  $A(x)$ .

Und eine einfache Anwendung der  $\implies$ -Elimination liefert  $\perp$ .

4. Für beliebige Mengen  $A, B, C$ , definieren Sie eine Funktion vom Typ

$$f : (A \rightarrow B \rightarrow C) \rightarrow (B \rightarrow A \rightarrow C).$$

*Lösung:* Die gesuchte Funktion  $f$  muß für jedes  $\varphi : A \rightarrow B \rightarrow C$  sowie für jedes  $b \in B$  und  $a \in A$  einen wohldefinierten Wert in  $C$  liefern. Wir definieren daher:

$$f(\varphi, b, a) := \varphi(a, b).$$

Dabei haben wir  $f(\varphi, b, a)$  abkürzend für  $f(\varphi)(b)(a)$  verwendet; und ebenso  $\varphi(a, b)$  für  $\varphi(a)(b)$ .

5. Für beliebigen Mengen  $A$  und  $B$ , definieren Sie eine Funktion vom Typ

$$h : (((A \rightarrow B) \rightarrow B) \rightarrow B) \rightarrow (A \rightarrow B).$$

*Lösung:* Die Funktion  $h$  sollte für  $\varphi : ((A \rightarrow B) \rightarrow B) \rightarrow B$  und  $a \in A$  einen Wert in  $B$  liefern. Es ist hier nicht möglich  $\varphi$  auf  $a$  anzuwenden (Typverletzung). Wir müssen erst eine Funktion  $\psi : (A \rightarrow B) \rightarrow B$  definieren. Diese muß für ein  $f : A \rightarrow B$  einen Wert in  $B$  liefern, was durch

$$\psi(f) := f(a)$$

tatsächlich leicht möglich ist. Damit läßt sich nun auch  $h$  selbst definieren, nämlich als

$$h(\varphi, a) := \varphi(\psi).$$

Zusammenfassend könnten wir auch schreiben:

$$h := \varphi \mapsto a \mapsto \varphi(f \mapsto f(a)).$$

(Man vergleiche diese Konstruktion mit dem Beweis der entsprechenden Aussage.)

6. Zeigen Sie:

$$\forall_{n \in \mathbb{N}} \exists_{m \in \mathbb{N}} m > n.$$

*Lösung:* Sei  $n \in \mathbb{N}$ .

Dann gilt:  $n + 1 \in \mathbb{N}$  und  $n + 1 > n$ . Somit  $\exists_{m \in \mathbb{N}} m > n$ .

Was passiert hier, wenn man die Reihenfolge der Quantoren vertauscht?

*Lösung:* Die Aussage

$$\exists_{m \in \mathbb{N}} \forall_{n \in \mathbb{N}} m > n$$

bedeutet dagegen, daß es eine natürliche Zahl gäbe, die größer als jede natürliche Zahl ist, was natürlich falsch ist.

Was läßt sich allgemein über die Beziehung von Aussagen der Form

$$\forall_{x \in X} \exists_{y \in Y} P(x, y) \quad \text{und} \quad \exists_{y \in Y} \forall_{x \in X} P(x, y)$$

zueinander sagen?

*Lösung:* Die zweite Aussage impliziert die erste, aber (allgemein) nicht umgekehrt.

7. Zeigen Sie:

$$\left( \exists_{x \in X} A(x) \implies B \right) \implies \left( \forall_{x \in X} A(x) \implies B \right)$$

*Lösung:* Annahme:  $\exists_{x \in X} A(x) \implies B$ ,

zweite Annahme:  $\forall_{x \in X} A(x)$ ;

zu zeigen:  $B$ .

Gemäß  $\exists$ -Elimination führen wir ein neues Symbol  $x \in X$  ein, von dem wir annehmen:

$$A(x) \implies B.$$

Dieses setzen wir nun in die zweite Annahme ein ( $\forall$ -Elimination); es gilt daher:

$$A(x).$$

Daraus schließen wir nun  $B$  (mit  $\mathcal{E}$ ) und sind fertig.

*Anmerkung:* Eigentlich haben wir exakt denselben Beweis schon im Beispiel 3 durchgeführt (rechts nach links).

8. Übungen zu SAGE folgen in einem eigenen Übungs-Worksheet: <http://www.algebra.uni-linz.ac.at/Students/Win/ml08w/exc/e6.sws>.

*Lösung:* <http://www.algebra.uni-linz.ac.at/Students/Win/ml08w/exc/s6.sws>.

*Lösung:* Anmerkung: Bekannterweise bindet Punktrechnung stärker als Strichrechnung. Allgemeiner gilt üblicherweise die folgende Reichenfolge: Funktionsanwendung (z.B.  $f(x)$ ), Potenzieren, Multiplizieren und Dividieren, Addieren und Subtrahieren, Vergleichsoperatoren ( $<$ ,  $=$ , Teilbarkeit), Logisches Und, Logisches Oder, Logische Implikation und Äquivalenz, Quantoren. Stehen gleichrangige Operatoren nebeneinander, so beginnt man meist links zu lesen; Ausnahmen: Potenzieren ( $x^{y^z}$  ist als  $x^{(y^z)}$  zu lesen, sowie die Implikation. Vergleichsoperatoren dagegen werden meist als mit einer Konjunktion verbunden interpretiert:  $x < y < z$  ist dasselbe wie  $x < y \wedge y < z$ .