Kapitel 4

Beweismethoden

$$\frac{A(1), \forall n \in \mathbb{N} : A(n) \Rightarrow A(n+1)}{\forall n \in \mathbb{N} : A(n)}$$

Inhalt

Beweismethoden

- Die meisten mathematischen Sätze oder Folgerungen haben die Form

$$\alpha \Rightarrow \beta$$

  Dabei sind α und β (prädikatenlogische) Formeln.
- α heißt Voraussetzung und β Behauptung eines Satzes.
- Sätze, die $\alpha \Leftrightarrow \beta$ behaupten, sind äquivalent zu $\alpha \Rightarrow \beta \wedge \beta \Rightarrow \alpha$. Daher beschränken wir uns auf Implikationen.
- Wir betrachten folgende Beweisverfahren:
  1. direkter Beweis
  2. indirekter Beweis
  3. Widerspruchsbeweis
  4. Beweis durch Ringschluss
  5. vollständige Induktion

Direkter Beweis

Ein direkter Beweis eines Satzes $\alpha \Rightarrow \beta$ ist eine Folge

$$\gamma_1, \gamma_2, \ldots, \gamma_n = \beta$$

von Aussagen, wobei für jedes i mit $1 \leq i \leq n$ gilt:

- $\gamma_i = \alpha$ oder
- γ_i ist eine bereits bewiesene bekannte Aussage oder
- $\gamma_{j_1} \wedge \gamma_{j_2} \wedge \ldots \wedge \gamma_{j_r} \Rightarrow \gamma_i$ mit $j_1, j_2, \ldots, j_r < i$.

Bei den Zwischenschritten können also Kombinationen von vorher etablierten Aussagen verwendet werden.

Teiler

Definition 4.1

Es seien $p, q \in \mathbb{N}$.

p heißt Teiler von q oder p teilt q (Schreibweise: $p|q$) genau dann, wenn ein $a \in \mathbb{N}$ existiert, so dass $a \cdot p = q$ gilt.

Wir schreiben $p \nmid q$, wenn p kein Teiler von q ist.

Kurz:

$$\begin{aligned} p|q &\quad :\Leftrightarrow \quad \exists a \in \mathbb{N} : a \cdot p = q \\ p \nmid q &\quad :\Leftrightarrow \quad \forall a \in \mathbb{N} : a \cdot p \neq q \end{aligned}$$

Beispiel 4.2

Wir zeigen mit einem direkten Beweis:

$$p|q \wedge q|r \Rightarrow p|r$$

In Worten: Wenn p Teiler von q ist und wenn q Teiler von r ist, dann ist auch p Teiler von r.

$$
\begin{array}{lcll}
\gamma_1 & = & p|q \wedge q|r & \text{Voraussetzung} \\
\gamma_2 & = & p|q & \text{folgt aus } \gamma_1 \\
\gamma_3 & = & \exists a \in \mathbb{N} : a \cdot p = q & \text{folgt aus } \gamma_2 \text{ nach Def. für } | \\
\gamma_4 & = & q|r & \text{folgt aus } \gamma_1 \\
\gamma_5 & = & \exists b \in \mathbb{N} : b \cdot q = r & \text{folgt aus } \gamma_4 \text{ nach Def. für } | \\
\gamma_6 & = & b \cdot (a \cdot p) = r & \text{folgt aus } \gamma_3 \text{ und } \gamma_5 \\
\gamma_7 & = & (b \cdot a) \cdot p = r & \text{folgt aus } \gamma_6 \text{ mit Assoziativgesetz} \\
\gamma_8 & = & \exists c \in \mathbb{N} : c \cdot p = r & \text{folgt aus } \gamma_7 \text{ mit } c = b \cdot a \\
\gamma_9 & = & p|r & \text{folgt aus } \gamma_8 \text{ nach Def. für } |
\end{array}
$$

Indirekter Beweis

Ein indirekter Beweis nutzt die Äquivalenz:

$$(\alpha \Rightarrow \beta) \Leftrightarrow (\neg\beta \Rightarrow \neg\alpha)$$

Manchmal ist es einfacher, die rechte anstelle der linken Folgerung zu beweisen.

Beispiel 4.3

Wir beweisen eine weitere Teilbarkeitsregel:

> *Wenn die letzten beiden Ziffern einer natürlichen Zahl z als Zahl betrachtet durch 4 teilbar sind, dann ist auch z durch 4 teilbar.*

Wir formalisieren:

$$\begin{aligned} \alpha &= x \in \mathbb{N}_{0,99} \wedge 4|x \wedge y \in \mathbb{N}_0 \\ \beta &= 4|(100y + x) \end{aligned}$$

Hinweis: $z = 100y + x$

Wir zeigen jetzt $\neg\beta \Rightarrow \neg\alpha$. Es ist:

$$\begin{aligned} \neg\alpha &= x \notin \mathbb{N}_{0,99} \vee 4 \nmid x \vee y \notin \mathbb{N}_0 \\ \neg\beta &= 4 \nmid (100y + x) \end{aligned}$$

Fortsetzung Beispiel.

Wenn $x \notin \mathbb{N}_{0,99}$ oder $y \notin \mathbb{N}_0$ gilt, dann ist $\neg\alpha$ erfüllt. Daher genügt es

$$x \in \mathbb{N}_{0,99} \wedge y \in \mathbb{N}_0 \wedge 4 \nmid (100y + x) \Rightarrow 4 \nmid x$$

zu beweisen. Dies tun wir direkt:

$$\begin{array}{rcll}
4 \nmid (100y + x) & \Rightarrow & \frac{100y+x}{4} \notin \mathbb{N}_0 & \\
& \Rightarrow & \frac{100y}{4} + \frac{x}{4} \notin \mathbb{N}_0 & \\
& \Rightarrow & 25y + \frac{x}{4} \notin \mathbb{N}_0 & \\
& \Rightarrow & \frac{x}{4} \notin \mathbb{N}_0 & \text{weil } y \in \mathbb{N}_0 \\
& \Rightarrow & 4 \nmid x & \text{weil } x \in \mathbb{N}_{0,99}
\end{array}$$

Widerspruchsbeweis

Ein Widerspruchsbeweis nutzt die Äquivalenz:

$$(\alpha \Rightarrow \beta) \Leftrightarrow ((\alpha \wedge \neg\beta) \Rightarrow 0)$$

Wir nehmen also sowohl α als auch die Negation der Folgerung β, also $\neg\beta$, als wahr an und versuchen, daraus einen Widerspruch zu folgern.

Beispiel 4.4

Ein klassisches Beispiel für einen Widerspruchsbeweis ist zu zeigen, dass $\sqrt{2}$ keine rationale Zahl ist.

Annahme: $\sqrt{2} \in \mathbb{Q}$
Dann existieren teilerfremde Zahlen $p, q \in \mathbb{N}$ mit $\sqrt{2} = \frac{p}{q}$.

$$\begin{aligned} & \sqrt{2} = \frac{p}{q} \\ \Rightarrow \quad & 2 = \frac{p^2}{q^2} \\ \Rightarrow \quad & 2q^2 = p^2 \\ \Rightarrow \quad & 2 | p^2 \end{aligned}$$

p^2 hat aber die gleichen Primfaktoren wie p. Da 2 eine Primzahl ist, muss also auch $2|p$ gelten. Also existiert ein a mit $p = 2 \cdot a$.

Fortsetzung Beispiel.

$$
\begin{aligned}
 & p = 2 \cdot a \\
\Rightarrow\ & 2q^2 = (2a)^2 \\
\Rightarrow\ & 2q^2 = 4a^2 \\
\Rightarrow\ & q^2 = 2a^2 \\
\Rightarrow\ & 2|q^2 \\
\Rightarrow\ & 2|q
\end{aligned}
$$

Widerspruch zu p und q sind teilerfremd.

Ringschluss

Einen Ringschluss können wir nutzen, um die paarweise Äquivalenz von mehr als zwei Aussagen zu zeigen.

Statt

$$\alpha_1 \Leftrightarrow \alpha_2 \Leftrightarrow \cdots \Leftrightarrow \alpha_k$$

zeigen wir

$$\alpha_1 \Rightarrow \alpha_2 \Rightarrow \cdots \Rightarrow \alpha_k \Rightarrow \alpha_1$$

Für jede der Implikationen können wir wiederum eine der schon vorgestellten Techniken nutzen (direkter Beweis, indirekter Beweis, Widerspruchsbeweis).