

UNIVERSITÄT
LEIPZIG

Lineare Algebra 1

Łukasz Grabowski

Mathematisches Institut

1. Aussagenlogik - Wiederholung

2. Beweise und Beweisprinzipien

3. Arithmetik

- Atome - “Grundaussagen”, $A, B, C, \ldots$
- Junktoren: $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\iff$
- Formeln, z.B. $(A \Rightarrow B) \vee (C \iff (B \wedge A))$.
- Wenn wir eine Formel haben und die Werte ihrer Atome belegen, können wir den Wert der Formel berechnen.
  - z.B. falls $A = 0, B = 1, C = 0$ dann $(A \Rightarrow B) \vee (C \iff (B \wedge A)) = 1$,

- Eine Formel ist
  - eine *Tautologie* , falls sie unabhängig von der Belegung der Atome wahr ist.
  - *unerfüllbar*, falls sie unabhängig von der Belegung der Atome falsch ist.
  - *erfüllbar*, falls es eine Belegung der Atome gibt, so dass die Formel wahr ist,
  - *widerlegbar*, falls es eine Belegung der Atome gibt, so dass die Formel falsch ist.

- Zwei Formeln sind *äquivalent* genau dann, wenn deren Wahrheitswerte für alle Belegungen der Atome übereinstimmen. Schreibweise: $F \equiv G$.
  - Z.B. $A \Rightarrow B \equiv \neg A \vee B$ (“Elimination von $\Rightarrow$”).

- “Substitutionsprinzip”: durch *Äquivalenzketten*, können wir zeigen, dass zwei Formel äquivalent sind,
- **Beispiel.** Die Formeln $(A \wedge \neg B) \Rightarrow C$ und $(A \Rightarrow B) \vee C$ sind äquivalent.
  - Wir fangen mit $(A \wedge \neg B) \Rightarrow C$ an.
  - äquivalent zu $\neg(A \wedge \neg B) \vee C$ (Elimination von $\Rightarrow$)
  - äquivalent zu $(\neg A \vee \neg\neg B) \vee C$ (De Morgan)
  - äquivalent zu $(\neg A \vee B) \vee C$ (Involution $\neg$)
  - äquivalent zu $(A \Rightarrow B) \vee C$ (Elimination von $\Rightarrow$)

1. Aussagenlogik - Wiederholung

2. Beweise und Beweisprinzipien

3. Arithmetik

- Im Allgemeinen wollen wir in der Mathematik häufig etwas in der Form beweisen: Wenn A wahr ist, dann B ist auch wahr.
  - Mit anderen Worten: Wir wollen zeigen, dass die Implikation $A \Rightarrow B$ wahr ist.
- Wir haben schon eingie Beispiele gesehen.
  - Seien $d, a, b \in \mathbb{Z}$. Falls $d \mid a$ und $d \mid b$ dann $d \mid a + b$.
  - Beweis: Falls $d \mid a$ und $d \mid b$ dann existieren $k, l \in \mathbb{Z}$ so dass $a = dk, b = dl$, woraus folgt $a + b = d(k + l)$, was bedeutet, dass $d \mid a + b$.
- Hier A ist die Aussage: "d, a, b sind ganze Zahlen mit der Eigenschaft dass $d \mid a$ und $d \mid b$"
- B ist die Aussage "$d \mid a + b$".
- Das ist ein Beispiel eines direktes Beweises.

Beweisprinzip: Kontraposition

- Anstelle eines Beweises der Aussage $A \to B$ kann ein Beweis für die Aussage $\neg B \to \neg A$ geführt werden.
  - $A \Rightarrow B$ ist falsch gdw $A = 1, B = 0$; und $\neg B \Rightarrow \neg A$ ist falsch gdw $\neg B = 1, \neg A = 0$. Das gilt gdw $A = 1, B = 0$.
- **Beispiel.** Sei n eine beliebige ganze Zahl. Falls n^2 gerade ist, so ist auch n gerade.
  - Hier A ist "n hat die Eigenschaft dass n^2 gerade ist." und B ist "n hat die Eigenschaft dass n gerade ist."
  - Wir wollen $A \Rightarrow B$ zeigen. Stattdessen im Beweiss werden wir $\neg B \Rightarrow \neg A$ zeigen, dh. falls n ungerade ist, so ist auch n^2 ungerade.

Beweis. Nehmen wir an, dass n ungerade ist, Deswegen können wir eine ganze Zahl k finden sodass $n = 2k + 1$.

Dann $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, und damit ist n^2 ungerade. Dies beweist die Kontraposition und somit auch die ursprüngliche Aussage. □

Beweisprinzip: Indirekter Beweis oder „Beweis durch Widerspruch“

- Eine Behauptung A ist bewiesen, wenn aus ihrer Negation ein Widerspruch folgt.

Satz. Es gibt keine rationale Zahl x mit $x^2 = 2$.

Beweis. Beweis durch Widerspruch. Wir nehmen an, dass es eine rationale Zahl x gibt, sodass $x^2 = 2$.

- Dann existieren teilerfremde ganze Zahlen m und n mit $n \neq 0$ und $x = \frac{m}{n}$. Also auch

$$2 = x^2 = (\tfrac{m}{n})^2 = \tfrac{m^2}{n^2}$$

und damit $2n^2 = m^2$, womit m^2 gerade ist. Somit ist auch m gerade, also existiert eine ganze Zahl k mit $m = 2k$.

- Es gilt $2n^2 = m^2 = (2k)^2 = 4k^2$, also $n^2 = 2k^2$.

- Also ist auch n^2 gerade und damit auch n. Da m und n gerade sind, sind sie nicht teilerfremd.

- Es gibt also eine teilerfremde Darstellung und gleichzeitig kann es diese nicht geben. Widerspruch. Folglich gilt die Behauptung. □

- Zur Analyse der Beweisstruktur betrachten wir:
  - $A =$ “Es gibt keine rationale Zahl x mit $x^2 = 2$.”
  - $B =$ “ Es existieren teilerfremde ganze Zahlen m und n mit $n \neq 0$ und $(\frac{m}{n})^2 = 2$.
  - Wir zeigten nacheinander die Aussagen $\neg A \Rightarrow B$ und $\neg A \Rightarrow \neg B$ durch direkte Beweise. Es folgt, dass A gilt.
- Bei realer Beweisführung, eine passende Aussage B muss erst gefunden werden.

Beweisprinzip: Beweis von Äqivalenz durch zwei Implikationen

- Häufig wollen wir zeigen, dass zwei Aussagen äquivalent sind, d.h. A genau dann wenn B.
- Stattdessen können wir beweisen, dass $A \Rightarrow B$ und $B \Rightarrow A$.
- Beispiel: Eine ganze Zahl n ist gerade gdw n^2 gerade ist.

Beweis. • Wir haben schon früher gesehen dass $B \Rightarrow A$. Also müssen wir noch $A \Rightarrow B$ zeigen.

• Falls n ist gerade, wir können $k \in \mathbb{Z}$ finden mit $n = 2k$. Dann schreiben wir $n^2 = 4k^2 = 2 \cdot 2k^2$, also n^2 ist auch gerade. $\square$.

Satz. Sei $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$ eine natürliche Zahl mit $n \geqslant 2$. Dann n ist eine Primzahl gdw es gibt keine Primzahl p mit $p \leqslant \sqrt{n}$ und $p \mid n$

Beweis. • Sei n eine Primzahl. Dann der einzige Primzahlteiler von n ist n. Da $n > \sqrt{n}$, wir sehen dass tatsätzlich es gibt keine Primzahl p mit $p \leqslant \sqrt{n}$ und $p \mid n$.

• Sei jetzt n eine natürliche Zahl mit $n \geqslant 2$, so dass es gibt keine Primzahl p mit $p \leqslant \sqrt{n}$ und $p \mid n$. Wir möchten zeigen, dass n eine Primzahl ist.

► Nehmen wir an, dass n keine Primzahl ist. Wir betrachten den kleinsten Primzahlteiler q von n. Wir können schreiben $n = q \cdot r$, und $n > r \geqslant q$.

• Aber dann $q \leqslant \sqrt{n}$.

▹ Sonst hätten wir $n = qr > \sqrt{n}\sqrt{n} = n$, was ein Widerspruch ist.

► Wir haben also bewiesen, dass q eie Primzahl ist, und $q \leqslant \sqrt{n}$ und $q \mid n$. Dies beweist die Kontraposition, und somit auch die ursprüngliche Aussage. □

Beweisprinzip: Fallunterscheidung

- Die Fallunterscheidung: Innerhalb eines Beweises befinden wir uns in einem von mehreren möglichen Fällen. In jedem möglichen Fall können wir eine zusätzliche Annahme benutzen.
- Wichtige Schritte:
  - Vollständige Aufstellung der möglichen Fälle
  - Einzelbetrachtung eines jeden Falls mit Angabe eines Beweises unter Ausnutzung der zusätzlichen Annahme
- Bevor wir uns Beispiele ansehen, wollen wir noch einige weitere Grundlagen der Arithmetik einführen.

1. Aussagenlogik - Wiederholung

2. Beweise und Beweisprinzipien

3. Arithmetik

- Seien $a, b \in \mathbb{N}_+$. Der grösste gemeinsame Teiler von a und b ist die grösste narürliche Zahl d mit der Eigenschaft, dass $d \mid a$ und $d \mid b$. Sie wird mit $\mathrm{ggT}(a, b)$ bezeichnet.
  - Wir definieren auch $\mathrm{ggT}(0, a) = \mathrm{ggT}(a, 0) := a$ und für $a, b \in \mathbb{Z}$ definieren wir $\mathrm{ggT}(a, b) := \mathrm{ggT}(|a|, |b|)$.
- Der ggT wird mit dem Euklidichen Algorithmus berechnet. Wir führen eine Reihe von Divisionen mit Rest durch, bis wir den Rest 0 bekommen. Dann der letzte nicht-null Rest ist der gesuchte ggT.

- Z.B. seien $a = 161, b = 119$.

$$
\begin{aligned}
161 &= 1 \cdot 119 + 42 \\
119 &= 2 \cdot 42 + 35 \\
42 &= 1 \cdot 35 + 7 \\
35 &= 5 \cdot 7 + 0
\end{aligned}
$$

- Da der letzte nicht-null Rest ist 7, bedeutet es, dass $\mathrm{ggT}(161, 119) = 7$.

- Wir sehen dadurch, dass wir von oben nach unten in diesem Algorithmus gehen, dass falls $d \mid a$ und $d \mid b$, dann d teilt auch den letzten nicht-null Rest.

- Weiterhin, wenn wir von unten nach oben gehen, sehen wir auch dass falls d den letzten nicht-null Rest teilt, dann teil d auch a und b

- Dies zeigt tatsächlich, dass der letzte nicht-null Rest ist gleich $\mathrm{ggT}(a, b)$.
- Weiterhin haben wir den folgenden Satz bewiesen.

Satz. Falls $d \mid a$ und $d \mid b$, dann $d \mid \mathrm{ggT}(a, b)$. □

Satz. (Lemma von Bézout) Seien $a, b \in \mathbb{Z}$. Wir können ganze Zahlen x, y finden, die die Gleichung $aX + bY = \mathrm{ggT}(a, b)$ lösen.

Beweis. Wir erhalten dies, wenn wir von unten nach oben im Euklidischen Algorithmus gehen. Z.B. betrachten wir die Gleichung $161 \cdot X + 119 \cdot Y = 7$. Wir führen den Euklidischen Algorithmus durch:

$$\begin{aligned} 161 &= 1 \cdot 119 + 42 \\ 119 &= 2 \cdot 42 + 35 \\ 42 &= 1 \cdot 35 + 7 \\ 35 &= 5 \cdot 7 + 0 \end{aligned}$$

- Jetz gehen wir "von unten nach oben" wie folgt:

$7 = 42 - 1 \cdot 35 = 42 - 1 \cdot (119 - 2 \cdot 42) = -1 \cdot 119 + 3 \cdot 42 = -1 \cdot 119 + 3 \cdot (161 - 1 \cdot 119) = 3 \cdot 161 - 4 \cdot 119.$.
Also wir können $x := 3, y := -4$ setzen.