

UNIVERSITÄT
LEIPZIG

Lineare Algebra 1

Łukasz Grabowski

Mathematisches Institut

1. Beweise und Beweisprinzipien - Wiederholung

2. Arithmetik - Wiederholung

3. Modulare Arithmetik

4. Die Sprache der Prädikatenlogik

5. Beweisstrategien für Sätze mit Prädikaten und Quantoren

6. Weitere Beweis-Beispiele

- Direkter Beweis $A \Rightarrow B$.
- Kontraposition: Anstelle des Beweises einer Aussage $A \Rightarrow B$ kann ein Beweis für die Aussage $\neg B \Rightarrow \neg A$ geführt werden.
- „Beweis durch Widerspruch“: Eine Behauptung A ist bewiesen, wenn aus ihrer Negation ein Widerspruch folgt.
- Beweis von Äquivalenz durch zwei Implikationen
- Fallunterscheidung

1. Beweise und Beweisprinzipien - Wiederholung

2. Arithmetik - Wiederholung

3. Modulare Arithmetik

4. Die Sprache der Prädikatenlogik

5. Beweisstrategien für Sätze mit Prädikaten und Quantoren

6. Weitere Beweis-Beispiele

- Der $\mathrm{ggT}(a, b)$ 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.

- Das folgede Lemma erhalten wir, wenn wir von unten nach oben im Euklidischen Algorithmus gehen.

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.

1. Beweise und Beweisprinzipien - Wiederholung

2. Arithmetik - Wiederholung

3. Modulare Arithmetik

4. Die Sprache der Prädikatenlogik

5. Beweisstrategien für Sätze mit Prädikaten und Quantoren

6. Weitere Beweis-Beispiele

- Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}_+$. Wir sagen dass a und b *kongruent modulo* n sind, geschrieben $a \equiv b \mod n$, wenn a und b dengleichen Rest haben wenn wir sie durch n teilen.
  - $27 \equiv 7 \equiv 2 \mod 5$, $113 \equiv 15 \mod 7$, $2 \equiv -3 \mod 5$.
- Übung: $a \equiv b \mod n$ gdw $n \mid a - b$.

Satz. Seien $a, b, c, d \in \mathbb{Z}$ und sei $n \in \mathbb{N}_+$ so dass $a \equiv b \mod n$ und $c \equiv d \mod n$. Dann
- $a + c \equiv b + d \mod n$
- $ac \equiv bd \mod n$.

Beweis. Mit der gegeben Vorausetzung können wir schreiben: $n \mid b - a$ und $n \mid d - c$.
- Es folgt $n \mid b - a + d - c = (b + d) - (a + c)$, was bedeutet $b + d \equiv a + c \mod n$.
- Es folgt auch $n \mid d(a - b) - a(d - c)$, also $n \mid ac - bd$, was bedeutet $ac \equiv bd \mod n$. □

- **Beispiel.** Was ist $7^5 + 13^{20} \mod 5$? Modulo 5 haben wir:

$$7^5 + 13^{20} \equiv 2^5 + 3^{20} \equiv 2^5 + (-2)^{20} \equiv 2 \cdot (-1)^2 + (-1)^{10} \equiv 2 \cdot 1 + 1 \equiv 3.$$

Beispiel für das Beweisprinzip “Fallunterscheidung”.

Satz. Sei $n \in \mathbb{Z}$. Dann $n^2 \equiv 0 \mod 3$ oder $n^2 \equiv 1 \mod 3$

Beweis. Wir betrachten die folgenden Fälle: $n \equiv 0 \mod 3$, $n \equiv 1 \mod 3$, und $n \equiv 2 \mod 3$

- $n \equiv 0 \mod 3$, dann $n^2 \equiv 0^2 \equiv 0 \mod 3$.
- $n \equiv 1 \mod 3$, dann $n^2 \equiv 1^2 \equiv 1 \mod 3$.
- $n \equiv 2 \mod 3$, dann $n^2 \equiv 2^2 \equiv 1 \mod 3$.

□

1. Beweise und Beweisprinzipien - Wiederholung

2. Arithmetik - Wiederholung

3. Modulare Arithmetik

4. Die Sprache der Prädikatenlogik

5. Beweisstrategien für Sätze mit Prädikaten und Quantoren

6. Weitere Beweis-Beispiele

• Betrachten wir die bisherigen Beispiele erneut, so fallen einige Beschränkungen der Aussagenlogik ins Auge.

Satz. Sei n eine beliebige ganze Zahl. Falls n^2 gerade ist, so ist auch n gerade.

• Anders gesagt: wir haben die Aussage $P =$"jede ganze Zahl n hat die Eigenschaft dass wenn n^2 gerade ist dann ist auch n gerade."

• Was ist die Negation? $N =$"Existiert eine ganze Zahl n mit der Eigenschaft dass n^2 gerade ist, aber n ungerade ist".

• Problem 1: Es gibt keine Regeln der Aussagenlogik die uns sagen, dass tatsätzlich N die Negation von P ist.

• Problem 2: Ein Satz wie "n^2 ist gerade" ist keine echte Ausage. Dieser Satz wird zu einer Aussage nur wenn wir statt n eine konkrete Zahl nehmen, wie z.B. 58.

- Prädikatenlogik: die neuen Elemente im Vergleich mit Aussagenlogik:
  - ► *Variablen* und *Prädikaten*, die als “Aussagenschablonen” betrachtet werden können. Für jede Belegung der Variablen bekommen wir eine konkrete Aussage entsteht.
  - ► *Quantoren* (oder Quantifikatoren) zur Modellierung der Beschränkung bzw. Wahl der Variablen (“Es existiert eine Zahl so dass... ”, “für alle Zahlen gilt ”) .

Beispiel Sei QuadratGerade(n) die Aussagenschablone:

"Das Quadrat der Zahl n ist gerade."

und Gerade(n) die Aussagenschablone:

"Die Zahl n ist gerade."

- Also z.B. Gerade(5) ist eine Aussage.

- Wir führen jetzt noch eine Möglichkeit ein, wie man aus einem Prädikat eine Aussage erhält: *Quantifizierung*.
- Der *Allquantor* $\forall$ fordert die Gültigkeit der Aussagenschablone für *alle* möglichen Belegungen einer Variable,
- der *Existenzquantor* $\exists$ fordert die Gültigkeit der Aussagenschablone für *mindestens eine* Belegung einer Variable.
- Dabei nehmen wir entweder implizit ein Universum aller Objekte an, oder wir geben im Kontext der Formeln explizit einen Grundbereich für die Variablen.

- Die Formalisierung des Satzes “Sei n eine beliebige ganze Zahl. Falls n^2 gerade ist, so ist auch n gerade.”:

$$\forall n \left(\text{QuadratGerade}(n) \Rightarrow \text{Gerade}(n)\right)$$

wenn wir den Bereich der ganzen Zahlen betrachten.

- Oder wir könnten den Grundbereich für die Variable n im Quantor spezifizieren:

$$\forall\, n \in \mathbb{Z} \;\left(\text{QuadratGerade}(n) \Rightarrow \text{Gerade}(n)\right).$$

- Häufig schreibt man auch die Variablen unter Quantor, z.B.

$$\forall_{n\in\mathbb{Z}} \left(\text{QuadratGerade}(n) \Rightarrow \text{Gerade}(n)\right).$$

Beispiel

- Wir formalisieren die Aussage “Es gibt keine rationale Zahl x mit $x^2 = 2$.” als

$$\neg\Big(\exists_{x\in\mathbb{Q}}\, x^2 = 2\Big).$$

- Wir können es auch so schreiben:

$$\neg\Big(\exists_x\, x \in \mathbb{Q}, x^2 = 2\Big)$$

Wenn wir “ , ” zwischen Prädikaten benutzen, bedeutet es “und”.

- Wir haben die folgenden De Morgan-gesetze für Quantoren:
  - $\neg\forall x\, F$ ist äquivalent zu $\exists x\, \neg F$
  - $\neg\exists x\, F$ ist äquivalent zu $\forall x\, \neg F$
- **Beispiel.** Der Satz $\neg\Big(\exists_{x\in\mathbb{Q}}\, x^2 = 2\Big)$ ist äquivalent zu $\forall_{x\in\mathbb{Q}}\ x^2 \neq 2$.
- Wir können mehrere Quantoren in einer Formel haben.
  - Z.B. erst definieren wir das Prädikat $Prim(p)$ dass p ist eine Primzahl: $Prim(p) :=$ "$p \in \mathbb{N}, p > 1, (\forall_{d\in\mathbb{N}}(d|p \Rightarrow d = p \vee d = 1))$".
  - Jetzt können wir schreiben "jede natürliche Zahl die grösser als 1 ist hat einen Primteilerßo:

$$\forall_{n\in\mathbb{N}\setminus\{0,1\}}\exists_{p\in\mathbb{N}}\, Prim(p) \wedge p \mid n$$

1. Beweise und Beweisprinzipien - Wiederholung

2. Arithmetik - Wiederholung

3. Modulare Arithmetik

4. Die Sprache der Prädikatenlogik

5. Beweisstrategien für Sätze mit Prädikaten und Quantoren

6. Weitere Beweis-Beispiele

- Strategie für den Allquantor $\forall x\, F$
  - Wir nehmen ein **beliebiges** abstraktes Element u des Universums an.
  - Als Variable hat u genau die Eigenschaften, die alle Elemente des Universums gemein haben.
  - Wir zeigen F für u als Belegung von x.
- Strategie für den Existenzquantor $\exists x\, F$
  - Wir wählen ein **geeignetes** konkretes Element u des Universums.
  - Da u konkret ist, können Eigenschaften von u genutzt werden.
  - Wir zeigen F für u als Belegung von x.

Beispiel Für jede natürliche Zahl existiert eine echt größere gerade natürliche Zahl.

Formalisierung für das Universum natürlicher Zahlen:

$$\forall n \, \exists m \left(2 \mid m, m > n \right)$$

Beweisversuch. Sei n eine beliebige natürliche Zahl. Wir definieren $m := 2n$. Dann ist m offenbar durch 2 teilbar. Wir haben auch $m - n = 2n - n = n > 0$ und damit $m > n$ folgt. □

- Der Beweis ist *falsch*, denn die Annahme einer zusätzlichen Eigenschaft von n, d.h. $n > 0$, ist *nicht zulässig*.

Ein korrektes Beweis. Sei n eine beliebige natürliche Zahl. Wir definieren $m := 2(n + 1)$. Dann ist m offenbar durch 2 teilbar. Weiterhin gilt $m - n = 2(n + 1) - n = n + 2 > 0$ und damit ist $m > n$. □

Bispiele. Wir betrachten das Universum $\mathbb{N}$.

- Sei $A(x, y)$ das Prädikat $x + y = 2x$.
- Beweise dass $\forall x \exists y A(x, y)$.
  - Sei x beliebig, Sei $y := x$. Dann $x + y = x + x = 2x$, also $A(x, y)$ ist wahr □
- Beweise dass $\exists x A(x, x)$.
  - Sei $x := 2$, dann $A(x, x) = A(2, 2)$ lautet $2 + 2 = 4$, also die Aussage ist wahr. □
- Können wir schreiben $\forall x \exists x A(x, x)$? JEIN.
  - Formal ist das erlaubt, aber der innere Quantor bindet x neu. Der äußere Quantor hat damit keinen Einfluss auf die Aussage.
  - Um Verwirrung zu vermeiden, benutzen wir bei aufeinanderfolgenden Quantoren verschiedene Variablennamen: $\forall x \exists y A(x, y)$

- Verschiedene Prädikat-Aussagen können mit Hilfe von Junktoren kombiniert werden, z. B. $\Big(\exists x A(x)\Big) \wedge \Big(\forall x (A(x) \Rightarrow B(x))\Big)$
- Wir können die Variablennamen “recyceln”. Aber müssen wir nicht: $\Big(\exists x A(x)\Big) \wedge \Big(\forall y (A(y) \Rightarrow B(y))\Big)$.
- Die Ordnungsreihe ist wichtig. Die Aussage

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

ist wahr und die Aussage

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

ist falsch.

1. Beweise und Beweisprinzipien - Wiederholung

2. Arithmetik - Wiederholung

3. Modulare Arithmetik

4. Die Sprache der Prädikatenlogik

5. Beweisstrategien für Sätze mit Prädikaten und Quantoren

6. Weitere Beweis-Beispiele

Satz. Sei $n \in \mathbb{N}$, und seien $d_k \dots d_0$ die Dezimalstellen von n. Dann $3 \mid n$ gdw $3 \mid d_0 + \dots + d_k$.

Beweis.

- Wir haben $n = d_0 + 10 \cdot d_1 + 100 \cdot d_2 + \dots + 10^k \cdot d_k$.
- Wir haben $10^k \equiv 1^k \equiv 1 \mod 3$ für alle k.
- Es folgt dass $n \equiv d_0 + d_1 + \dots + d_k \mod 3$.
- Insbesondere $n \equiv 0 \mod 3$ gdw $d_0 + \dots + d_k \equiv 0 \mod 3$. □
- Notation: anstatt von $n = d_0 + 10 \cdot d_1 + 100 \cdot d_2 + \dots + 10^k \cdot d_k$ schreiben wir auch $n = \sum_{i=0}^{k} d_i 10^i$.

- Erinnerung: für jede reele Zahl x und jede $k \in \mathbb{N}_+$ gilt $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \ldots + x + 1)$.
- Erinnerung: für jede reele Zahl x und alle $a, b \in \mathbb{N}$ gilt $x^{ab} = (x^a)^b$.

Satz. Sei $n \in \mathbb{N}$. Falls $2^n - 1$ prim ist, dann ist auch n prim.

Beweis.
- Für $n = 0$ oder $n = 1$ ist $2^n - 1$ keine Primzahl. Wir können also $n \geq 2$ annehmen.
- Nehmen wir an n ist nicht prim.
- Dann schreiben wir $n = ab$ mit $a, b > 1$.
- Es folgt $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \ldots + 2^a + 1)$.
- Da $a > 1$, es folgt $2^a - 1 > 1$. Da auch $b > 1$, es folgt $2^a - 1 < 2^{ab} - 1 = 2^n - 1$, also $2^a - 1$ ist ein Teiler von $2^n - 1$ der strikt zwischen 1 und $2^n - 1$ liegt.
- Also ist $2^n - 1$ nicht prim, was die Kontraposition beweist, und damit auch die ursprüngliche Aussage. □