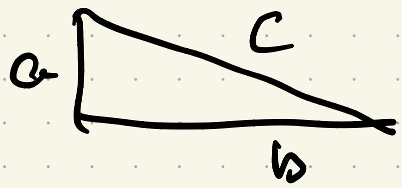
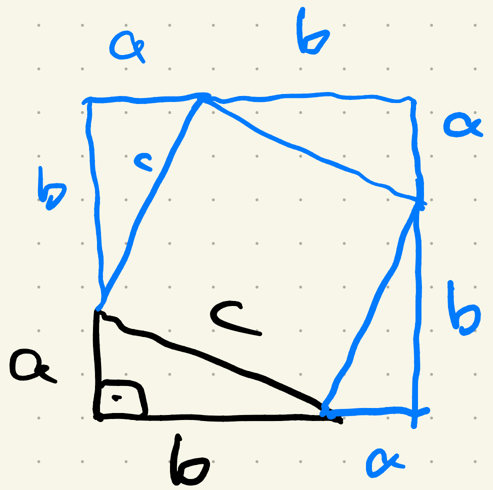
2 Kunst: das Beweisen

Satz 2.1



$$a^2+b^2=c^2$$

Beweis



$$(a+b)^2 = c^2 + 4\cdot\frac{a\cdot b}{2} \qquad \leftarrow (\text{wahr})$$

$$\Leftrightarrow \quad a^2+2ab+b^2 = c^2 + 2a\cdot b \quad \Big| -2ab$$

$$\Leftrightarrow \quad a^2+b^2 = c^2 \qquad \square$$

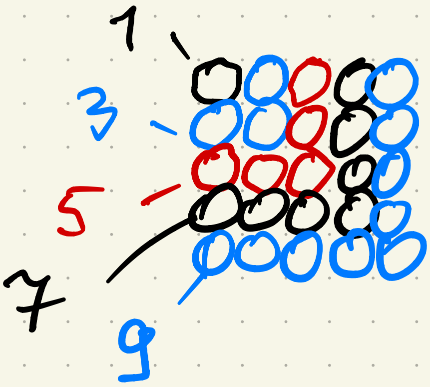
2.1 Vollständige Induktion

Bsp:

$$1 = 1 = 1^2$$
$$1+3 = 4 = 2^2$$
$$1+3+5 = 9 = 3^2$$
$$1+3+5+7 = 16 = 4^2$$
$$1+3+5+7+9 = 25 = 5^2$$
$$\vdots$$

Lemma: $\sum_{k=1}^{n}(2\cdot k-1) = n^2$ für alle $n\in\mathbb{N}$.

Beweis:



(Ist das ein Beweis?)

Vollständige Induktion, Schema:

(IA) • Beweise die Aussage für $n=1$ (bzw einen anderen Startwert)

(IS) • Beweise: Falls die Aussage für n wahr ist, dann auch für $n+1$.

IA: „Induktionsanfang" IS: Ind.-schluss

Bsp Beweis Lemma oben.

IA: $1 = \sum_{k=1}^{1}(2k-1) \overset{?}{=} 1^2 = 1$ wahr.

IS: Sei $\sum_{k=1}^{n}(2k-1) = n^2$ wahr.

IV Induktionsvoraussetzung

z.z. $\sum_{k=1}^{n+1}(2k-1) = (n+1)^2$

$$\Leftrightarrow \sum_{k=1}^{n}(2k-1) + 2(n+1)-1 = n^2+2n+1$$

$$\overset{IV}{\Leftrightarrow} \quad n^2 + 2n+2-1 = n^2+2n+1$$

wahr

$\square$

<u>Bsp.</u> für alle $n \in \mathbb{N}$: $2^n > n^2$.

Falsch • $2^2 > 2^2$ F $(=)$

• $2^3 > 3^2$ F $(<)$

• $2^4 > 4^2$ F $(=)$

$n=5$: $32 > 25$

$n=6$: $64 > 36$

$n=7$: $128 > 49$

$n=8$: $256 > 64$

<u>Bew.</u> <u>IA</u>: $2^5 = 32 > 25 = 5^2$

<u>IS</u>: Sei $2^n > n^2$ wahr.

z.z. $2^{n+1} > (n+1)^2$

$$\Leftrightarrow 2 \cdot 2^n > n^2+2n+1$$

$$\Leftrightarrow 2^n + 2^n > n^2+2n+1$$

Falls ① $2^n > n^2$ und

② $2^n > 2n+1$, bingo!

① ✓ IV. ②: $2^n > n^2 \overset{②}{>} 2n+1$

z.z. $n^2 > 2n+1$ für $n \geq 5$

$\Leftrightarrow n^2 - 2n - 1 > 0$

$\Leftrightarrow n^2 - 2n + 1 - 1 - 1 > 0$

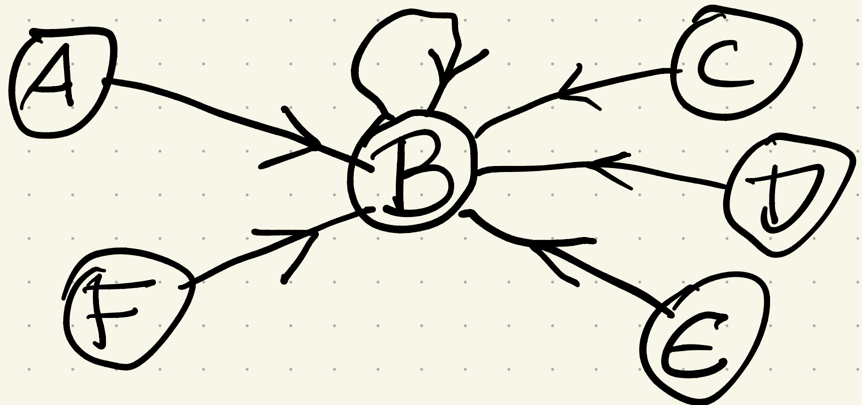
$\Leftrightarrow (n-1)^2 - 2 > 0$

$\Leftrightarrow (n-1)^2 > 2$ wahr für $n > 5$

---

3 Formale Logik

1:



2: Von B geht nur ein Pfeilweg, und zwar nach „ME“

Aussagen, die nur wahr oder falsch sein können:

1. „Die Erde ist ein Würfel"
2. „Bier ist gesund und lecker"
3. „Wenn es heute Hasen regnet, dann gibt es morgen Reibekuchen in der Mensa"

Form: 1. : A ← („atomare Aussage")

2. : B und C

3. : Wenn D, dann E

<u>Aussagenlogik</u>: Bausteine:

- A, B, C, D, ... (atomare Auss.)
- $\land$, $\lor$, $\neg$ („und", „oder", „nicht")

Alles, was wir daraus bauen können, ist eine logische Aussage (syntaktisch korrekt, also nicht „A ∧")

<u>Fragen</u>:
- Welche Formeln sind gleichbedeutend?
- Ist eine Formel erfüllbar?

(Kann sie wahr sein?)

- Folgt aus X immer Y?

<u>Regeln</u>: 1. Jede atomare Aussage kann Werte 0 oder 1 haben. (statt „falsch" oder „wahr")

2. $A \wedge B$, $A \vee B$, $\neg A$ erklären durch <u>Wahrheitswertetafeln</u>:

A	B	$A \wedge B$	$A \vee B$	$\neg B$	$\neg A \wedge \neg B$
0	0	0	0	1	1
0	1	0	1	0	0
1	0	0	1		0
1	1	1	1		0

<u>Bsp</u> • $A \wedge B$ vs. $(\neg A) \wedge (\neg B)$, gleichbedeutend?

• $(\neg A) \wedge (\neg B)$ vs. $\neg (A \vee B)$

<u>Vereinbarung</u>:

$\neg$ vor $\wedge, \vee$ vor $\Rightarrow$ vor $\Leftrightarrow$

Also $(\neg A) \wedge (\neg B)$ ist $\neg A \wedge \neg B$

A	B	$\neg A \wedge \neg B$	$\neg(A \vee B)$
0	0	1	1
0	1	0	0
1	0	0	0
1	1	0	0

also: $\neg A \wedge \neg B$ gleichbedeutend mit: $\neg(A \vee B)$

(de Morgansche Regel, vgl: $-x-y$
$= -(x+y)$)

Weitere Zeichen (eigtl. unnötig, aber bequem)

$\Rightarrow$: Folgezeichen (aka Implikation)

$\Leftrightarrow$: Äquivalenzzeichen

$\dot{\vee}$: exklusives oder (entweder oder, auch XOR, $\oplus$, ...)

A	B	$A \Rightarrow B$	$A \Leftrightarrow B$	$A \dot{\vee} B$
0	0	1	1	0
0	1	1	0	1
1	0	0	0	1
1	1	1	1	0

(Es ist $A \Rightarrow B$ gleichbed. mit $\neg A \vee B$)

Def • Eine Aussage heißt **Tautologie**, falls sie immer wahr ist (also für alle 0-1-Möglichkeiten für $A, B, \ldots$ immer 1 rauskommt)

• **unerfüllbar**: [analog] … immer 0 rauskommt; sonst **erfüllbar**

Fakt Aussage ist Tautologie, genau dann, wenn ihre Negation unerfüllbar ist.

z.B. $A \vee \neg A$ ist Tautologie

A	$A \vee \neg A$	$\neg(A \vee \neg A)$
0	1	0
1	1	0

unerfüllbar

$\equiv \neg A \wedge \neg\neg A$

$\equiv \neg A \wedge A$

Lemma 3.1 (Kontraposition)

$A \Rightarrow B$ gleichbedeutend mit $\neg B \Rightarrow \neg A$.

Beweis (mit Wahrheitswertetafeln, oder:)

$A \Rightarrow B$ glbd. $\neg A \vee B$ glbd. $B \vee \neg A$

glbd. $\neg\neg B \vee \neg A$ glbd. $\neg B \Rightarrow \neg A$ $\square$

Das liefert ein weiteres Beweisprinzip:
Um $A \Rightarrow B$ zu zeigen, reicht es
$\neg B \Rightarrow \neg A$ zu zeigen

Lemma 3.2: Für alle $n \in \mathbb{N}$ gilt:
ist n^2 gerade, dann auch n.

Beweis (Kontraposition)
z.z.: ist n^2 ungerade, dann auch n.
n ungerade, also $n = 2k-1$ $(k \in \mathbb{N})$
also $n^2 = (2k-1)^2 = 4k^2 - 4k + 1$
$$= \underbrace{4\cdot(k^2-k)}_{\text{gerade}} + 1. \qquad \square$$

... und noch ein Beweisprinzip:

- Widerspruchsbeweis:
  Um A zu beweisen, zeige,
  dass $\neg A$ falsch ist.
  Und zwar, indem wir aus $\neg A$
  logisch korrekt folgern, bis da
  eine offenbar falsche Aussage steht.

3.2 Prädikatenlogik

Bausteine wie eben, aber auch:

- $\forall, \exists$: Quantoren („für alle“, „es gibt“)
- $P(\cdot,\cdot)$: Prädikate, wahr oder falsch ($P(\cdot)$, $P(\cdot,\cdot)$, ...)
- f: Funktionszeichen

Das hilft: statt „für alle $n \in \mathbb{N}$“ nun „$\forall n \in \mathbb{N}$:“

z.B.
- $\forall n \in \mathbb{N}$: n^2 gerade, dann auch n. (wahr)
- $\exists n \in \mathbb{N}$: $2n \notin \mathbb{N}$ (falsch)

Nur ein toter alter weißer Mann
ist ein guter " " " .

wenn tot, dann gut.

Sei AWM die Menge alter weißer Männer.

$$\forall m \in AWM: \; T(m) \Rightarrow G(m)$$

d.h. $$\forall m \in AWM: \; \neg T(m) \vee G(m)$$

„Auf jeden Topf passt ein Deckel"

T: Menge der Töpfe

D: Menge aller Topf-Deckel

$$\forall t \in T \; \exists d \in D : P(d,t)$$

„... passt auf..."

<u>Negation</u>

- $A \xrightarrow{\neg} \neg A$
- $A \Rightarrow B \xrightarrow{\neg} \neg(\neg A \vee B) = A \wedge \neg B$
- $\forall t \in T : R(t) \xrightarrow{\neg} \exists t \in T : \neg R(t)$
- $\exists t \in T : R(t) \xrightarrow{\neg} \forall t \in T : \neg R(t)$

<u>Bsp</u> $\neg \forall m \in AWM : \neg T(m) \vee G(m)$

glbd. $\exists m \in AWM : \neg(\neg T(m) \vee G(m))$

" $\exists m \in AWM : T(m) \wedge \neg G(m)$

$$\neg \forall t \in T \; \exists d \in D : P(d,t)$$

glbd. $\exists t \in T \; \neg \exists d \in D : P(d,t)$

" $\exists t \in T \; \forall d \in D : \neg P(d,t)$