Diskrete Mathematik

Prof. Stefan Wolf

HS 2010

Michal Sudwoj

Geschrieben in
XeLaTeX

INHALTSVERZEICHNIS

Inhaltsverzeichnis

Teil I

Vorlesungsnotizen

0.1 Inhalt der Vorlesung

- Logik: Aussagenlogik , Beweise
- Mengenlehre: Alle Objekte
- Kombinatorik
- Graphentheorie
- Zahlentheorie, Algebra
  - Anwendungen: Kommunikation, Kryptologie, Fehlerkorrektur

Kapitel 1

Motivation

Worum geht es in dieser Vorlesung?

Bsp.1: Modellierung:

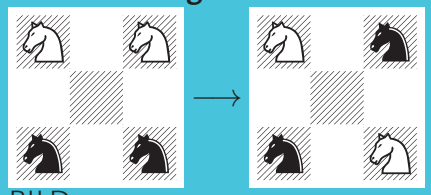


BILD
Fazit:

- Wegschälen vom Umweltlichen hat das Problem einfach gemacht $\Longrightarrow$ **Abbstraktion**
- Viele diskrete Probleme führen auf Graphen

Bsp.2: Zahlentheorie:

$$N = \{0, 1, 2, 3, \ldots\}$$

$a \mid b$ "a teil b" $a, b \in \mathbb{N}$

$a \mid b :\leftrightarrow \exists n \in \mathbb{N} : a \cdot n = b$

Bsp.:

$2 \mid 6$

$$3 \nmid 6$$
$$2 \equiv 5 \pmod 3$$
$$3 \not\equiv 5 \pmod 3$$

p Primzahl $:\leftrightarrow (a \mid p \rightarrow (a = 1 \vee a = p) \wedge p \neq 1)$

Intuition $\leftrightarrow$ Beweis
Jede Zahl hat eine **eindeutige** Primzahlzerlegung (nämlich:

$$p \mid (a \cdot b) \rightarrow p \mid a \vee p \mid b \quad ;$$

wir haben's noch nicht bewiesen)

Satz:
Es gibt unendlich viele Primzahlen

Bew.: Euklid:

Annahme: Es gibt nur endlich viele Primzahlen $p_1, \ldots, p_n$

$$M = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$$

$$\forall i : p_i \nmid M$$

↯ ■

Bsp.3: Kombinatorik ("systematisches Zählen"):

Kette mit p Perlen in a verschiedene Farben

Anzahl mögliche Ketten? a^n

Anzahl Muster?

Wie oft kommt jedes Muster vor?

Gegeben: p ist prim

$\Longrightarrow$ einfärbig: 1 mal

$\Longrightarrow$ mehrfärbig: p mal

$$\Longrightarrow \frac{a^p - a}{p} + a = a \cdot (1 + \frac{a^{p-1} - 1}{p})$$

a beliebig, p Primzahl

$$p \mid (a^p - a)$$

$a^p \equiv a \pmod{p}$
$(p \nmid a) \rightarrow (a^{p-1} \equiv 1 \pmod{p})$
Kleines Satz von Fermat

Bsp.4: Geometrie:

Rechteckige Terrase $a \cdot b \mid a, b \in \mathbb{N}$
Was sind die grösstmöglichen Quadratplatten, mit denen mann sie exakt belegen kann?
$a \geq b$ Quardat aufteilen in $b \cdot b$ und $(a-b) \cdot b$
Beobachtungen:

- Jede Belegung des ganzen führt auf separate Belegungen von
  $[b \cdot b]$ und $[(a-b) \cdot b]$
- Es reicht, $[(a-b) \cdot b]$ zu berechnen.

$$\mathrm{R}_{a-b}(b) = b \bmod (a-b)$$

Fortfahren, bis wir ein Quadrat erhalten. Warum wird das sicher passieren?
Spätestens bei $1 \cdot 1$
Algorithmus (Euklid):

a, b
$r_1 = \mathrm{R}_b(a)$
$r_2 = \mathrm{R}_{r_1}(b)$
$\vdots$
$r_n = \mathrm{R}_{r_{n-1}}(r_{n-2})$
$\vdots$

$r_k = \mathrm{ggT}(a, b)$
0

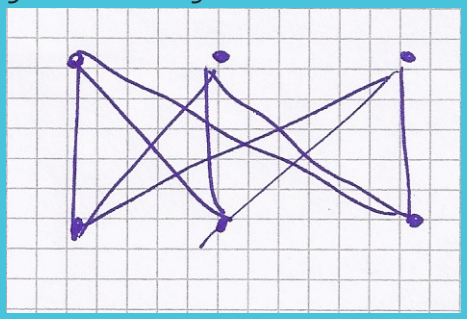
Bsp.5:

2 Sanuhren: 21 min und 15 min. Wir wollen 3 min abmessen.

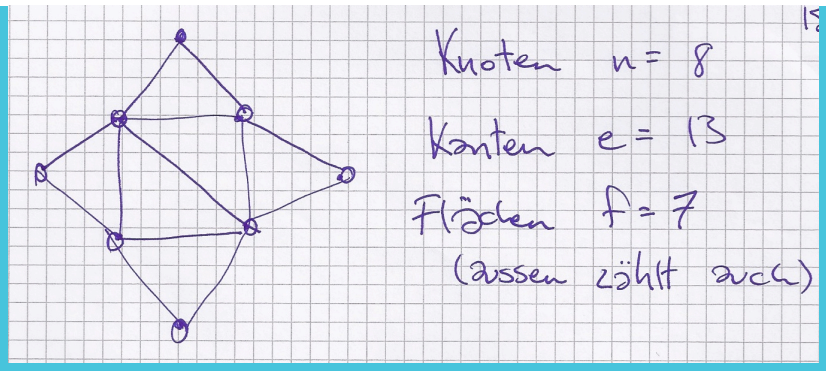
Euklid:	21,	15,	6,	3,	0
21 min:	1	0	1	-2	
15 min:	0	1	-1	3	

Bsp.6: Verbindungen ohne Überkreuzen:

3 Häuser mit 3 Werke verbinden → geht nicht!

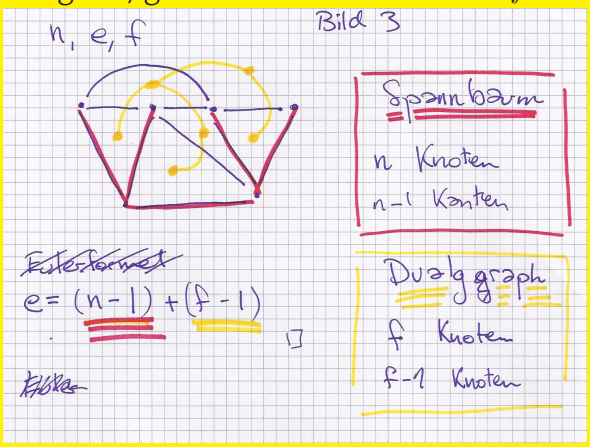


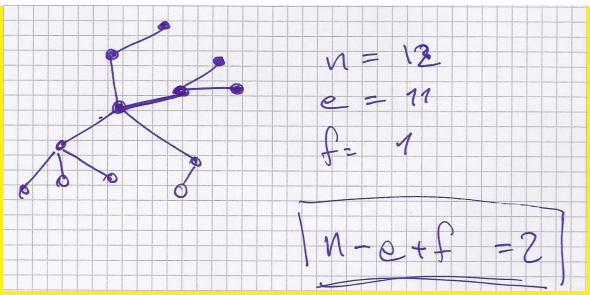
der Graph ist nicht **planar**.



Beweisidee::

Für einen Baum (kreislos, zusammenhängend) gilt $n = e + 1 \implies n - e + f = 2$





Eulersche Polyederformel

Kapitel 2

Logik

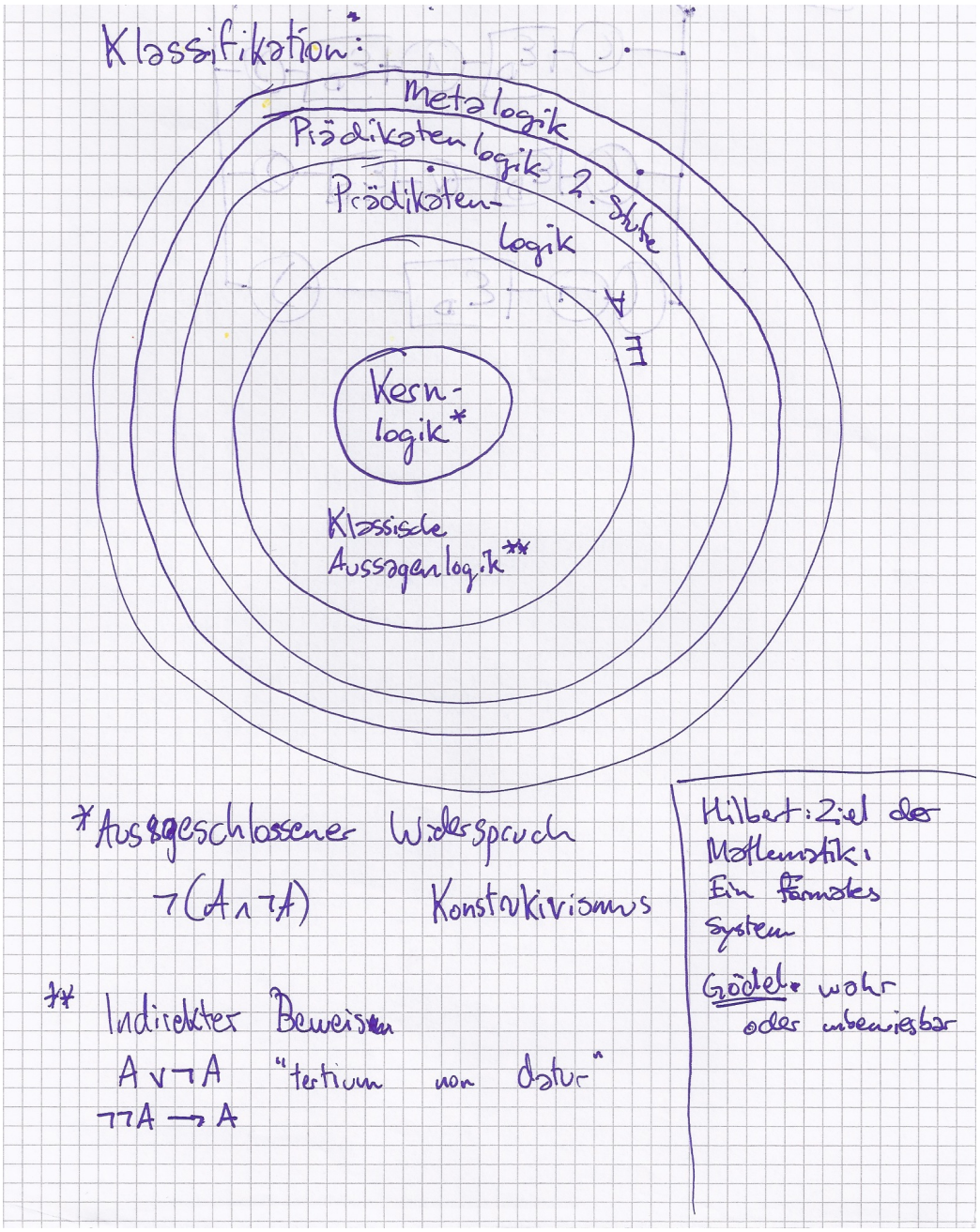
2.1 Was ist Logik?

"Septem artes liberalen", 7 freie Künste
Fächerkanon:

- Trivium
  - Grammatik
  - Rhetorik
  - Logik
- Quadrivium
  - Arithmetik
  - Geometrie
  - Musik
  - Astronomie

↳ "trivial"
"logos": argumentierende, begründende Rede, vernünftiges Sprechen
Logik: Lehre des Begründens, Argumentierens, Schliessens

1918:	Frege:	$\frac{\text{schön}}{\text{Ästhetik}} = \frac{\text{gut}}{\text{Ethik}} = \frac{\text{wahr}}{\text{Logik}}$
1970:	Patzig:	Logik = Theorie der Aussagen, die aufgrund **ihrer Form** wahr sind.
1985:	Menne:	Logik = Lehre von der **Folgerichtigkeit**


Klassifikation:
Metalogik
Prädikatenlogik 2. Stufe
Prädikaten-
logik
∀
∃
Kern-
logik*
Klassische
Aussagenlogik**
*Ausgeschlossener Widerspruch
¬(A ∧ ¬A)
Konstruktivismus
** Indirekter Beweis
A ∨ ¬A "tertium non datur"
¬¬A → A
Hilbert: Ziel der
Mathematik:
Ein formales
System
Gödel: wahr
oder unbeweisbar

Gibt es $r_1, r_2 \notin \mathbb{Q}$ mit ${r_1}^{r_2} \in \mathbb{Q}$? Ja.

$\sqrt{2} \notin \mathbb{Q}$ $\quad [l \implies$ Bruch nicht gekürzt.$]$

$\sqrt{2}^{\sqrt{2}} \in \mathbb{Q} \vee \sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$ $\quad \sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = 2$

2.2 Aussagenlogik

2.2.1 Definitionen

Def.: Aussage:
Eine Aussage ist ein sprachlicher Ausdruck, der wahr oder falsch ist.

Bsp.:

- Wenn es regnet, dann sind die Strassen nass.
- Wenn der Hahn kräht auf dem Mist, ändert das Wetter oder es bleibt wie es ist. (Tautologie)
- Dies ist keine Aussage. (Aussage, falsch)
- Diese Aussage ist falsch.
- Wale sind Fische und Fische sind Tiere.

Atomare Aussagen mit **Junktoren** verbunden → Zusammengesetzte Aussagen.
Junktoren als Wahrheitsfunktionen

↳ Wahrheitstabellen
`http://en.wikipedia.org/wiki/Logical_connective`
AND (konjunktion)

A	B	$A \wedge B$
W	W	W
W	F	F
F	W	F
F	F	F

NOT

A	$\neg A$
W	F
W	F

NAND (universell)

A	B	$A \mid B$
W	W	F
W	F	W
F	W	W
F	F	W

OR (disjunktion)

A	B	$A \vee B$
W	W	W
W	F	W
F	W	W
F	F	F

XOR (ausschliessendes Oder)

A	B	$A \oplus B$
W	W	F
W	F	W
F	W	W
F	F	F

XNOR (Äquivalenz)

A	B	$A \leftrightarrow B$
W	W	W
W	F	F
F	W	F
F	F	W

$A \leftrightarrow B \equiv \neg(A \oplus B)$

Implikation

A	B	$A \rightarrow B$
W	W	W
W	F	F
F	W	W
F	F	W

$A \rightarrow B \equiv (\neg A) \vee B$

Bem.:

$A \to B$ ist nicht gleich $B \to A$ oder $\neg A \to \neg B$

$A \to B \equiv \neg B \to \neg A$ (indirekter Beweis)
$B \to A \equiv \neg A \to \neg B$

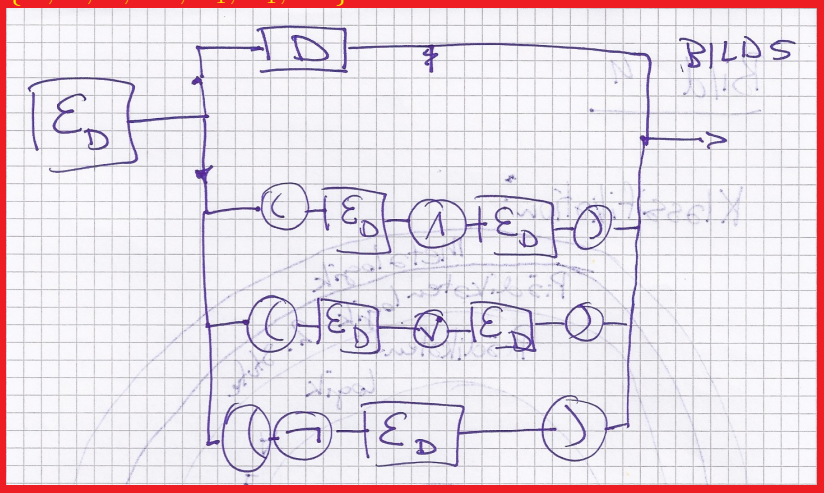
Syntax $\leftrightarrow$ Semantik

Syntax:	Welche Zeichenketten sind korrekte Formeln?
Semantik:	Für korrekte Formeln: wahr oder falsch?

2.2.2 Syntax der Aussagenlogik

Def.: korrekte Formel:

Syntaktisch korrekte Formel ε_D über Atomformeln $D := \{A, B, C, \ldots, A_1, B_1, \ldots\}$



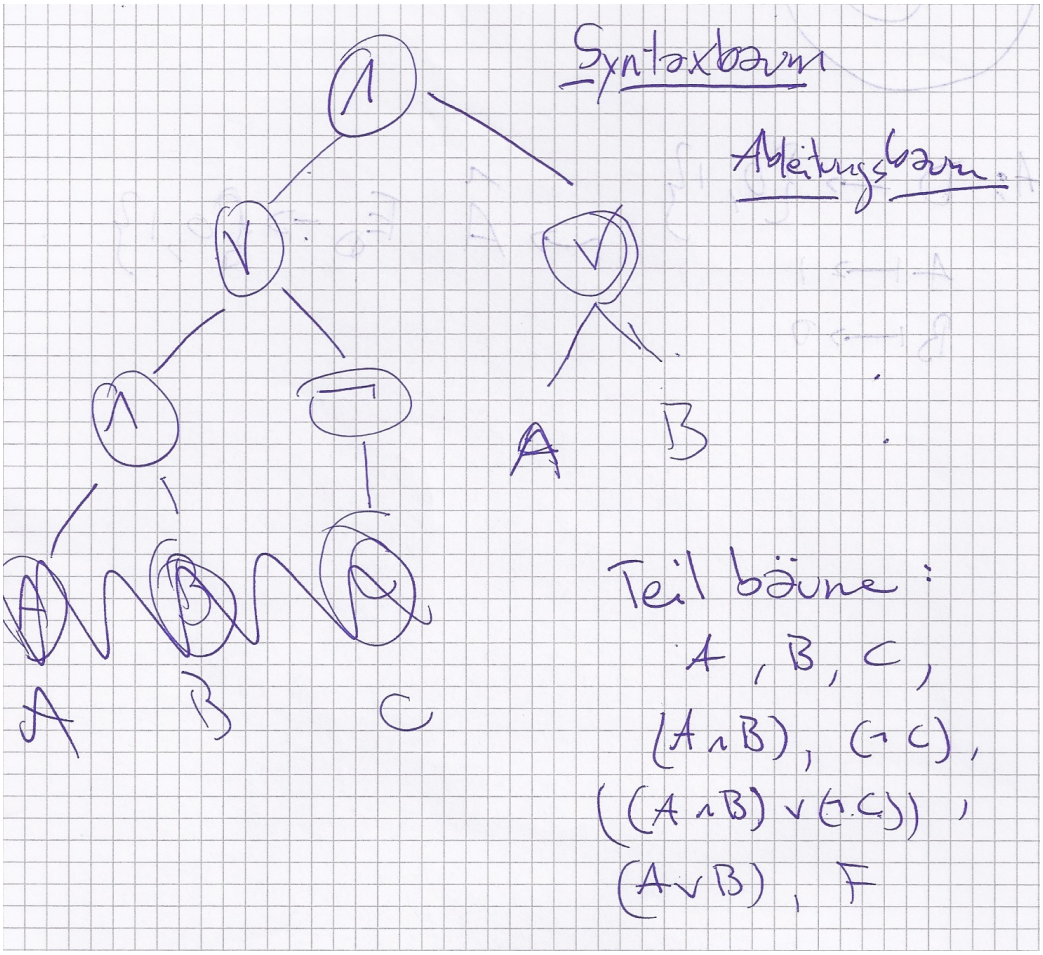
Syntaktisch korrekte Formeln ε_D ist definiert über Atomformeln D:

- Atomformeln
- Falls f und g syntaktisch korrekt, dann auch $(\neg f), (f \wedge g), (f \vee g)$
- Das ist alles.

Bsp.:

- A
- $(\neg A)$

- $(\neg(\neg A))$
- B
- $(A \wedge B)$
- $(A \wedge A)$
- $(((A \wedge B) \vee (\neg C)) \wedge (A \vee B))$



Teilformel = Teilstring, der selbst eine Formel ist.

Bsp.:

- A
- B
- C
- $(A \wedge B)$
- $(\neg C)$
- $((A \wedge B) \vee (\neg C))$
- $(A \vee B)$
- F

2.2.3 Semantik der Aussagenlogik

Wahrheitswerte der Atomformeln → Wahrheitswerte der zusammengesetzten Formeln

Vollständige Wahrheitstabelle

$(((A \wedge B) \vee (\neg C)) \wedge (A \vee B))$

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

Def.: Belegung:
D , ε_D wie oben.

$\mathcal{A} : D \to \{0,1\}$ Belegung
$\hat{\mathcal{A}} : \varepsilon_D \to \{0,1\}$ Fortsetzung von $\mathcal{A}$

- $\hat{\mathcal{A}}(D) := \mathcal{A}(D)$ für Atomformel D
- $\hat{\mathcal{A}}((F \wedge G)) := \hat{\mathcal{A}}(F) \wedge \hat{\mathcal{A}}(G)$
- $\hat{\mathcal{A}}((F \vee G)) := \hat{\mathcal{A}}(F) \vee \hat{\mathcal{A}}(G)$
- $\hat{\mathcal{A}}((\neg F)) := 1 - \hat{\mathcal{A}}(F)$

Vereinfachungen:

- Weglassen von Klammern