

# Diskrete Strukturen

## Vorlesung 1: Logik

Andreas Maletti

14. Oktober 2014

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## Fähigkeiten

- Standardnotation lesen und schreiben
- Einführung mathematisches Denken
- Beweise lesen und analysieren
- (formale) Beweise führen

## heutige Vorlesung

- ① Einführung Aussagenlogik
- ② Äquivalenz von komplexen Aussagen
- ③ Tautologien und Unerfüllbarkeit

Bitte Fragen direkt stellen!

Organisation

## Materialien

- Folien und Ankündigungen im OLAT-Kurs:  
[W14.Inf.DiskreteStrukturen](#)
- Literatur (Selbststudium und Vertiefung):
  -  **CHRISTOPH MEINEL, MARTIN MUNDHENK**  
*Mathematische Grundlagen der Informatik*  
Vieweg+Teubner, 5. Auflage, 2011
  -  **ANGELIKA STEGER**  
*Diskrete Strukturen — Band 1*  
*Kombinatorik, Graphentheorie, Algebra*  
Springer-Verlag, 2. Auflage, 2007

# Organisation

## Vorlesung

- dienstags, 17:15–18:45 Uhr, Hörsaal 2
- keine VL am **2. Dezember 2014** — *dies academicus*

## Übungen

- Übungsgruppen (jede Woche):

Wochentag	Zeit	Raum	Übungsleiter
montags	11:15–12:45	SG 3-10	CLAUDIUS RÖHL
montags	15:15–16:45	SG 3-10	THOMAS WEIDNER
dienstags	13:15–14:45	SG 3-13	CHRISTOPH GAMM
dienstags	15:15–16:45	SG 3-10	PETER LEUPOLD
mittwochs	11:15–12:45	SG 3-13	HANNES STRASS
mittwochs	13:15–14:45	SG 3-14	DOREEN HEUSEL
freitags	11:15–12:45	SG 3-14	CHRISTOPH GAMM

- keine Übung: **13.–17.10., 31.10., 19.11., 02.12.**  
— bitte Alternativtermin in der gleichen Woche wählen

## Übungen

- Hausaufgabenkontrolle:  
KAI HAINKE, SVEN KUBITZKY, KASIMIR WANSING
- Übungs- und Hausaufgabenblätter im OLAT
- bitte für Übungsgruppe im OLAT anmelden  
→ richtige Email-Adresse im OLAT hinterlegen

## Sprechstunden

● CHRISTOPH GAMM	nach Vereinbarung
● DOREEN HEUSEL	nach Vereinbarung
● PETER LEUPOLD	dienstags, 11-12 Uhr
● ANDREAS MALETTI	mittwochs, 15-16 Uhr
● CLAUDIO RÖHL	montags, 13-14 Uhr
● HANNES STRASS	nach Vereinbarung
● THOMAS WEIDNER	nach Vereinbarung

## Prüfungsvorbereitung

- erfolgreiche Lösen der Hausaufgaben

Punkte (in %)	Konsequenz
$\leq 49$	Prüfungsteilnahme überdenken
50–59	Prüfung vermutlich machbar
60–74	+1 Bonuspunkt ( $\approx 3\%$ ) für die Prüfung
75–89	+2 Bonuspunkte ( $\approx 7\%$ ) für die Prüfung
$\geq 90$	+3 Bonuspunkte ( $\approx 10\%$ ) für die Prüfung

- Abgabe der Hausaufgaben vor der Vorlesung  
(Abgabedatum steht auf dem Aufgabenblatt)

Grundlagen der Logik

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## StVO I, § 30(3) — Sonn- und Feiertagsfahrverbot [editiert]

An Sonn- und Feiertagen dürfen in der Zeit 0.00–22.00 Uhr Lastkraftwagen mit einer zulässigen Gesamtmasse über 7,5 t sowie Anhänger hinter Lastkraftwagen nicht verkehren. Dies gilt nicht für

- ① [...] und/oder
- ② die Beförderung von
  - a frischer Milch und frischen Milcherzeugnissen,
  - b frischem Fleisch und frischen Fleischerzeugnissen,
  - c frischen Fischen, lebenden Fischen und frischen Fischerzeugn.,
  - d leicht verderblichem Obst und Gemüse, und/oder
- ③ Leerfahrten im Zusammenhang mit Fahrten nach ②, und/oder
- ④ [...]

## §1.1 Definition (Aussage)

**Aussage** ist eine Repräsentation eines Satzes,  
der entweder **wahr** (1) oder **falsch** (0) ist

(genau ein Wahrheitswert, auch wenn evtl. unbekannt)

## Beispiele

- “*L befördert frische Milch*” ist eine Aussage  
für einen geg. Lastkraftwagen *L*
- “*D ist ein Feiertag*” ist eine Aussage  
für ein geg. Datum *D*
- “*2 ist eine Primzahl*” ist eine **wahre** Aussage
- “*2 + 2 = 5*” ist eine **falsche** Aussage

## weitere Beispiele

- “Jede gerade natürliche Zahl  $n > 2$  ist die Summe zweier Primzahlen” ist eine Aussage  
Wahrheitswert unbekannt (GOLDBACHs Vermutung, 1742)
- “Dieser Satz ist falsch” ist **keine** Aussage  
kann semantisch weder wahr noch falsch sein — Selbstreferenz

CHRISTIAN GOLDBACH (\* 1690; † 1764)

- studierte Medizin und Jura in Königsberg
- erlernte später Mathematik
- Tutor von Zar PETER II



## Aussagenlogik — Aussagen

fahm, nicht bestätigen, ob wirne aber sijon und fortwährend,  
 a manier singlet series lauter numeros unis modo in das quadrata  
 divisibilis gelingt auf folgen Weise will ich auf nun conjecture  
 bezadiom: das jahr Zahl welche sich zuzogen numeris primis  
 zusammengesetzt ist ein aggregatione von allen numerorum  
 primorum, die alle wan will / die unitatem mit reziproquem  
 hif auf da congerior omnia unitat. zim formul  

$$4 = \begin{cases} 1+1+1+1 \\ 1+1+2 \\ 1+3 \end{cases}$$

$$5 = \begin{cases} 2+3 \\ 1+1+1+2 \\ 1+1+1+1+1 \end{cases}$$

$$6 = \begin{cases} 1+5 \\ 1+2+3 \\ 1+1+1+1+1 \\ 1+1+1+1+2 \end{cases}$$
 dcl

Linear<sup>1</sup> folgen wir ganz offensichtlich den dementsprechenden  
von Pontryagin.

Si v. sit functionis  $y = f(x)$ . eiusmodi ut facta  $v = c \cdot \text{numero constante}$ , determinari posset  $x$  per  $c$ . et reliquias constantes in functione expressas, poterit etiam determinari valor ipsius  $x$ . in aequatione  $v = (av + b)(cv + d)$ .

Si anticipatur curva cuius abscissa sit  $x$ , applicata seu sit summae fieri  $\frac{x^n}{n \cdot 2^{n-1}}$  posita n. pro expressione terminorum, haec est applicata  $= \frac{x}{1 \cdot 2} + \frac{x^2}{2 \cdot 2^2} + \frac{x^3}{3 \cdot 2^3} + \frac{x^4}{4 \cdot 2^4} + \text{etc.}$  dico, si fuerit abscissa = 1, applicatio fieri  $= \frac{1}{2} = \frac{1}{3}$ : sed haec fieri  $= \frac{1}{2}$   
 abscissa = 1, applicatio fieri  $= \frac{1}{2} = \frac{1}{3}$ : sed haec fieri  $= \frac{1}{2}$   
 $\frac{1}{2}$   
 $\frac{1}{3}$   
 $\frac{1}{2}$

4 vel major infraenum.  
Jf. uno fons ex aliis ex fons ex aliis, Baffeffmij  
fons ex aliis ex fons ex aliis, ergo huius D  
Iur. st. n. 742.7 Gdssatt.

## Gegenstand der Logik

- **nicht** die Wahrheitsbestimmung von Basis-Aussagen  
(dies ist Aufgabe der Fachgebiete)
- Formalisierung von (komplexen) Aussagenverknüpfungen
- Bewertung von Aussagenverknüpfungen  
basierend auf Wahrheitswerten der Teilaussagen
- Schlussregeln

## Notation (Junktoren)

- (Basis-)Aussagen  $A, B, C, \dots$  aber auch "hatFisch"
- Negation  $\neg A$  nicht  $A$
- Konjunktion  $A \wedge B$   $A$  und  $B$
- Disjunktion  $A \vee B$   $A$  oder  $B$
- Implikation  $A \rightarrow B$  wenn  $A$ , dann  $B$

## Erklärungsversuch Notation

- Konjunktion  $A \wedge B$   $A$  und  $B$ 
  - entspricht  $A \cap B$  (unten offen)
  - Elemente von  $A \cap B$  müssen in  $A$  und  $B$  liegen
- Disjunktion  $A \vee B$   $A$  oder  $B$ 
  - entspricht  $A \cup B$  (oben offen)
  - Elemente von  $A \cup B$  müssen in  $A$  oder  $B$  liegen

## §1.2 Interpretation

- Jede Aussage (auch jede Aussagenverknüpfung) ist entweder **wahr** (1) oder **falsch** (0)
- Wahrheit von Aussagenverknüpfungen ergibt sich aus Wahrheit der Teilaussagen gemäß folgender Tabelle

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

## Schwierigkeit: Implikation

- $A \rightarrow B$  besteht aus **Vorbedingung A** und **Folgerung B**
- $A \rightarrow B$  ist genau dann falsch, wenn die Vorbedingung A gilt, aber die Folgerung B nicht

## Beispiel

- "Wenn es regnet, dann nehme ich den Schirm mit."
- Formalisierung: **Regen  $\rightarrow$  Schirm**
- wenn es nicht regnet, dann kann ich den Schirm mitnehmen oder daheim lassen (Vorbedingung nicht erfüllt)
- wenn es regnet und ich den Schirm nicht mitnehme, dann gilt die Aussage **Regen  $\rightarrow$  Schirm** nicht

## §1.3 Definition

- (aussagenlogische) **Atome** = primitive Aussagen wie  $A$ ,  $B$
- (aussagenlogische) **Formeln** = Aussagen inkl. Verknüpfungen

## Notizen

- Wahrheit eines Atoms abhängig von fachlicher “Aussage”
- Wahrheit einer Formel nur abh. von Wahrheit ihrer Atome

## Interesse

- wir sind an **wahren** Aussagen (Theoremen) interessiert  
→ Erkenntnisgewinn und Verständnis der Welt

## Nachweis

- die Wahrheit einer Aussage muss erst nachgewiesen werden  
→ **Beweis**

## Wahrheitswertetabelle

- einfachste Beweismethode
- Nachweis der Wahrheit der Aussage  
unabh. von der Wahrheit ihrer Atome

## Wahrheitswertetabelle

- Beweisschema für komplexe Aussagen
- tabellarische Auflistung aller Möglichkeiten
- funktioniert evtl. nicht bei Abhängigkeiten zw. Aussagen

### §1.4 Beispiel

- "Wenn  $A$  und  $B$  gelten, dann gilt  $A$ ."
- dabei können  $A$  und  $B$  beliebig komplexe Aussagen sein
- Formalisierung:  $(A \wedge B) \rightarrow A$
- Beweis durch Wahrheitswertetabelle:

$A$	$B$	$A \wedge B$	$(A \wedge B) \rightarrow A$
0	0	0	1
0	1	0	1
1	0	0	1
1	1	1	1

## §1.5 Beispiel

- “Eine natürliche Zahl, die nicht ungerade ist, ist gerade.”
- Formalisierung:  $\neg U \rightarrow G$
- Fachwissen: “Jede natürliche Zahl ist gerade oder ungerade.”
- neue Formalisierung:  $(U \vee G) \rightarrow (\neg U \rightarrow G)$

Beweis.

Beweis mit Wahrheitswertetabelle (mit Fachwissen):

$U$	$G$	$U \vee G$	$\neg U$	$\neg U \rightarrow G$	$(U \vee G) \rightarrow (\neg U \rightarrow G)$
0	0	0	1	0	1
0	1	1	1	1	1
1	0	1	0	1	1
1	1	1	0	1	1



StVO I, § 30(3) — Sonn- und Feiertagsfahrverbot [editiert]

[...] Dies gilt nicht für

- ① [...]
- ② die Beförderung von
  - a frischer Milch und frischen Milcherzeugnissen,
  - b frischem Fleisch und frischen Fleischerzeugnissen,
  - c frischen Fischen, lebenden Fischen und frischen Fischerzeugn.,
  - d leicht verderblichem Obst und Gemüse,

[...]

## Formalisierung

- $\neg((\text{hatMilch} \wedge \text{hatMilchE}) \wedge (\text{hatFleisch} \wedge \text{hatFleischE}) \wedge \dots)$
- $\neg((\text{hatMilch} \vee \text{hatMilchE}) \wedge (\text{hatFleisch} \vee \text{hatFleischE}) \wedge \dots)$
- $\neg((\text{hatMilch} \wedge \text{hatMilchE}) \vee (\text{hatFleisch} \wedge \text{hatFleischE}) \vee \dots)$
- $\neg((\text{hatMilch} \vee \text{hatMilchE}) \vee (\text{hatFleisch} \vee \text{hatFleischE}) \vee \dots)$

# Aussagenlogik — Formalisierung

hM	hME	hF	hFE	hM $\wedge$ hME	hF $\wedge$ hFE	hM $\vee$ hME	hF $\vee$ hFE
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	0	0	0	1
0	0	1	1	0	1	0	1
0	1	0	0	0	0	1	0
0	1	0	1	0	0	1	1
0	1	1	0	0	0	1	1
0	1	1	1	0	1	1	1
1	0	0	0	0	0	1	0
1	0	0	1	0	0	1	1
1	0	1	0	0	0	1	1
1	0	1	1	0	1	1	1
1	1	0	0	1	0	1	0
1	1	0	1	1	0	1	1
1	1	1	0	1	0	1	1
1	1	1	1	1	1	1	1

## Frage

Welche (weiteren) Beweistechniken kennen Sie?

## Mögliche Antworten

- beidseitige Implikationen
- Implikationskette
- Ringschluss
- indirekter Beweis
- Kontraposition
- vollständige Induktion
- ...

Äquivalenz

## §1.6 Definition (Äquivalenz)

Zwei Aussagen  $A$  und  $B$  sind äquivalent (geschrieben:  $A \leftrightarrow B$ ), genau dann wenn (gdw.) deren Wahrheitswerte übereinstimmen

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

## Beispiele

- $U \vee G$  und  $\neg U \rightarrow G$  sind äquivalent (siehe §1.5)
- $A \vee B$  und  $A \rightarrow B$  sind **nicht** äquivalent (siehe §1.2)

# Aussagenlogik — Äquivalenz

äquivalente Formeln	Bezeichnung
$A \wedge B$	$B \wedge A$ Kommutativität von $\wedge$
$A \vee B$	$B \vee A$ Kommutativität von $\vee$
$(A \wedge B) \wedge C$	$A \wedge (B \wedge C)$ Assoziativität von $\wedge$
$(A \vee B) \vee C$	$A \vee (B \vee C)$ Assoziativität von $\vee$
$A \wedge (B \vee C)$	$(A \wedge B) \vee (A \wedge C)$ Distributivität von $\wedge$
$A \vee (B \wedge C)$	$(A \vee B) \wedge (A \vee C)$ Distributivität von $\vee$
$A \wedge A$	$A$ Idempotenz von $\wedge$
$A \vee A$	$A$ Idempotenz von $\vee$
$\neg\neg A$	$A$ Involution $\neg$
$\neg(A \wedge B)$	$(\neg A) \vee (\neg B)$ DEMORGAN-Gesetz für $\wedge$
$\neg(A \vee B)$	$(\neg A) \wedge (\neg B)$ DEMORGAN-Gesetz für $\vee$

## §1.7 Theorem

$F_1 = A \vee (B \wedge C)$  und  $F_2 = (A \vee B) \wedge (A \vee C)$  sind äquivalent

Beweis.

Mit Wahrheitstabelle:

$A$	$B$	$C$	$B \wedge C$	$F_1$	$A \vee B$	$A \vee C$	$F_2$	$F_1 \leftrightarrow F_2$
0	0	0	0	0	0	0	0	1
0	0	1	0	0	0	1	0	1
0	1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	1	1
1	0	0	0	1	1	1	1	1
1	0	1	0	1	1	1	1	1
1	1	0	0	1	1	1	1	1
1	1	1	1	1	1	1	1	1



## Vorsicht

$F_1 = (A \rightarrow B) \rightarrow C$  und  $F_2 = A \rightarrow (B \rightarrow C)$   
sind **nicht** äquivalent.

## Beweis.

Mit Wahrheitstwertetabelle:

$A$	$B$	$C$	$A \rightarrow B$	$F_1$	$B \rightarrow C$	$F_2$	$F_1 \leftrightarrow F_2$
0	0	0	1	0	1	1	0
...	...	...	...	...	...	...	...



## §1.8 Beweisprinzip: beidseitige Implikationen

- die Aussage  $A \leftrightarrow B$  entspricht " $A \rightarrow B$  und  $B \rightarrow A$ " ( $A \leftarrow B$ )
- formal:**  $(A \leftrightarrow B) \leftrightarrow ((A \rightarrow B) \wedge (B \rightarrow A))$
- um  $A \leftrightarrow B$  zu zeigen, reicht es  $A \rightarrow B$  und  $B \rightarrow A$  zu zeigen

### Beweis dieser Aussage

$$F = (A \leftrightarrow B) \leftrightarrow ((A \rightarrow B) \wedge (B \rightarrow A))$$

$A$	$B$	$A \leftrightarrow B$	$A \rightarrow B$	$B \rightarrow A$	$(A \rightarrow B) \wedge (B \rightarrow A)$	$F$
0	0	1	1	1	1	1
0	1	0	1	0	0	1
1	0	0	0	1	0	1
1	1	1	1	1	1	1

## §1.9 Äquivalenzen für $\rightarrow$ und $\leftrightarrow$

- $A \rightarrow B$  und  $\neg A \vee B$  sind äquivalent
- $A \leftrightarrow B$  und  $(A \rightarrow B) \wedge (B \rightarrow A)$  sind äquivalent (siehe §1.8)

Beweis.

Mit Wahrheitstabelle:

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



## §1.10 Substitutionsprinzip

- äquivalente Formeln können füreinander substituiert werden
- Beweisprinzip: Äquivalenzkette

## §1.11 Theorem (Beweisprinzip: Kontraposition)

$A \rightarrow B$  und  $\neg B \rightarrow \neg A$  sind äquivalent

(“wenn  $A$ , dann  $B$ ” entspricht “wenn nicht  $B$ , dann nicht  $A$ ”)

Beweis.

Folge äquivalenter Formeln:

(Äquivalenzkette)

$$A \rightarrow B$$

gdw.  $\neg A \vee B$

§1.9

gdw.  $\neg A \vee \neg \neg B$

Inv.  $\neg$

gdw.  $\neg \neg B \vee \neg A$

Komm.  $\vee$

gdw.  $\neg B \rightarrow \neg A$

§1.9



## §1.12 Theorem

Sei  $n \in \mathbb{Z}$  beliebig. Falls  $n^2$  gerade ist, so ist auch  $n$  gerade.

Beweis.

Kontraposition von QuadratGerade  $\rightarrow$  ZahlGerade:

$$\neg\text{ZahlGerade} \rightarrow \neg\text{QuadratGerade}$$

Falls  $n$  nicht gerade ist, dann gilt  $n = 2k + 1$  für ein  $k \in \mathbb{Z}$  und

$$n^2 = (2k + 1)^2 = (2k)^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1 ,$$

womit  $n^2$  wieder ungerade (nicht gerade) ist.

(nutzt auch Fachwissen und Implikationskette — siehe später)



## Beispiel

[...] Dies gilt

$$\neg((\text{hatMilch} \vee \text{hatMilchE}) \vee (\text{hatFleisch} \vee \text{hatFleischE}) \vee \dots)$$

## Vereinfachung

$$\neg((\text{hatMilch} \vee \text{hatMilchE}) \vee (\text{hatFleisch} \vee \text{hatFleischE}))$$

gdw.  $\neg(\text{hatMilch} \vee \text{hatMilchE}) \wedge \neg(\text{hatFleisch} \vee \text{hatFleischE})$

gdw.  $\neg\text{hatMilch} \wedge \neg\text{hatMilchE} \wedge \neg\text{hatFleisch} \wedge \neg\text{hatFleischE}$

## Vereinfachung — weiteres Beispiel

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

gdw.  $A \wedge (B \vee C) \wedge A$

gdw.  $A \wedge A \wedge (B \vee C)$

gdw.  $A \wedge (B \vee C)$

Tautologien

## §1.13 Definition

Eine Formel ist

- eine **Tautologie**, falls sie immer wahr ist  
(unabh. von der Belegung der Atome)
- **unerfüllbar**, falls sie immer falsch ist  
(unabh. von der Belegung der Atome)
- **erfüllbar**, falls sie nicht unerfüllbar ist

## Beispiel

- $(A \wedge A) \leftrightarrow A$  ist eine **Tautologie** (Idem.  $\wedge$ )
- **Gerade**  $\leftrightarrow \neg$ **Ungerade** ist **erfüllbar**, aber keine **Tautologie**  
(auch wenn diese Aussage mit Fachwissen wahr ist)

# Aussagenlogik — Tautologien

klassische Tautologien	Bezeichnung
$A \vee \neg A$	ausgeschlossenes Drittes
$((A \vee B) \wedge (A \rightarrow C) \wedge (B \rightarrow C)) \rightarrow C$	Fallunterscheidung
$(A \wedge (A \rightarrow B)) \rightarrow B$	<i>modus ponens</i>
$((A \rightarrow B) \wedge (B \rightarrow C)) \rightarrow (A \rightarrow C)$	Syllogismus (Transitivität von $\rightarrow$ )
$(A \rightarrow B) \leftrightarrow (\neg B \rightarrow \neg A)$	Kontraposition
$((A \rightarrow B) \wedge (A \rightarrow \neg B)) \rightarrow \neg A$	<i>reductio ad absurdum</i> (indirekter Beweis)
$(A \wedge B) \rightarrow A$	Abschwächung für $\wedge$
$A \rightarrow (A \vee B)$	Abschwächung für $\vee$
$A \leftrightarrow B$	für äquivalente Aussagen $A$ und $B$

## §1.14 Theorem (modus ponens)

$F = (A \wedge (A \rightarrow B)) \rightarrow B$  ist eine Tautologie.

(gelten  $A$  und “wenn  $A$ , dann  $B$ ”, dann gilt auch  $B$ )

Beweis.

Mit Fallunterscheidung:

- falls  $B$  wahr ist, dann ist  $F = \dots \rightarrow B$  wahr
- falls  $B$  falsch ist, dann ist entweder
  - $A$  wahr, womit  $A \wedge (A \rightarrow B)$  falsch ist
  - $A$  falsch, womit  $A \wedge (A \rightarrow B)$  auch falsch ist

Da  $F' = A \wedge (A \rightarrow B)$  falsch ist, ist  $F = F' \rightarrow B$  wahr

□

## §1.15 Theorem

$((A \rightarrow B) \wedge (B \rightarrow C)) \rightarrow (A \rightarrow C)$  ist eine Tautologie.

(Transitivität von  $\rightarrow$ )

Beweis.

Kontraposition:  $F = \neg(A \rightarrow C) \rightarrow \underbrace{\neg((A \rightarrow B) \wedge (B \rightarrow C))}_{F'}$

Fallunterscheidung:

- Falls  $\neg(A \rightarrow C)$  falsch ist, dann ist  $F$  wahr.
- Falls  $\neg(A \rightarrow C)$  wahr ist, dann ist  $A \rightarrow C$  falsch, woraus  $A$  wahr und  $C$  falsch folgen
  - Sei  $B$  falsch. Dann ist  $A \rightarrow B$  falsch und damit  $F'$  wahr
  - Sei  $B$  wahr. Dann ist  $B \rightarrow C$  falsch und damit  $F'$  wahr

Da  $F'$  wahr ist, ist auch  $F$  wahr



## Notizen

- Schlussregeln sollten immer Tautologien sein  
z.B.  $(A \rightarrow B) \leftrightarrow (\neg B \rightarrow \neg A)$  — Kontraposition
- jede Tautologie ist erfüllbar
- Vorsicht mit der Negation:
  - ①  $\neg F$  ist unerfüllbar für jede Tautologie  $F$   
( $\neg F$  ist für jede Belegung falsch)
  - ②  $F$  kann erfüllbar sein, falls  $F$  **keine** Tautologie ist  
( $F$  ist nicht für jede Belegung wahr)



- Aussagenlogische Formeln und Interpretation
- Äquivalenz
- Tautologien und Erfüllbarkeit
- Grundlegende Beweistechniken

Erste Übungsserie wird demnächst im OLAT publiziert.

# Diskrete Strukturen

## Vorlesung 2: Logik & Naive Mengenlehre

Andreas Maletti

21. Oktober 2014

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## heutige Vorlesung

- ① Basiswissen Prädikatenlogik
- ② Einführung Mengen
- ③ Grundoperationen mit Mengen

Bitte Fragen direkt stellen!

Organisation

## Übungen

- Übungsgruppen (jede Woche):

Wochentag	Zeit	Raum	Übungsleiter
montags	11:15–12:45	SG 3-10	CLAUDIUS RÖHL
montags	15:15–16:45	SG 3-10	THOMAS WEIDNER
montags	15:15–16:45	SG 1-11	DOREEN HEUSEL
dienstags	11:15–12:45	SG 3-13	HANNES STRASS
dienstags	13:15–14:45	SG 3-13	CHRISTOPH GAMM
dienstags	15:15–16:45	SG 3-10	PETER LEUPOLD
mittwochs	13:15–14:45	SG 3-14	DOREEN HEUSEL
freitags	11:15–12:45	SG 3-14	CHRISTOPH GAMM

- keine Übung: 13.–17.10., 31.10., 19.11., 02.12.
  - bitte Alternativtermin in der gleichen Woche wählen

## Moduleinschreibung

- Einstriebeschluss: **26. Oktober 2014**
- wer im TOOL eingeschrieben ist, kann aufatmen
- wer noch nicht angemeldet ist, kann
  - sich im TOOL anmelden (es gibt mal wieder ein paar Plätze)
  - sich in die Anmeldeliste nach der VL eintragen
- Abmeldefrist: **25. Januar 2015**

Rückblick: Grundlagen der Logik

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## Wiederholung

- ¬ Negation nicht
- ∧ Konjunktion und
- ∨ Disjunktion oder
- Implikation wenn ..., dann ...
- ↔ Äquivalenz genau dann wenn

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

Theorem (§1.14 — modus ponens)

$F = (A \wedge (A \rightarrow B)) \rightarrow B$  ist eine Tautologie.

(gelten  $A$  und “wenn  $A$ , dann  $B$ ”, dann gilt auch  $B$ )

Beweis.

Mit Fallunterscheidung:

- falls  $B$  wahr ist, dann ist  $F = \dots \rightarrow B$  wahr
- falls  $B$  falsch ist, dann ist entweder
  - $A$  wahr, womit  $A \wedge (A \rightarrow B)$  falsch ist
  - $A$  falsch, womit  $A \wedge (A \rightarrow B)$  auch falsch ist

Da  $F' = A \wedge (A \rightarrow B)$  falsch ist, ist  $F = F' \rightarrow B$  wahr

□

## Theorem (§1.15)

$((A \rightarrow B) \wedge (B \rightarrow C)) \rightarrow (A \rightarrow C)$  ist eine Tautologie.

(Transitivität von  $\rightarrow$ )

Beweis.

Kontraposition:  $F = \neg(A \rightarrow C) \rightarrow \underbrace{\neg((A \rightarrow B) \wedge (B \rightarrow C))}_{F'}$

Fallunterscheidung:

- Falls  $\neg(A \rightarrow C)$  falsch ist, dann ist  $F$  wahr.
- Falls  $\neg(A \rightarrow C)$  wahr ist, dann ist  $A \rightarrow C$  falsch, woraus  $A$  wahr und  $C$  falsch folgen
  - Sei  $B$  falsch. Dann ist  $A \rightarrow B$  falsch und damit  $F'$  wahr
  - Sei  $B$  wahr. Dann ist  $B \rightarrow C$  falsch und damit  $F'$  wahr

Da  $F'$  wahr ist, ist auch  $F$  wahr



## §2.1 Theorem (indirekter Beweis)

$\underbrace{((A \rightarrow B) \wedge (A \rightarrow \neg B)) \rightarrow \neg A}_{F'} \text{ ist eine Tautologie.}$

in Worten: wenn man aus  $A$  einen Widerspruch ableiten kann, dann kann  $A$  nicht gelten

Beweis.

Wahrheitswertetabelle:

$A$	$B$	$A \rightarrow B$	$\neg B$	$A \rightarrow \neg B$	$F'$	$\neg A$	$F' \rightarrow \neg A$
0	0	1	1	1	1	1	1
0	1	1	0	1	1	1	1
1	0	0	1	1	0	0	1
1	1	1	0	0	0	0	1

Offensichtlich gilt sogar  $F' \leftrightarrow \neg A$



## §2.2 Theorem

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

Beweis (indirekt).

Sei  $x \in \mathbb{Q}$ , so dass  $x^2 = 2$ .

Negation der Aussage

Dann existieren teilerfremde  $m, n \in \mathbb{Z}$  mit  $n \neq 0$ , so dass  $x = \frac{m}{n}$ .

Also  $2n^2 = m^2$ , womit  $m^2$  gerade ist. Gemäß §1.12 (aus der letzten VL) ist somit auch  $m$  gerade, so dass  $m = 2k$  mit  $k \in \mathbb{Z}$ .

$$2n^2 = m^2 = (2k)^2 = 4k^2 \quad \Rightarrow \quad n^2 = 2k^2$$

Also ist auch  $n^2$  gerade und damit ist  $n$  gerade gemäß §1.12.

Da  $m$  und  $n$  gerade sind, sind sie nicht teilerfremd (gemeinsamer Teiler 2). Folglich gilt das Theorem. □

## Theorem (§2.2)

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

$$\neg A$$

## Beweisstruktur.

Es existieren teilerfremde  $m, n \in \mathbb{Z}$  mit  $n \neq 0$  und  $(\frac{m}{n})^2 = 2$

$$B$$

Wir zeigten zunächst  $A \rightarrow B$  und danach  $\neg B$

Damit gilt auch  $A \rightarrow \neg B$ , da  $\neg B$  wahr ist.

Wir haben also  $A \rightarrow B$  und  $A \rightarrow \neg B$  gezeigt. Folglich gilt  $\neg A$  gemäß §2.1. □

## Notizen

- äquivalent:  $(A \rightarrow (B \wedge \neg B)) \rightarrow \neg A$
- anstatt  $B \wedge \neg B$  kann jede unerfüllbare Aussage stehen
- indirekte Beweise sind nicht konstruktiv;  
sie zeigen nur Widerspruch auf
- lieber *direkt* als *indirekt* beweisen

Prädikatenlogik

## Theorem (§1.12)

Sei  $n \in \mathbb{Z}$  beliebig. Falls  $n^2$  gerade ist, so ist auch  $n$  gerade.

## Probleme

- dies ist natürlich eine Aussage,  
aber deren interne Struktur können wir nicht modellieren
- die Abhängigkeit von  $n$  können wir nicht modellieren  
QuadratGerade = “ $n^2$  gerade” und ZahlGerade = “ $n$  gerade”  
für eine Konstante  $n$   
→ Aussagenschablonen
- auch die beliebige Wahl von  $n$  können wir nicht modellieren  
→ Quantoren

## Intuition

- eine **Aussagenschablone** ist ein Satz, der Variablen verwendet, so dass für jede Belegung der Variablen eine Aussage entsteht
- **Quantoren** verlangen Wahrheit der Aussagen, die man durch best. Instanziierungen einer Aussagenschablone erhält

## Formalisierung von §1.12

Sei  $n \in \mathbb{Z}$  beliebig. Falls  $n^2$  gerade ist, so ist auch  $n$  gerade.

$$(\forall n \in \mathbb{Z}). (\text{QuadratGerade}(n) \rightarrow \text{ZahlGerade}(n))$$

## §2.3 Begriffe

- **Variablen** (üblicherweise kleingeschrieben)  
können als Parameter von Prädikaten auftreten
- **Prädikat** — Aussagenschablone  
bildet zusammen mit Variablen als Parameter ein Atom

## Beispiele

- **Atom:** ZahlGerade( $n$ ) Wahrheit hängt nun von  $n$  ab  
  - **Prädikat:** ZahlGerade
  - **Variable:**  $n$ZahlGerade(2) ist wahr  
ZahlGerade(3) ist falsch
- **Atom:** Summe( $x, y, z$ )  
  - **Prädikat:** Summe
  - **Variablen:**  $x, y, z$Summe( $x, y, z$ ) wahr  
gdw.  $x + y = z$

## Notizen

- die bekannten Junktoren können weiterhin verwendet werden  
(auch zur Verknüpfung von Aussagenschablonen)
  - die Wahrheit einer Aussagenschablone lässt sich erst bei Kenntnis der Belegung der Variablen bestimmen
- Mechanismus für Umwandlung Aussagenschablone in Aussage

## §2.4 Quantoren

Sei  $F$  eine prädikatenlogische Formel.

- $(\forall x \in X).F$  ist eine Formel, die wahr ist, gdw.  $F$  für alle  $x \in X$  wahr ist  $\forall A =$  für Alle Allquantor
  - $(\exists x \in X).F$  ist eine Formel, die wahr ist, gdw.  $x \in X$  existiert, so dass  $F$  für dieses  $x$  wahr ist  $\exists E =$  Existiert ein Existenzquantor

Durch Quantifizierung aller Variablen erhält man eine Aussage.

## Beispiel (§2.2)

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

Formalisierung:  $\neg(\exists x \in \mathbb{Q}).(x^2 = 2)$

## weitere Beispiele

- Jede ganze Zahl ist größer 0.

falsch

$$(\forall n \in \mathbb{Z}).\text{Größer0}(n) \quad (\forall n \in \mathbb{Z}).(n > 0)$$

- Jede gerade natürliche Zahl  $n > 2$  ist die Summe zweier Primzahlen.

unbekannt

$$(\forall n \in \mathbb{N}). \left( ((n > 2) \wedge \text{ZahlGerade}(n)) \rightarrow (\exists i, j \in \mathbb{N}). (\text{Prim}(i) \wedge \text{Prim}(j) \wedge (i + j = n)) \right)$$

## komplexe Beispiele

- CAUCHY-Konvergenz einer Folge  $(x_i)_{i \in \mathbb{N}}$

$$(\forall \epsilon \in \mathbb{R}_{>0}).(\exists n \in \mathbb{N}).(\forall i \in \mathbb{N}).(\forall j \in \mathbb{N}).$$
$$((i \geq n) \wedge (j \geq n)) \rightarrow (|x_j - x_i| < \epsilon)$$

- Grenzwert  $\lim_{i \rightarrow n} f(i)$  einer Funktion  $f: \mathbb{R} \rightarrow \mathbb{R}$  ist  $\ell$  gdw.

$$(\forall \epsilon \in \mathbb{R}_{>0}).(\exists \delta \in \mathbb{R}_{>0}).(\forall i \in \mathbb{R}).$$
$$(0 < |i - n| < \delta) \rightarrow (|f(i) - \ell| < \epsilon)$$

AUGUSTIN-LOUIS CAUCHY (\* 1789; † 1857)

- franz. Mathematiker
- Pionier der Analysis
- Verfechter des formalen Beweises



weitere äquivalente Formeln	Bezeichnung
$\neg(\forall x \in X).F$	( $\exists x \in X$ ). $\neg F$ Negation Allquantor
$\neg(\exists x \in X).F$	( $\forall x \in X$ ). $\neg F$ Negation Existenzquantor

→ siehe Übung

Grundbegriff: Menge

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## §2.5 Definition (Menge — nach [CANTOR, 1895])

Eine **Menge** ist eine Zusammenfassung von unterscheidbaren Objekten zu einem Ganzen. Die zusammengefassten Objekte heißen **Elemente** von  $M$ .

## Original [CANTOR, 1895]

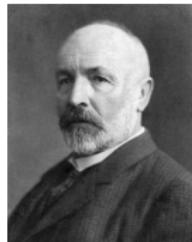
Unter einer **Menge** verstehen wir jede Zusammenfassung  $M$  von bestimmten wohlunterschiedenen Objekten  $m$  unsrer Anschauung oder unseres Denkens (welche **Elemente** von  $M$  genannt werden) zu einem Ganzen.

## Notiz

verbale Definition → naive Mengenlehre

## GEORG CANTOR (\* 1845; † 1918)

- dtsch. Mathematiker
- Begründer der modernen Mengenlehre
- Kardinal- und Ordinalzahlen



### § 1.

#### Der Mächtigkeitsbegriff oder die Cardinalzahl.

Unter einer ‚Menge‘ verstehen wir jede Zusammenfassung  $M$  von bestimmten wohlunterschiedenen Objecten  $m$  unsrer Anschauung oder unseres Denkens (welche die ‚Elemente‘ von  $M$  genannt werden) zu einem Ganzen.

## §2.6 Definition (Menge)

- Menge als Zusammenfassung von bestimmten Objekten (ihren Elementen)
- für jede Menge  $M$  und jedes Objekt  $m$  ist  $m$  entweder
  - ein Element von  $M$   $m \in M$
  - oder nicht  $\neg(m \in M)$  oder besser:  $m \notin M$
- “entweder ... oder ...” entspricht **exklusivem Oder**

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

- jede Menge ist unterscheidbar von jedem ihrer Elemente  $\{3\} \neq 3$

## Beispiele

- Menge aller Lastkraftwagen

Definition mit Eigenschaft

- Menge aller Lastkraftwagen,  
die (jetzt) frischen Fisch transportieren

Einschränkung einer anderen Menge

- Menge mit den Elementen 1, 2 und 3

(vollständige) Aufzählung

- Menge mit den Elementen 0, 1, 2, usw.

(unvollständige) Aufzählung

## §2.7 Notation zur Definition von Mengen

- **Leere Menge:**  $\emptyset$  hat keine Elemente
- **Basismengen:** sei Lkw die Menge aller Lastkraftwagen  
textuelle Definition
- **Einschränkung:**  $\{L \in \text{Lkw} \mid \text{hatFisch}(L)\}$   
enthält genau die Elemente  $L$  von Lkw,  
für die  $\text{hatFisch}(L)$  wahr ist  
$$M = \{x \in X \mid F\}$$
 mit Aussagenschablone  $F$
- **vollständige Aufzählung:**  $\{1, 2, 3\}$   
funktioniert nur bei endlichen Mengen
- **unvollständige Aufzählung:**  $\{0, 1, 2, \dots\}$   
Muster muss klar erkennbar sein

## Notizen

- Elemente unterscheidbar (Mehrfachnennungen unnütz)

$$\{1, 2, 3, 1\} = \{1, 2, 3\} \quad \text{und} \quad \left\{0,5\right\} = \left\{\frac{1}{2}, \frac{2}{4}, 2 \cdot \frac{6}{24}\right\}$$

- nur Gruppierung; keine Anordnung (Reihenfolge irrelevant)

$$\{3, 2, 1\} = \{1, 2, 3\}$$

- dies gilt allg. für Mengen, nicht nur für Aufzählungen
- **Klassiker:** bei  $x, y, z \in \{1, 2, 3\}$   
formal:  $(x \in \{1, 2, 3\}) \wedge (y \in \{1, 2, 3\}) \wedge (z \in \{1, 2, 3\})$   
kann  $x = y = z$  gelten

## §2.8 Definition (Gleichheit)

Mengen  $M$  und  $N$  sind **gleich** (kurz:  $M = N$ ),  
wenn sie (exakt) die gleichen Elemente haben

**Formal:**  $M = N$  gdw.  $(\forall m \in M).(m \in N) \wedge (\forall n \in N).(n \in M)$

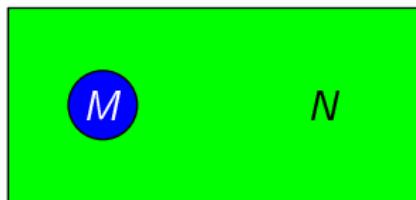
## Beispiel

- $M_2 = \{n \in \mathbb{N} \mid n \text{ ist durch 2 teilbar}\}$  nat. Zahlen mit Teiler 2
- $G = \{n \in \mathbb{N} \mid \text{ZahlGerade}(n)\}$  gerade nat. Zahlen
- es gilt  $M_2 = G$

## §2.9 Definition (Teilmenge)

Menge  $M$  ist eine **Teilmenge** von der Menge  $N$  (kurz:  $M \subseteq N$ ), falls jedes Element von  $M$  auch Element von  $N$  ist

**Formal:**  $M \subseteq N$  gdw.  $(\forall m \in M).(m \in N)$



## Beispiel

- $M_4 = \{n \in \mathbb{N} \mid n \text{ ist durch } 4 \text{ teilbar}\}$  nat. Zahlen mit Teiler 4
- $G = \{n \in \mathbb{N} \mid \text{ZahlGerade}(n)\}$  gerade nat. Zahlen
- es gilt  $M_4 \subseteq G$

## Notizen

- Alternativen zu  $M \subseteq N$  ( $M$  ist Teilmenge von  $N$ ):
  - $N \supseteq M$  ( $N$  ist Obermenge von  $M$ )
  - manchmal auch:  $M \subset N$  (werden wir nicht verwenden)
- Was bedeutet:  $M \not\subseteq N$ ?

$$M \not\subseteq N$$

$$\text{gdw. } \neg(M \subseteq N)$$

$$\text{gdw. } \neg(\forall m \in M).(m \in N)$$

$$\text{gdw. } (\exists m \in M).\neg(m \in N)$$

$$\text{gdw. } (\exists m \in M).(m \notin N)$$

in Worten:  $M \not\subseteq N$  gdw. es ein Element  $m$  von  $M$  gibt, welches kein Element von  $N$  ist

## Fragen

Welche Aussagen gelten für  $M = \{\emptyset, \{\emptyset\}\}$ ?

- $\emptyset \in M$  ✓
- $\{\emptyset\} \in M$  ✓
- $\{\{\emptyset\}\} \in M$  ✗
- $\emptyset \subseteq M$  ✓
- $\{\emptyset\} \subseteq M$  ✓
- $\{\{\emptyset\}\} \subseteq M$  ✓

## §2.10 Theorem

Für alle Mengen  $M$  und  $N$  gilt:  $M = N$  gdw.  $M \subseteq N$  und  $N \subseteq M$ .

Beweis.

Direkt durch Einsetzen der Definitionen:

$$M = N$$

$$\text{gdw. } (\forall m \in M).(m \in N) \wedge (\forall n \in N).(n \in M) \quad \S 2.8$$

$$\text{gdw. } (M \subseteq N) \wedge (\forall n \in N).(n \in M) \quad \S 2.9$$

$$\text{gdw. } (M \subseteq N) \wedge (N \subseteq M) \quad \S 2.9$$



## Beispiele

- $\emptyset = \{\}$  leere Menge  
(hat keine Elemente)
- $\mathbb{N} = \{0, 1, 2, \dots\}$  natürlichen Zahlen  
(manchmal auch ohne 0)
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$  ganzen Zahlen
- $\mathbb{Q} = \left\{ \frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{Z}, n \neq 0 \right\}$  rationalen Zahlen  
(‘,’ heißt “und” in Eigenschaften)
- $\mathbb{R} = \text{Menge aller reellen Zahlen}$  reellen Zahlen

## Operationen auf Mengen

## §2.11 Definition (Vereinigung, Schnitt, Differenz)

Seien  $M$  und  $N$  Mengen.

- **Vereinigung**  $M \cup N$  von  $M$  und  $N$  besteht aus den Elementen, die Element von  $M$  oder Element von  $N$  sind

$$M \cup N = \{x \mid x \in M \text{ oder } x \in N\}$$

- **Schnitt**  $M \cap N$  von  $M$  und  $N$  besteht aus den Elementen, die Element von  $M$  und Element von  $N$  sind

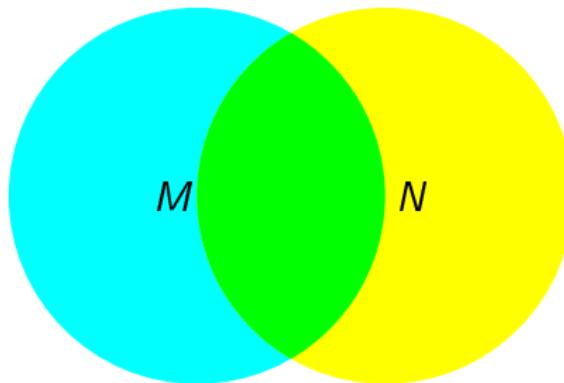
$$M \cap N = \{x \mid x \in M, x \in N\} = \{x \in M \mid x \in N\}$$

- **Differenz**  $M \setminus N$  von  $M$  ohne  $N$  besteht aus den Elementen, die Element von  $M$  aber nicht Element von  $N$  sind

$$M \setminus N = \{x \mid x \in M, x \notin N\} = \{x \in M \mid x \notin N\}$$

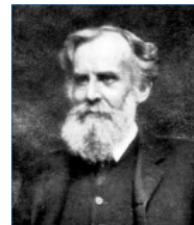
## Grafische Darstellung

- VENN-Diagramme
- Vereinigung  $M \cup N$ , Schnitt  $M \cap N$ , Differenz  $M \setminus N$



JOHN VENN (\* 1834; † 1923)

- engl. Mathematiker
- Lehrer der Logik in Cambridge



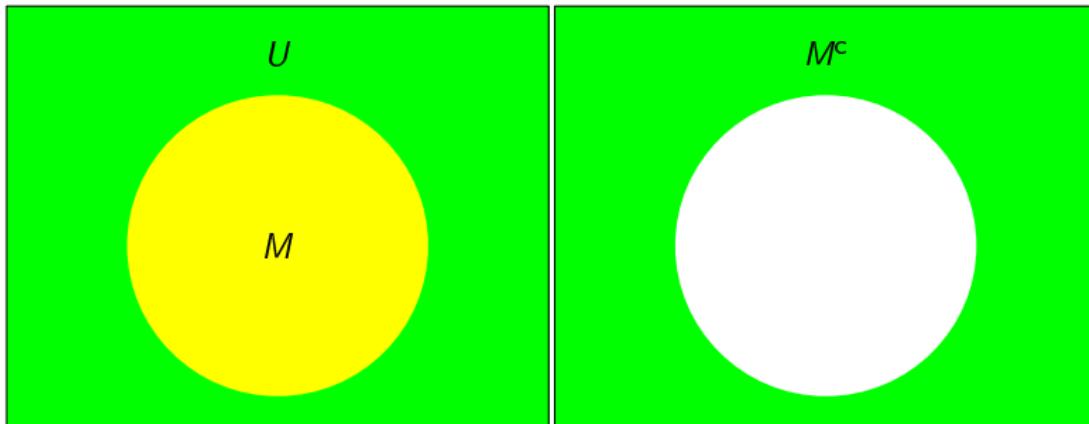
Grundmenge  $U$

(häufig implizit)

## §2.12 Definition (Komplement)

Das **Komplement**  $M^c$  von  $M \subseteq U$  beinhaltet genau die Elemente von  $U$ , die nicht Elemente von  $M$  sind.

$$M^c = \{u \in U \mid u \notin M\} = U \setminus M$$



## §2.13 Theorem

①  $x \in \{y \mid F(y)\}$  gdw.  $F(x)$

②  $x \notin M$  gdw.  $x \in M^c$

Grundmenge  $U$  und  $x \in U$

### Beweis.

#### ① Beidseitige Implikationen

( $\leftarrow$ ) Falls  $F(x)$  gilt, dann auch  $x \in \{y \mid F(y)\}$ .

( $\rightarrow$ ) Falls  $F(x)$  nicht gilt, dann gilt auch  $x \notin \{y \mid F(y)\}$ . Per Kontraposition gilt daher  $F(x)$ , falls  $x \in \{y \mid F(y)\}$ .

#### ② Beiseitige Implikationen

( $\leftarrow$ ) Sei  $x \in M^c = U \setminus M = \{y \mid y \in U, y \notin M\}$ . Nach ① gilt daher  $x \in U$  und  $x \notin M$ .

( $\rightarrow$ ) Sei  $x \in U$  und  $x \notin M$ . Dann gilt nach ① auch  $x \in \{y \mid y \in U, y \notin M\} = U \setminus M = M^c$ .



# Mengenlehre — Rechenregeln

gleiche Mengen		Bezeichnung
$A \cap B$	$B \cap A$	Kommutativität von $\cap$
$A \cup B$	$B \cup A$	Kommutativität von $\cup$
$(A \cap B) \cap C$	$A \cap (B \cap C)$	Assoziativität von $\cap$
$(A \cup B) \cup C$	$A \cup (B \cup C)$	Assoziativität von $\cup$
$A \cap (B \cup C)$	$(A \cap B) \cup (A \cap C)$	Distributivität von $\cap$
$A \cup (B \cap C)$	$(A \cup B) \cap (A \cup C)$	Distributivität von $\cup$
$A \cap A$	$A$	Idempotenz von $\cap$
$A \cup A$	$A$	Idempotenz von $\cup$
$(A^c)^c$	$A$	Involution $\cdot^c$
$(A \cap B)^c$	$A^c \cup B^c$	DEMORGAN-Gesetz für $\cap$
$(A \cup B)^c$	$A^c \cap B^c$	DEMORGAN-Gesetz für $\cup$

## §2.13 Theorem

Für alle Mengen  $M, N, P$  gilt

$$M \cup (N \cap P) = (M \cup N) \cap (M \cup P)$$

Beweis.

Direkt durch Anwendung der Definitionen:

$$\begin{aligned} M \cup (N \cap P) &= \{x \mid (x \in M) \vee (x \in N \cap P)\} \\ &= \{x \mid (x \in M) \vee (x \in \{y \mid (y \in N) \wedge (y \in P)\})\} \\ &= \{x \mid (\underbrace{x \in M}_A) \vee (\underbrace{(x \in N)}_B \wedge \underbrace{(x \in P)}_C)\} \quad \text{§2.13} \\ &= \{x \mid (\underbrace{(x \in M)}_A \vee \underbrace{(x \in N)}_B) \wedge (\underbrace{(x \in M)}_A \vee \underbrace{(x \in P)}_C)\} \\ &= \{x \mid (x \in M \cup N) \wedge (x \in M \cup P)\} \\ &= (M \cup N) \cap (M \cup P) \end{aligned}$$

□

- Grundwissen Prädikatenlogik
- Grundbegriffe Mengenlehre
- Definition von Mengen
- Beziehungen zwischen Mengen (Gleichheit, Teilmengen)
- Operationen und Rechenregeln für Mengen

Zweite Übungsserie ist bereits im OLAT.

# Diskrete Strukturen

## Vorlesung 3: Naive Mengenlehre & Relationen

Andreas Maletti

28. Oktober 2014

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## heutige Vorlesung

- ① Verallgemeinerung Vereinigung und Schnitt
- ② Potenzmenge
- ③ Vollständige Induktion
- ④ Relationen und deren Eigenschaften

Bitte Fragen direkt stellen!

Notation

## notationelle Varianten

- sind natürlich akzeptabel
- es muss aber eindeutig verständlich bleiben

## Beispiele

- $(\forall x \in X).(\exists y \in Y).(x \leq y)$
- $\forall x \exists y : (x \in X \wedge y \in Y) \rightarrow (x \leq y)$
- $(\forall x \in X)(\exists y \in Y) : (x \leq y)$
- ...

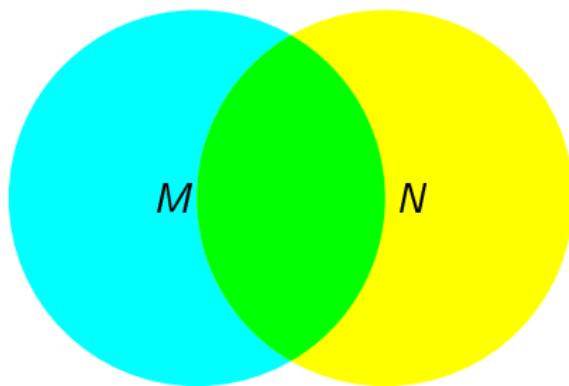
Rückblick: Mengen und Operationen

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

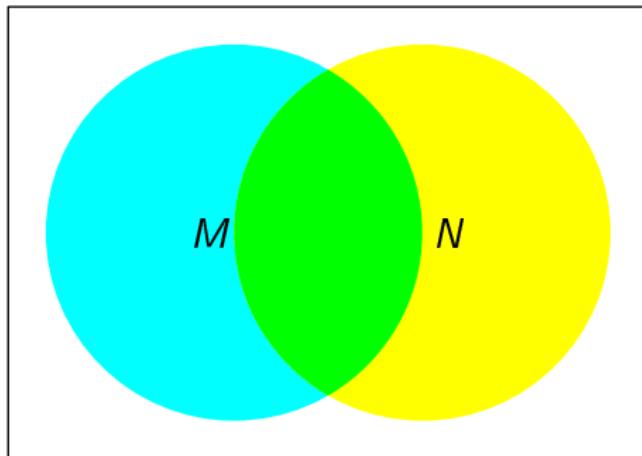
## Notation

- $x \in X$  heißt “ $x$  ist Element der Menge  $X$ ” Negation:  $x \notin X$
- **Teilmenge**  $M \subseteq N$  gdw.  $(\forall x \in M).(x \in N)$
- **Mengeneinschränkung**  $\{x \in X \mid F\}$
- Vereinigung  $M \cup N$ , Schnitt  $M \cap N$ , Differenz  $M \setminus N$



## Vorsicht

- Differenz ‘\’ entspricht **nicht** der logischen Implikation ‘ $\rightarrow$ ’
- $A \rightarrow B$  gdw.  $\neg A \vee B$
- wir betrachten also  $M^c \cup N$



## §3.1 Theorem

Seien  $M$ ,  $N$  und  $U$  Mengen, so dass  $M \subseteq U$  und  $N \subseteq U$ . Dann gilt:  
(gemeinsame Grundmenge  $U$  — Universum)

$$M \setminus N = (M^c \cup N)^c$$

### Beweis.

Wir wissen bereits:  $(M^c \cup N)^c = (M^c)^c \cap N^c = M \cap N^c$ . Es bleibt zu zeigen (z.zg.):  $M \setminus N = M \cap N^c$ .

$$\begin{aligned}M \setminus N &= \{x \mid (x \in M) \wedge (x \notin N)\} \\&= \{x \mid (x \in M) \wedge (x \in N^c)\} \\&= M \cap N^c\end{aligned}$$

□

Universum  $U$

weitere Eigenschaften	Bezeichnung
$A \cup A^c = U$	ausgeschlossenes Drittes
$((A \subseteq B) \wedge (B \subseteq C)) \rightarrow (A \subseteq C)$	Syllogismus (Transitivität von $\subseteq$ )
$(A \subseteq B)$ gdw. $(B^c \subseteq A^c)$	Kontraposition
$(A \cap B) \subseteq A$	Abschwächung für $\cap$
$A \subseteq (A \cup B)$	Abschwächung für $\cup$

## Notizen

- Jede Tautologie liefert die Universalmenge  $U$  beim Umschreiben von  $\wedge$ ,  $\vee$ ,  $\neg$  (nutze  $A \rightarrow B$  gdw.  $\neg A \vee B$ )
  - Tautologie:  $(A \wedge (A \rightarrow B)) \rightarrow B$  gdw.  $\neg(A \wedge (\neg A \vee B)) \vee B$
  - für Mengen:

$$\begin{aligned}(A \cap (A^c \cup B))^c \cup B &= A^c \cup (A^c \cup B)^c \cup B \\ &= A^c \cup (A \cap B^c) \cup B \\ &= ((A^c \cup A) \cap (A^c \cup B^c)) \cup B \\ &= (U \cap (A^c \cup B^c)) \cup B \\ &= A^c \cup B^c \cup B \\ &= U\end{aligned}$$

- Jede unerfüllbare Formel liefert die leere Menge  $\emptyset$

## §3.2 Theorem (Monotonie)

Seien  $M \subseteq M'$  und  $N \subseteq N'$ . Dann gelten

$$(M \cap N) \subseteq (M' \cap N') \quad \text{und} \quad (M \cup N) \subseteq (M' \cup N')$$

Beweis.

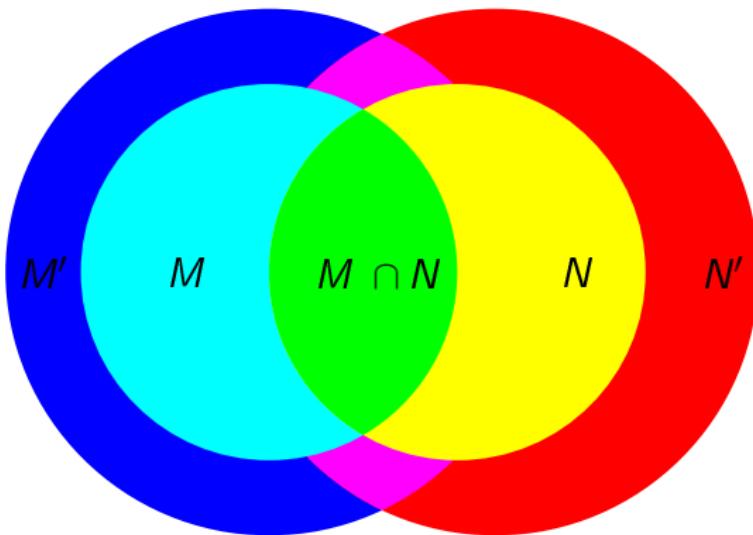
- zu  $(M \cap N) \subseteq (M' \cap N')$ :

Sei  $x \in (M \cap N)$ . Dann  $x \in M$  und  $x \in N$ . Da  $M \subseteq M'$  und  $N \subseteq N'$  folgen  $x \in M'$  und  $x \in N'$ . Folglich  $x \in (M' \cap N')$ .

- zu  $(M \cup N) \subseteq (M' \cup N')$ :

Sei  $x \in (M \cup N)$ . Dann  $x \in M$  oder  $x \in N$ . Da  $M \subseteq M'$  und  $N \subseteq N'$  folgt  $x \in M'$  oder  $x \in N'$ . Folglich  $x \in (M' \cup N')$ .  $\square$

# Mengenlehre — weitere Eigenschaften



## §3.3 Theorem

Für alle Mengen  $M$  und  $N$  sind folgende Aussagen äquivalent:

- ①  $M \subseteq N$
- ②  $M \cap N = M$
- ③  $M \cup N = N$

Beweis.

Durch Äquivalenz zu ①: ①  $\leftrightarrow$  ② und ①  $\leftrightarrow$  ③

- zu ①  $\rightarrow$  ② und ①  $\rightarrow$  ③: Da  $M \subseteq N$  folgt durch Monotonie

$$M = M \cap M \subseteq M \cap N \quad \text{und} \quad M \cup N \subseteq N \cup N = N \quad (\S 3.2)$$

Trivialerweise  $M \cap N \subseteq M$  und  $N \subseteq M \cup N$ .

- zu ②  $\rightarrow$  ① und ③  $\rightarrow$  ①:

$$M = M \cap N \subseteq N \quad \text{und} \quad M \subseteq M \cup N = N$$

□

Verallgemeinerung: Vereinigung und Schnitt

## Bemerkungen

- Vereinigung und Schnitt bisher nur zweistellig  
(zwei Argumente)  
→ Verallgemeinerung für beliebig viele Argumente

## §3.4 Definition

Sei  $I$  eine Menge und  $M_i$  eine Menge für jedes  $i \in I$

- $\bigcup_{i \in I} M_i = \{x \mid \text{es existiert } i \in I, \text{ so dass } x \in M_i\}$   
 $= \{x \mid (\exists i \in I). (x \in M_i)\}$
- $\bigcap_{i \in I} M_i = \{x \mid \text{für alle } i \in I \text{ gilt } x \in M_i\}$   
 $= \{x \mid (\forall i \in I). (x \in M_i)\}$

## Beispiele

- für jede Menge  $M$  gilt:  $M = \bigcup_{m \in M} \{m\}$
- **geschlossenes Intervall**  $[u, o]$  für  $u, o \in \mathbb{R}$  mit  $u \leq o$

$$[u, o] = \{r \in \mathbb{R} \mid u \leq r \leq o\}$$

- es gilt  $\mathbb{R} = \bigcup_{n \in \mathbb{N}} [-n, n] = \bigcup_{r \in \mathbb{R}_{\geq 0}} [-r, r]$

## Beweis.

Durch Ringinklusion:  $\mathbb{R} \subseteq \bigcup_{n \in \mathbb{N}} [-n, n] \subseteq \bigcup_{r \in \mathbb{R}_{\geq 0}} [-r, r] \subseteq \mathbb{R}$

- zu  $\mathbb{R} \subseteq \bigcup_{n \in \mathbb{N}} [-n, n]$ : Sei  $r \in \mathbb{R}$  und  $n = \lceil |r| \rceil$  (aufrunden; i.e.,  $|r| \leq n$ ). Dann gilt  $-n \leq r \leq n$  und damit  $r \in [-n, n]$ . Also auch  $r \in \bigcup_{n \in \mathbb{N}} [-n, n]$ .
- zu  $\bigcup_{n \in \mathbb{N}} [-n, n] \subseteq \bigcup_{r \in \mathbb{R}_{\geq 0}} [-r, r]$ : trivial, da  $\mathbb{N} \subseteq \mathbb{R}_{\geq 0}$
- zu  $\bigcup_{r \in \mathbb{R}_{\geq 0}} [-r, r] \subseteq \mathbb{R}$ :  $[-r, r] \subseteq \mathbb{R}$  für alle  $r \in \mathbb{R}_{\geq 0}$

□

## Beispiel

- Sei  $r \in \mathbb{R}_{\geq 0}$  eine reelle Zahl. Dann ist

$$\bigcap_{\substack{x \in \mathbb{R}_{\geq 0} \\ r \in [-x, x]}} [-x, x] = [-r, r]$$

- Beweis in der Übung

## §3.5 Notationsvarianten

- $\bigcup_{i=u}^o M_i = \bigcup_{i \in I} M_i$  und  $\bigcap_{i=u}^o M_i = \bigcap_{i \in I} M_i$   
für  $I = \{u, u+1, \dots, o\} \subseteq \mathbb{N}$  (bekannt von  $\sum$  und  $\prod$ )
- $\bigcup \{M_i \mid i \in I\} = \bigcup_{i \in I} M_i$  und  $\bigcap \{M_i \mid i \in I\} = \bigcap_{i \in I} M_i$

## Sonderfälle

- $\bigcup_{i \in \emptyset} M_i = \emptyset$
- $\bigcap_{i \in \emptyset} M_i = U$  für Universum  $U$  (oder undefiniert)

## Beispiele

- $\bigcup \{\{1, 3, 5\}, \{1, 2, 3\}, \{2, 3, 5\}\} = \{1, 2, 3, 5\}$
- $\bigcap \{\{1, 3, 5\}, \{1, 2, 3\}, \{2, 3, 5\}\} = \{3\}$

gleiche Mengen	Bezeichnung
$M \cap (\bigcup_{i \in I} M_i)$	Distributivitt von $\cap$
$M \cup (\bigcap_{i \in I} M_i)$	Distributivitt von $\cup$
$\bigcap_{i \in I} A$	Idempotenz von $\bigcap$ ; $I \neq \emptyset$
$\bigcup_{i \in I} A$	Idempotenz von $\bigcup$ ; $I \neq \emptyset$
$(\bigcap_{i \in I} M_i)^c$	DEMORGAN-Gesetz fr $\bigcap$
$(\bigcup_{i \in I} M_i)^c$	DEMORGAN-Gesetz fr $\bigcup$

Potenzmenge

## §3.6 Definition (Potenzmenge)

Sei  $M$  eine Menge. Dann ist die **Potenzmenge**  $\mathcal{P}(M)$  die Menge

$$\mathcal{P}(M) = \{N \mid N \subseteq M\}$$

aller Teilmengen von  $M$

### Beispiele

- $\mathcal{P}(\emptyset) = \{\emptyset\}$
- $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$
- $\mathcal{P}(\{1, 2, 3\})$  ist die Menge

$$\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

## §3.7 Definition (naive Kardinalität)

Eine Menge  $M$  ist **endlich**, falls sie endlich viele Elemente hat.

- Falls  $M$  endlich ist, dann ist  $|M|$  die Anzahl ihrer Elemente
- Falls  $M$  unendlich (nicht endlich) ist,  
dann schreiben wir  $|M| \geq \infty$  (zunächst)

## §3.8 Theorem (Erklärung “Potenzmenge”)

Sei  $M$  eine endliche Menge. Dann gilt  $|\mathcal{P}(M)| = 2^{|M|}$ .

Beweis.

... wir brauchen zunächst noch eine neue Beweistechnik ...

Vollständige Induktion

## §3.9 Theorem (Prinzip der vollständigen Induktion)

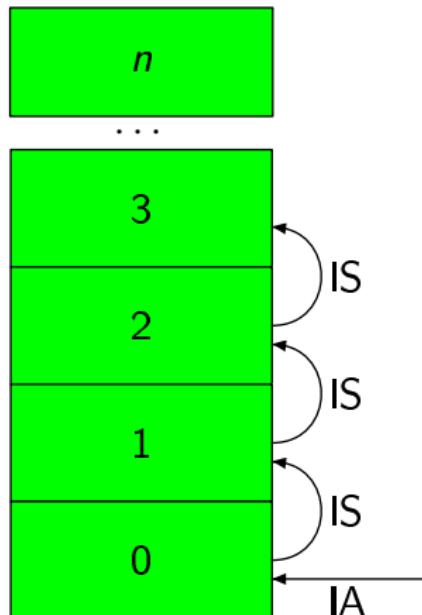
Sei  $F(x)$  eine Aussagenschablone mit einer Variable  $x$ . Gelten

- **Induktionsanfang (IA):**  $F(0)$  und
- **Induktionsschritt (IS):**  $F(n) \rightarrow F(n+1)$  für alle  $n \in \mathbb{N}$ ,  
 $(\forall n \in \mathbb{N}).(F(n) \rightarrow F(n+1))$

dann gilt  $F(x)$  für alle  $x \in \mathbb{N}$ .  $(\forall x \in \mathbb{N}).F(x)$

## Notizen

- $F(0)$  gilt offensichtlich gem. Induktionsanfang IA
- daraus folgt gem. Induktionsschritt dann  $F(1)$  IS
- woraus gem. Induktionsschritt  $F(2)$  folgt, etc. IS
- im Induktionsschritt (IS) heißen:
  - $F(n)$  die **Induktionshypothese (IH)** oder -voraussetzung
  - $F(n+1)$  die **Induktionsbehauptung (IB)**



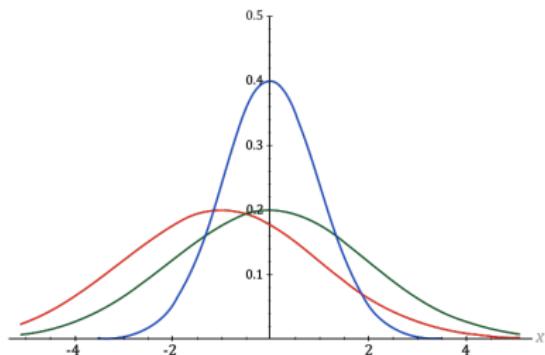
## Beispiel (Summenformel von GAUSS)

- Aussage:  $\sum_{i=1}^n i = \frac{n(n+1)}{2}$  für alle  $n \in \mathbb{N}$
- Induktionsanfang:  $\sum_{i=1}^0 i = 0 = \frac{0 \cdot 1}{2}$
- Induktionshypothese:  $\sum_{i=1}^n i = \frac{n(n+1)}{2}$
- Induktionsbehauptung: zu zeigen:  $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$

$$\begin{aligned}\sum_{i=1}^{n+1} i &= \sum_{i=1}^n i + (n+1) \\&= \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \quad (\text{IH}) \\&= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}\end{aligned}$$

CARL FRIEDRICH GAUSS (\* 1777; † 1855)

- dtsch. Mathematiker, Astronom und Physiker
- Integralsätze & Glockenkurve
- Formel zur Berechnung von Ostern



## Theorem (§3.8)

Sei  $M$  eine endliche Menge. Dann gilt  $|\mathcal{P}(M)| = 2^{|M|}$ .

Beweis (genauer in Übung).

per vollständiger Induktion über  $|M|$ :

**IA:** Die einzige Menge  $M$  mit  $|M| = 0$  ist  $M = \emptyset$ . Zusätzlich  $\mathcal{P}(\emptyset) = \{\emptyset\}$ , also gilt  $|\mathcal{P}(\emptyset)| = |\{\emptyset\}| = 1 = 2^0 = 2^{|\emptyset|}$ .

**IS:** Sei  $M$  eine Menge, so dass  $|M| = n + 1$  für ein  $n \in \mathbb{N}$ . Wähle  $x \in M$  beliebig. Dann ist

$$\mathcal{P}(M) = \mathcal{P}(M \setminus \{x\}) \cup \{N \cup \{x\} \mid N \in \mathcal{P}(M \setminus \{x\})\}$$

Unter Beachtung der Disjunktheit (nächste Folie) gilt

$$|\mathcal{P}(M)| = 2 \cdot |\mathcal{P}(M \setminus \{x\})| = 2 \cdot 2^{|M|-1} = 2^{|M|},$$

wobei  $|\mathcal{P}(M \setminus \{x\})| = 2^{|M|-1}$  per Induktionshypothese



## §3.10 Definition

Zwei Mengen  $M$  und  $N$  sind **disjunkt** gdw.  $M \cap N = \emptyset$

### Beispiele

- $\{1, 2, 3\}$  und  $\{2, 4, 6\}$  sind **nicht** disjunkt
- $\{1, 2, 3\}$  und  $\{4, 5, 6\}$  sind disjunkt

## §3.11 Theorem (Beweis in der Übung)

Für alle endlichen Mengen  $M$  und  $N$  gilt

$$\max(|M|, |N|) \leq |M \cup N| \stackrel{(\ddagger)}{\leq} |M| + |N| ,$$

mit Gleichheit bei  $(\ddagger)$  gdw.  $M$  und  $N$  disjunkt sind.

## Frage

Formulieren Sie das entsprechende Resultat für den Schnitt!

$$\dots \leq |M \cap N| \leq \dots$$

$$0 \leq |M \cap N| \leq \min(|M|, |N|)$$

Begriff: Relation

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## FACEBOOK-Freunde

- Wer hat mehr als 1.000 FACEBOOK-Freunde?
- Wer hat zwischen 100 und 1.000 FACEBOOK-Freunde?
- Wer hat zwischen 0 und 100 FACEBOOK-Freunde?
- Wer nutzt FACEBOOK gar nicht?

## Repräsentation

Wie kann man die Freundschaften erfassen?

- speichere zu jedem Mitglied seine Freunde → **sehr ineffizient**
- speichere als Mengen von Beziehungen

## §3.12 Definition (Mengenprodukt)

Für alle Mengen  $M$  und  $N$  ist das (kartesische) **Produkt**  $M \times N$  definiert durch

$$M \times N = \{(m, n) \mid m \in M, n \in N\} ,$$

die Menge aller Paare von Elementen aus  $M$  und  $N$ .

## Notizen

- $\{m, n\}$  heißt Menge mit Elementen  $m$  und  $n$
- $(m, n)$  heißt (**geordnetes**) **Paar** oder **Sequenz**
- Reihenfolge relevant;  $(m, n) \neq (n, m)$ , falls  $m \neq n$

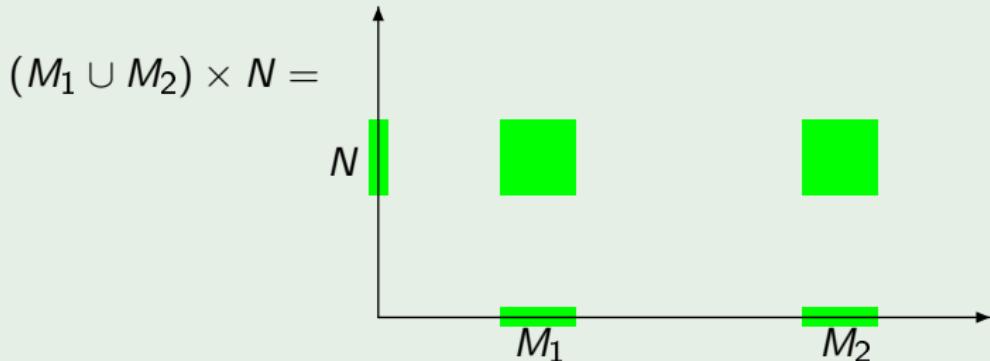
# Relationen — Mengenprodukt

## Beispiele

- sei  $M = \{1, 2, 3\}$  und  $N = \{1, 3\}$

$$M \times N = \{(1, 1), (1, 3), (2, 1), (2, 3), (3, 1), (3, 3)\}$$

- seien  $M_1 = [2, 3]$ ,  $M_2 = [6, 7]$  und  $N = [2, 3]$



- sei  $F$  die Menge der FACEBOOK-Nutzer

$$\{(x, y) \in F \times F \mid x \text{ ist FACEBOOK-Freund von } y\}$$

## §3.13 Definition (Relation)

Eine **Relation**  $R$  von  $M$  nach  $N$  ist eine Teilmenge  $R \subseteq M \times N$ .

Ist  $M = N$ , so heißt  $R$  auch **Relation auf  $M$** .

## Beispiele

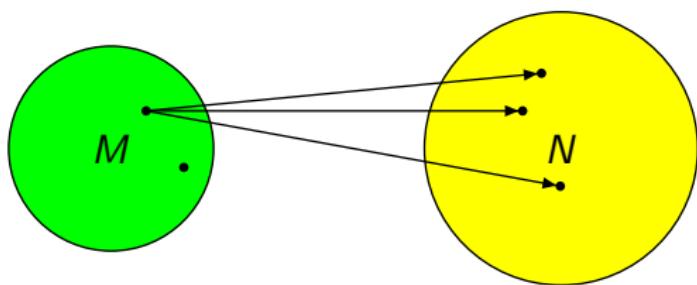
- sei  $B$  die Menge der Bundesbürger; Relation von  $B$  nach  $\mathbb{N}$

$$\{(p, n) \in B \times \mathbb{N} \mid p \text{ hat Identifikationsnummer } n\}$$

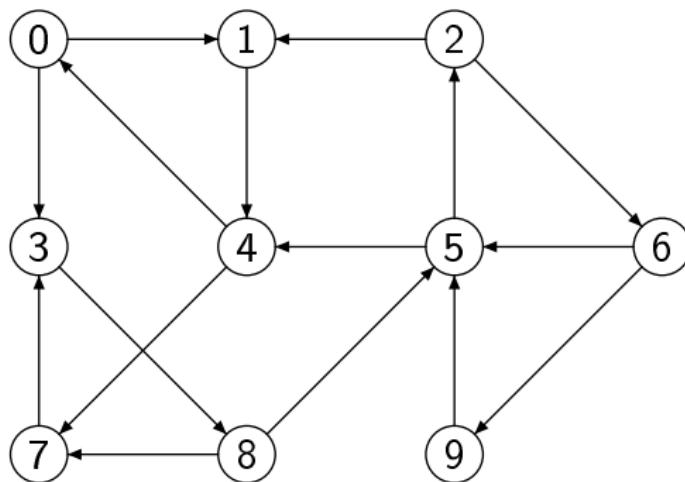
- $\leq = \{(n, n') \in \mathbb{N} \times \mathbb{N} \mid n \leq n'\}$  ist Relation auf  $\mathbb{N}$
- $\subseteq$  ist eine Relation auf  $\mathcal{P}(M)$
- Freund-Relation auf den FACEBOOK-Nutzern  $F$

$$\{(x, y) \in F \times F \mid x \text{ ist FACEBOOK-Freund von } y\}$$

Relation von  $M$  nach  $N$  (Elemente unbenannt):



Relation auf  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$  (Elemente benannt):



$$\{(0,1), (0,3), (1,4), (2,1), (2,6), (3,8), (4,0), (4,7), (5,2), (5,4), (6,5), (6,9), (7,3), (8,5), (8,7), (9,5)\}$$

## Notation

sei  $R$  eine Relation von  $M$  nach  $N$

- statt  $(m, n) \in R$  schreiben wir auch  $m R n$  oder  $R(m, n)$   
Mittelposition insb. für nicht-alphanumerische Zeichen wie  $\leq$
- statt  $(m, n) \notin R$  schreiben wir auch  $m \not R n$   
insb. für nicht-alphanumerische Zeichen wie  $=$
- wir nehmen an, dass Relationszeichen stärker binden  
als die logischen Verknüpfungen

$$(x \leq y \wedge y \leq x) \rightarrow x = y$$

heißt  $((x \leq y) \wedge (y \leq x)) \rightarrow (x = y)$

- ebenso lassen wir evtl. äußere Klammern um  $(x, y) \in R$  weg

## Eigenschaften von Relationen

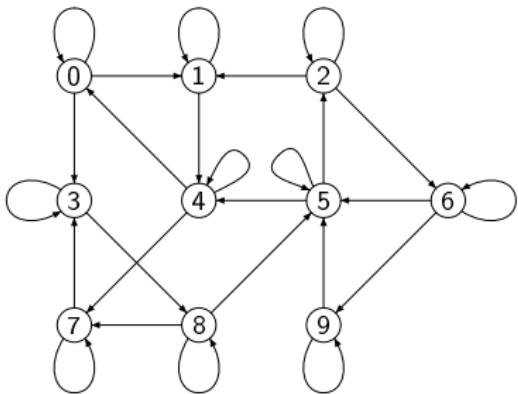
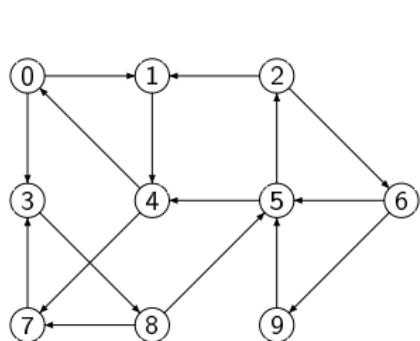
## §3.14 Definition

Eine Relation  $R \subseteq M \times M$  auf  $M$  heißt

- **reflexiv** gdw.  $(\forall m \in M). (m, m) \in R$
- **irreflexiv** gdw.  $(\forall m \in M). (m, m) \notin R$

# Relationen — Eigenschaften

irreflexiv (keine Schleifen) und reflexiv (alle Schleifen)



## §3.14 Definition

Eine Relation  $R \subseteq M \times M$  auf  $M$  heißt

- **symmetrisch** gdw.

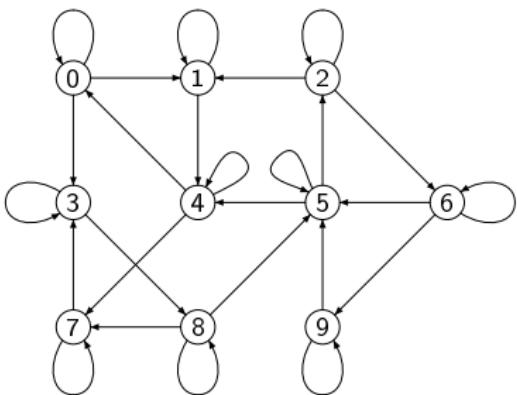
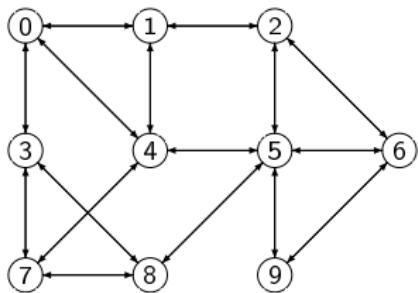
$$(\forall m, m' \in M). ((m, m') \in R \rightarrow (m', m) \in R)$$

- **antisymmetrisch** gdw.

$$(\forall m, m' \in M). \left( ((m, m') \in R \wedge (m', m) \in R) \rightarrow m = m' \right)$$

# Relationen — Eigenschaften

symmetrisch (wenn Pfeil, dann beidseitig) und  
antisymmetrisch (beidseitige Pfeile nur bei Schleifen)



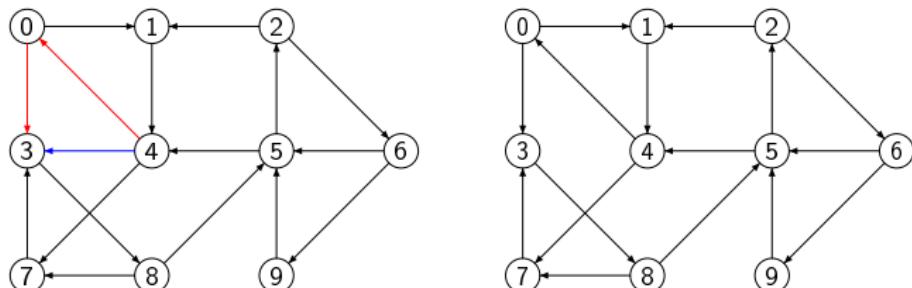
## §3.14 Definition

Eine Relation  $R \subseteq M \times M$  auf  $M$  heißt

- **transitiv** gdw.  $(\forall m, m', m'' \in M).$   
 $\left( ((m, m') \in R \wedge (m', m'') \in R) \rightarrow (m, m'') \in R \right)$
- **linear** gdw.  $(\forall m, m' \in M).((m, m') \in R \vee (m', m) \in R)$

# Relationen — Eigenschaften

**transitiv** (für jede Kette existiert auch eine “Abkürzung”) und  
**linear** (mind. ein Pfeil zwischen 2 Elementen)



(diese Relationen sind also nicht transitiv und nicht linear)

## Beispiele

- $\emptyset$  ist eine Relation auf  $\mathbb{N}$
- $\leq = \{(n, n') \in \mathbb{N} \times \mathbb{N} \mid n \leq n'\}$  Relation auf  $\mathbb{N}$
- $= = \{(n, n) \mid n \in \mathbb{N}\}$  ist eine Relation auf  $\mathbb{N}$
- $\subseteq$  ist eine Relation auf  $\mathcal{P}(M)$  mit  $|M| \geq 2$
- Freund-Relation auf den FACEBOOK-Nutzern  $F$

$$\text{Fr} = \{(x, y) \in F \times F \mid x \text{ ist FACEBOOK-Freund von } y\}$$

Eigenschaft \ Relation	$\emptyset$	$\leq$	$=$	$\subseteq$	Fr
reflexiv	<b>X</b>	<b>✓</b>	<b>✓</b>	<b>✓</b>	<b>X</b>
irreflexiv	<b>✓</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>✓</b>
symmetrisch	<b>✓</b>	<b>X</b>	<b>✓</b>	<b>X</b>	<b>✓</b>
antisymmetrisch	<b>✓</b>	<b>✓</b>	<b>✓</b>	<b>✓</b>	<b>X</b>
transitiv	<b>✓</b>	<b>✓</b>	<b>✓</b>	<b>✓</b>	<b>X</b>
linear	<b>X</b>	<b>✓</b>	<b>X</b>	<b>X</b>	<b>X</b>

- Verallgemeinerung Vereinigung und Schnitt
- Potenzmenge
- Vollständige Induktion
- Einführung Relationen und deren Eigenschaften

Dritte Übungsserie ist bereits im OLAT.

# Diskrete Strukturen

## Vorlesung 4: Relationen & Funktionen

Andreas Maletti

4. November 2014

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## heutige Vorlesung

- ① Äquivalenzrelationen
- ② Operationen auf Relationen
- ③ Ordnungsrelationen
- ④ Einführung Funktionen

Bitte Fragen direkt stellen!

Organisation

## Fehler

- DS 3, Seite 56 [Beispiel verallgemeinerter Schnitt]:  
es sollte  $r \in \mathbb{R}_{\geq 0}$  (statt  $r \in \mathbb{R}$ ) heißen  
sonst ist  $[-r, r]$  nicht definiert
- werde ich korrigieren; Vermerk hier bleibt

Rückblick: Relationen

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

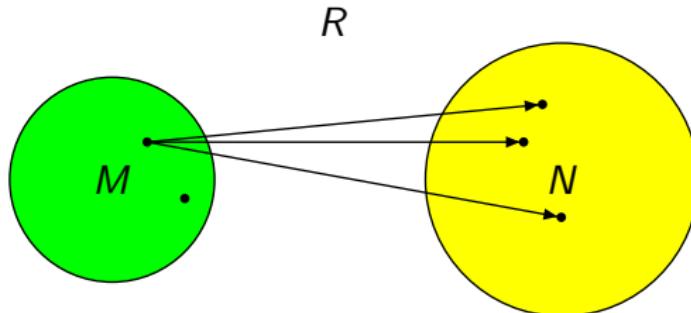
## Definition (§3.12 und §3.13)

Für alle Mengen  $M$  und  $N$  ist das **Produkt**  $M \times N$  definiert durch

$$M \times N = \{(m, n) \mid m \in M, n \in N\}$$

Eine **Relation**  $R$  von  $M$  nach  $N$  ist eine Teilmenge  $R \subseteq M \times N$ .

Ist  $M = N$ , so heißt  $R$  auch **Relation auf  $M$** .



## Äquivalenzrelationen

## §4.1 Definition (Äquivalenzrelation)

Eine Relation  $\equiv$  auf  $M$  ist eine **Äquivalenzrelation**  
gdw. sie reflexiv, symmetrisch und transitiv ist

- $(\forall m \in M). m \equiv m$  reflexiv
- $(\forall m, m' \in M). (m \equiv m' \rightarrow m' \equiv m)$  symmetrisch
- $(\forall m, m', m'' \in M). ((m \equiv m' \wedge m' \equiv m'') \rightarrow m \equiv m'')$  transitiv

Eigenschaft \ Relation	$\emptyset$	$\leq$	$=$	$\subseteq$	Fr
reflexiv	X	✓	✓	✓	X
irreflexiv	✓	X	X	X	✓
symmetrisch	✓	X	✓	X	✓
antisymmetrisch	✓	✓	✓	✓	X
transitiv	✓	✓	✓	✓	X
linear	X	✓	X	X	X

## Beispiele

- ①  $=$  auf  $\mathbb{N}$  ist eine Äquivalenzrelation
- ②  $\leq$  auf  $\mathbb{N}$  ist **keine** Äquivalenzrelation
- ③  $R_2 = \{(n, n') \in \mathbb{N} \times \mathbb{N} \mid n + n' \text{ ist gerade}\}$   
ist eine Äquivalenzrelation

Beweis zu ③.

- **reflexiv:** für alle  $n \in \mathbb{N}$  ist  $n + n = 2n$  gerade, also  $(n, n) \in R_2$
- **symmetrisch:** Seien  $n, n' \in \mathbb{N}$ , so dass  $(n, n') \in R_2$ .  
Damit ist  $n + n' = n' + n$  gerade, womit auch  $(n', n) \in R_2$  gilt.
- **transitiv:** Seien  $n, n', n'' \in \mathbb{N}$ , so dass  $(n, n') \in R_2$  und  $(n', n'') \in R_2$ . Daher sind  $n + n'$  und  $n' + n''$  gerade; d.h. es existieren  $k, k' \in \mathbb{N}$ , so dass  $n + n' = 2k$  und  $n' + n'' = 2k'$ .  
$$n + n'' = (2k - n') + (2k' - n') = 2k + 2k' - 2n' = 2(k + k' - n')$$
womit auch  $n + n''$  gerade ist und daher  $(n, n'') \in R_2$ . □

Wie sieht  $R_2$  aus?

- $(0, 0) \in R_2$  und  $(0, 1) \notin R_2$  und  $(0, 2) \in R_2$   
→ 0 steht genau zu allen geraden Zahlen in Relation
- $(1, 0) \notin R_2$  und  $(1, 1) \in R_2$  und  $(1, 2) \notin R_2$   
→ 1 steht genau zu allen ungeraden Zahlen in Relation
- $(2, 0) \in R_2$  und  $(2, 1) \notin R_2$  und  $(2, 2) \in R_2$   
→ 2 steht genau zu allen geraden Zahlen in Relation

$R_2$  unterscheidet zwischen gerade/ungerade

## §4.2 Definition (Äquivalenzklasse)

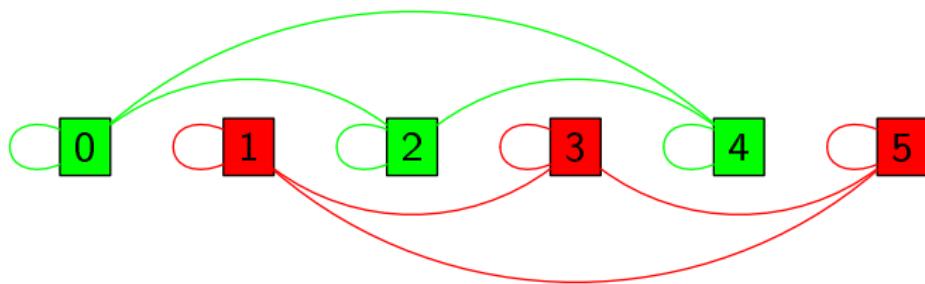
Sei  $\equiv$  eine Äquivalenzrelation auf  $M$  und  $m \in M$  beliebig. Dann ist

$$[m]_{\equiv} = \{m' \in M \mid m \equiv m'\}$$

die  $m$ -Äquivalenzklasse von  $\equiv$ .

# Relationen — Äquivalenzrelationen

statt beidseitiger Pfeile verwenden wir Splines ohne Pfeile



## Notation und Begriffe

Sei  $\equiv$  eine Äquivalenzrelation auf  $M$  und  $m \in M$

- jedes  $m' \in [m]_{\equiv}$  heißt **Vertreter** oder **Repräsentant** der Äquivalenzklasse  $[m]_{\equiv}$
- sofern  $\equiv$  sich aus dem Kontext ergibt, schreiben wir einfach  $[m]$  statt  $[m]_{\equiv}$

## §4.3 Theorem

Sei  $\equiv$  eine Äquivalenzrelation auf  $M$  und seien  $m, m' \in M$ . Dann gilt  $m \equiv m'$  gdw.  $[m] = [m']$ .

Beweis.

beidseitige Implikationen:

- ( $\rightarrow$ ) Sei  $m \equiv m'$ . Z.zg.  $[m] = [m']$  durch beidseitige Teilmengen:
  - ( $\subseteq$ ) Sei  $m'' \in [m]$ . Dann gilt  $m \equiv m''$ . Mit Symmetrie folgt aus  $m \equiv m'$  auch  $m' \equiv m$  und vermittels Transitivität gilt damit  $m' \equiv m''$ . Folglich  $m'' \in [m']$ .
  - ( $\supseteq$ ) Sei  $m'' \in [m']$ . Dann gilt  $m' \equiv m''$ . Vermittels Transitivität gilt damit  $m \equiv m''$ . Folglich  $m'' \in [m]$ .
- ( $\leftarrow$ ) Sei  $[m] = [m']$ . Gemäß Reflexivität gilt  $m' \in [m'] = [m]$ . Also  $m \equiv m'$ . □

## §4.4 Definition

Sei  $\equiv$  eine Äquivalenzrelation auf  $M$ . Dann ist

$$(M/\equiv) = \{[m]_{\equiv} \mid m \in M\}$$

die Menge aller Äquivalenzklassen von  $\equiv$

(auch: Quotient von  $M$  via  $\equiv$ )

## Beispiele

- $(\mathbb{N}/=) = \{\{0\}, \{1\}, \{2\}, \dots\}$
- $(\mathbb{N}/R_2) = \{\{0, 2, 4, 6, \dots\}, \{1, 3, 5, 7, \dots\}\} = \{G, U\}$

## §4.5 Definition (Zerlegung)

Sei  $M$  eine Menge. Eine **Zerlegung von  $M$**  ist eine Menge  $\mathcal{N} \subseteq \mathcal{P}(M)$ , so dass

- ①  $\emptyset \notin \mathcal{N}$  (alle Teilmengen nicht leer)
- ②  $M = \bigcup \mathcal{N}$  (jedes Element vertreten)
- ③  $N \cap N' = \emptyset$  für alle  $N, N' \in \mathcal{N}$  mit  $N \neq N'$  (zwei verschiedene Elemente sind disjunkt)

## Beispiele

- $(\mathbb{N}/=) = \{\{0\}, \{1\}, \{2\}, \dots\}$
- $(\mathbb{N}/R_2) = \{\{0, 2, 4, 6, \dots\}, \{1, 3, 5, 7, \dots\}\} = \{G, U\}$

## §4.6 Theorem

Sei  $\equiv$  eine Äquivalenzrelation auf  $M$ .

Dann ist  $(M/\equiv)$  eine Zerlegung von  $M$ .

Beweis.

Sei  $\mathcal{M} = (M/\equiv)$ . Offensichtlich ist  $\mathcal{M} \subseteq \mathcal{P}(M)$ .

Z.zg.  $\mathcal{M}$  ist Zerlegung (§4.5 Punkte ①–③):

- ① (*Direkt.*)  $\equiv$  ist reflexiv und damit  $m \in [m]$  für jedes  $m \in M$ .  
Also gilt  $[m] \neq \emptyset$  und damit  $\emptyset \notin \mathcal{M} = \{[m] \mid m \in M\}$ .
- ② (*Beidseitige Teilmengen.*)  $\bigcup \mathcal{M} \subseteq M$  ist trivial. Für jedes  $m \in M$  gilt  $m \in [m] \subseteq \bigcup \mathcal{M}$  wie in ①, womit  $M \subseteq \bigcup \mathcal{M}$ .
- ③ (*Kontraposition, dann beidseitige Teilmengen.*) Seien  $M_1, M_2 \in \mathcal{M}$  mit  $M_1 \cap M_2 \neq \emptyset$ . Dann existiert  $m \in M_1 \cap M_2$ . Für jedes  $m' \in M_1$  gilt  $m \equiv m'$  und damit  $m' \in M_2$ . Also  $M_1 \subseteq M_2$ . Ebenso  $M_2 \subseteq M_1$  da  $m \equiv m''$  und  $m'' \in M_1$  für alle  $m'' \in M_2$ .



## §4.7 Theorem

Sei  $\mathcal{N}$  eine Zerlegung von  $M$ . Dann ist

$$\equiv = \{(m, m') \in M \times M \mid (\exists N \in \mathcal{N}). \{m, m'\} \subseteq N\}$$

eine Äquivalenzrelation auf  $M$ .

### Beweis.

Offensichtlich ist  $\equiv$  eine Relation auf  $M$ .

- **reflexiv:** Sei  $m \in M$ . Da  $M = \bigcup \mathcal{N}$  (§4.5), gibt eine Menge  $N \in \mathcal{N}$  mit  $m \in N$ . Also  $m \equiv m$ .
- **symmetrisch:** Sei  $m \equiv m'$ . Dann existiert  $N \in \mathcal{N}$  mit  $\{m, m'\} \subseteq N$ . Folglich auch  $m' \equiv m$ .
- **transitiv:** Seien  $m \equiv m'$  und  $m' \equiv m''$ . Also existieren  $N, N' \in \mathcal{N}$  mit  $\{m, m'\} \subseteq N$  und  $\{m', m''\} \subseteq N'$ . Da  $m' \in N \cap N'$  gilt  $N = N'$  nach §4.5 ③. Folglich  $\{m, m''\} \subseteq N$  und damit  $m \equiv m''$ .

□

## §4.8 Korollar

- Sei  $\equiv$  eine Äquivalenzrelation auf  $M$ . Dann gilt

$$\equiv = \{(m, m') \in M \times M \mid (\exists N \in (M/\equiv)). \{m, m'\} \subseteq N\}$$

- Sei  $\mathcal{N}$  eine Zerlegung von  $M$ . Dann gilt  $\mathcal{N} = (M/\equiv)$ , wobei

$$\equiv = \{(m, m') \in M \times M \mid (\exists N \in \mathcal{N}). \{m, m'\} \subseteq N\}$$

## Zusammenfassung

- Äquivalenzrelationen und Zerlegungen sind (stark) korrespondierende Begriffe

Operationen mit Relationen

## Notizen

- Relationen sind spezielle Mengen
- alle Mengenoperationen auch auf Relationen anwendbar  
(Vereinigung, Schnitt, Differenz, Komplement)
- spezielle Struktur liefert neue Operationen

## §4.9 Definition

Seien  $R \subseteq M \times N$  und  $R' \subseteq N \times P$  Relationen.

- Die **inverse Relation  $R^{-1}$**  von  $R$  ist definiert durch  
(Tausch der Komponenten; Umkehr der Pfeile)

$$R^{-1} = \{(n, m) \in N \times M \mid (m, n) \in R\}$$

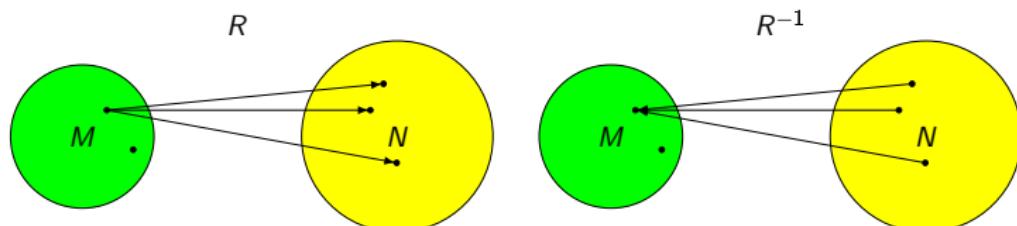
- Die **Komposition  $R ; R'$**  von  $R$  gefolgt von  $R'$  ist definiert durch  
(auch Verkettung)

$$R ; R' = \{(m, p) \in M \times P \mid (\exists n \in N). (R(m, n) \wedge R'(n, p))\}$$

## Beispiel — Inverses

- sei  $R = \{(1, 1), (1, 3), (2, 2), (2, 4), (3, 2)\}$

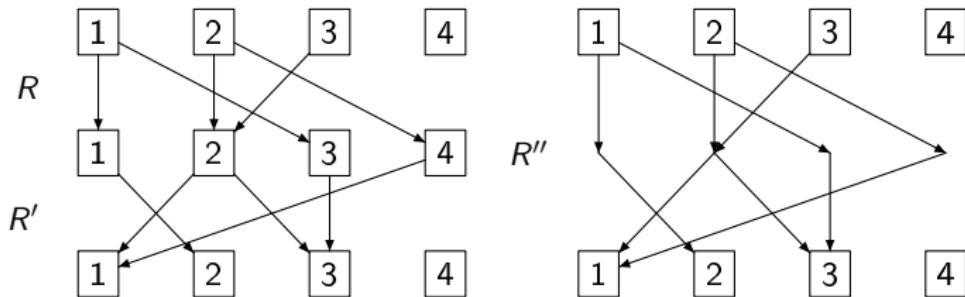
$$R^{-1} = \{(1, 1), (3, 1), (2, 2), (4, 2), (2, 3)\}$$



## Beispiel — Komposition

- seien  $R = \{(1, 1), (1, 3), (2, 2), (2, 4), (3, 2)\}$   
und  $R' = \{(1, 2), (2, 1), (2, 3), (3, 3), (4, 1)\}$

$$R'' = R ; R' = \{(1, 2), (1, 3), (2, 1), (2, 3), (3, 1), (3, 3)\}$$



Rückblick: Eigenschaften von Relationen

## §4.10 Definition

Für jede Menge  $M$  existieren folgende Relationen auf  $M$ :

- die **leere Relation**  $\emptyset$
- die **Identität**  $\text{id}_M = \{(m, m) \mid m \in M\}$   
(dies ist die Äquivalenzrelation  $=$ )
- die **Allrelation**  $M \times M$

## Definition (§3.14)

Eine Relation  $R$  auf  $M$  heißt

- **reflexiv** gdw.  $(\forall m \in M). (m, m) \in R$
- **irreflexiv** gdw.  $(\forall m \in M). (m, m) \notin R$

## §4.11 Theorem

Eine Relation  $R$  auf  $M$  ist

- **reflexiv** gdw.  $\text{id}_M \subseteq R$
- **irreflexiv** gdw.  $\text{id}_M \cap R = \emptyset$

## Definition (§3.14)

Eine Relation  $R$  auf  $M$  heißt

- **symmetrisch** gdw.  
 $(\forall m, m' \in M). ((m, m') \in R \rightarrow (m', m) \in R)$
- **antisymmetrisch** gdw.  
 $(\forall m, m' \in M). \left( ((m, m') \in R \wedge (m', m) \in R) \rightarrow m = m' \right)$

## §4.12 Theorem

Eine Relation  $R$  auf  $M$  ist

- **symmetrisch** gdw.  $R \subseteq R^{-1}$
- **antisymmetrisch** gdw.  $R \cap R^{-1} \subseteq \text{id}_M$

## Definition (§3.14)

Eine Relation  $R$  auf  $M$  heißt

- **transitiv** gdw.  $(\forall m, m', m'' \in M). ((m, m') \in R \wedge (m', m'') \in R) \rightarrow (m, m'') \in R$
- **linear** gdw.  $(\forall m, m' \in M). ((m, m') \in R \vee (m', m) \in R)$

## §4.13 Theorem

Eine Relation  $R$  auf  $M$  ist

- **transitiv** gdw.  $R ; R \subseteq R$
- **linear** gdw.  $R \cup R^{-1} = M \times M$

## Beispiele

- $\emptyset$  ist Relation auf  $\mathbb{N}$
- $\leq = \{(n, n') \in \mathbb{N} \times \mathbb{N} \mid n \leq n'\}$  ist Relation auf  $\mathbb{N}$
- $\text{id}_{\mathbb{N}} = \{(n, n) \mid n \in \mathbb{N}\}$  ist Relation auf  $\mathbb{N}$
- $\subseteq$  ist Relation auf  $\mathcal{P}(M)$  mit  $|M| \geq 2$
- Freund-Relation auf den FACEBOOK-Nutzern  $F$

$$\text{Fr} = \{(x, y) \in F \times F \mid x \text{ ist FACEBOOK-Freund von } y\}$$

Eigenschaft \ Relation	$\emptyset$	$\leq$	$\text{id}_{\mathbb{N}}$	$\subseteq$	Fr
reflexiv	$\text{X}$	$\checkmark$	$\checkmark$	$\checkmark$	$\text{X}$
irreflexiv	$\checkmark$	$\text{X}$	$\text{X}$	$\text{X}$	$\checkmark$
symmetrisch	$\checkmark$	$\text{X}$	$\checkmark$	$\text{X}$	$\checkmark$
antisymmetrisch	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\text{X}$
transitiv	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\text{X}$
linear	$\text{X}$	$\checkmark$	$\text{X}$	$\text{X}$	$\text{X}$

Ordnungsrelationen

## §4.14 Definition (Ordnungsrelation)

Eine Relation  $\preceq$  auf  $M$  ist eine **Ordnungsrelation** gdw. sie reflexiv, antisymmetrisch und transitiv ist.

- $(\forall m \in M). m \preceq m$  reflexiv
- $(\forall m, m' \in M). ((m \preceq m' \wedge m' \preceq m) \rightarrow m = m')$  antisymmetrisch
- $(\forall m, m', m'' \in M). ((m \preceq m' \wedge m' \preceq m'') \rightarrow m \preceq m'')$  transitiv

Das Paar  $(M, \preceq)$  heißt dann **teilweise geordnete Menge**.

Ist  $\preceq$  linear, dann heißt  $(M, \preceq)$  auch **linear geordnete Menge**.

- $(\forall m, m' \in M). (m \preceq m' \vee m' \preceq m)$  linear

## Beispiele

- ①  $\text{id}_{\mathbb{N}}$  ist eine Ordnungsrelation, aber nicht linear
- ②  $\leq$  auf  $\mathbb{N}$  ist eine lineare Ordnungsrelation
- ③  $| = \{(n, n') \in \mathbb{N}_+ \times \mathbb{N}_+ \mid n \text{ teilt } n'\}$  ist eine Ordnungsrelation  
wobei  $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$

Beweis zu ③.

- **reflexiv:** für alle  $n \in \mathbb{N}_+$  teilt  $n$  sich selbst, also  $n|n$ .
- **antisymmetrisch:** Seien  $n|n'$  und  $n'|n$ . Dann gilt  $n \leq n'$  und  $n' \leq n$ , womit  $n = n'$  folgt (Antisymmetrie von  $\leq$ ).
- **transitiv:** Seien  $n|n'$  und  $n'|n''$ . D.h. es existieren  $k, k' \in \mathbb{N}_+$ , so dass  $kn = n'$  und  $k'n' = n''$ . Also

$$n'' = k'n' = k'(kn) = (k'k)n ,$$

womit auch  $n|n''$  gilt. □

## Beispiele

- $\emptyset$  ist eine Relation auf  $\mathbb{N}$
- $\leq = \{(n, n') \in \mathbb{N} \times \mathbb{N} \mid n \leq n'\}$  Relation auf  $\mathbb{N}$
- $\text{id}_{\mathbb{N}} = \{(n, n) \mid n \in \mathbb{N}\}$  ist eine Relation auf  $\mathbb{N}$
- $\subseteq$  ist eine Relation auf  $\mathcal{P}(M)$  mit  $|M| \geq 2$
- Freund-Relation auf den FACEBOOK-Nutzern  $F$

$$\text{Fr} = \{(x, y) \in F \times F \mid x \text{ ist FACEBOOK-Freund von } y\}$$

Eigenschaft \ Relation	$\emptyset$	$\leq$	$\text{id}_{\mathbb{N}}$	$\subseteq$	Fr
reflexiv	$\times$	✓	✓	✓	$\times$
irreflexiv	✓	$\times$	$\times$	$\times$	✓
symmetrisch	✓	$\times$	✓	$\times$	✓
antisymmetrisch	✓	✓	✓	✓	$\times$
transitiv	✓	✓	✓	✓	$\times$
linear	$\times$	✓	$\times$	$\times$	$\times$

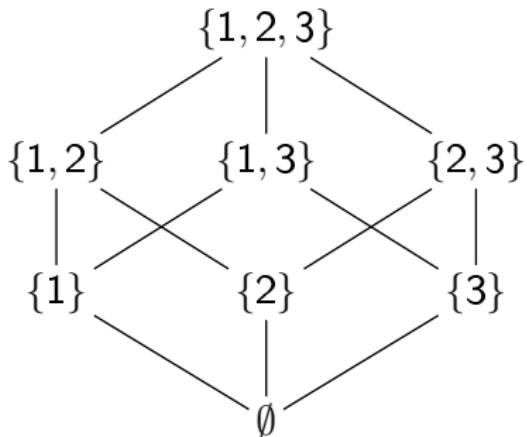
## Alternative Bezeichnungen

- **partiell geordnet** = teilweise geordnet
- **Kette** = linear geordnete Menge

## HASSE-Diagramm

- grafische Darstellung endlicher teilweise geordneter Mengen
- alle Kanten sind per Konvention nach oben gerichtet
- Kanten aus  $\text{id}_M$  (Schleifen) nicht dargestellt
- Kanten, die sich mittels Transitivität aus anderen Kanten ergeben, werden nicht dargestellt

# Relationen — Ordnungsrelationen



HELMUT HASSE (\* 1898; † 1979)

- dtsch. Mathematiker
- Algebra und algebraische Zahlentheorie
- unterschrieb "Bekenntnis der deutschen Professoren zu ADOLF HITLER"



© Konrad Jacobs

## Frage

- Wie viele teilweise geordnete Mengen  $(M, \preceq)$  mit  $M = \{1, 2, 3\}$  gibt es? 19
- Wie viele linear geordnete Mengen  $(M, \preceq)$  mit  $M = \{1, 2, 3\}$  gibt es? 6

Funktionen

## Beispiele

- sei  $B$  die Menge der Bundesbürger; Relation von  $B$  nach  $\mathbb{N}$

$$\{(p, n) \in B \times \mathbb{N} \mid p \text{ hat Identifikationsnummer } n\}$$

- Freund-Relation auf den FACEBOOK-Nutzern  $F$

$$\{(x, y) \in F \times F \mid x \text{ ist FACEBOOK-Freund von } y\}$$

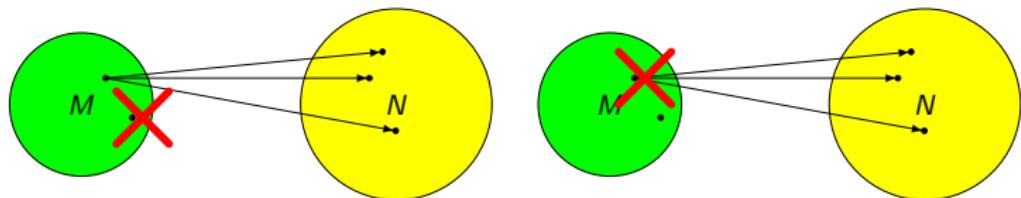
## Diskussion

- manchmal ist eine eindeutige Zuordnung gewünscht  
z.B. Identifikationsnummer
- derartige Relationen sehr relevant in Praxis (Programmierung) und Theorie (Mathematik)

## Eigenschaften

- jedes  $m \in M$  sollte einen Partner haben
  - jedes  $m \in M$  sollte eindeutigen Partner haben
- jedes  $m \in M$  sollte genau einen Partner haben

Illustration einer Relation, die keine eindeutige Zuordnung liefert:



## §4.15 Definition (Funktion)

Eine Relation  $R \subseteq M \times N$  ist eine **Funktion** oder **Abbildung** gdw. für jedes  $m \in M$  genau ein  $n \in N$  existiert, so dass  $(m, n) \in R$ .

- *Formalisierung:* ... mind. ein  $n \in N$  ...

$$(\forall m \in M). (\exists n \in N). R(m, n)$$

(jedes  $m \in M$  hat einen Partner)

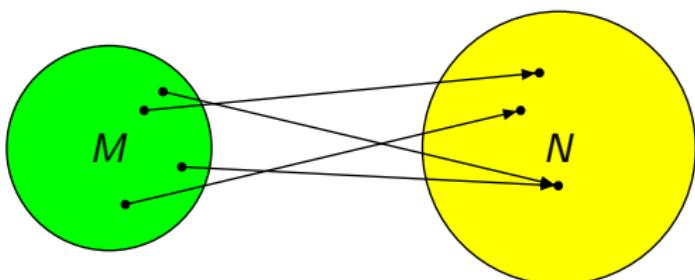
- *Formalisierung:* ... höchstens ein  $n \in N$  ...

$$(\forall m \in M). (\forall n, n' \in N). \left( (R(m, n) \wedge R(m, n')) \rightarrow n = n' \right)$$

(alle Partner von  $m$  sind gleich)

## Beispiele

- sei  $B$  die Menge der Bundesbürger; Relation von  $B$  nach  $\mathbb{N}$ 
$$\{(p, n) \in B \times \mathbb{N} \mid p \text{ hat Identifikationsnummer } n\}$$
ist (vermutlich) eine Funktion
- Freund-Relation auf den FACEBOOK-Nutzern  $F$ 
$$\{(x, y) \in F \times F \mid x \text{ ist FACEBOOK-Freund von } y\}$$
ist (vermutlich) **keine** Funktion
- $R = \{(n, n') \mid n \in \mathbb{N}, n' = 2n\}$  ist eine Funktion
- $\text{id}_M$  ist eine Funktion



## §4.16 Notation

Sei  $f \subseteq M \times N$  eine Funktion von  $M$  nach  $N$

## Beispiele

- sei  $\text{id}_M: M \rightarrow M$  die Funktion, so dass für alle  $m \in M$

$$\text{id}_M(m) = m$$

- sei  $\text{verdoppeln}: \mathbb{N} \rightarrow \mathbb{N}$  die Funktion, so dass für alle  $n \in \mathbb{N}$

$$\text{verdoppeln}(n) = 2n$$

## §4.17 Definition

Sei  $f: M \rightarrow N$ .

- $M$  heißt **Definitionsbereich von  $f$**
- $N$  heißt **Bildbereich von  $f$**

alternativ: **Wertebereich** oder **Zielbereich**

- für alle  $M' \subseteq M$  ist  $f(M') = \{f(m) \mid m \in M'\}$   
die Menge aller Bilder von Elementen aus  $M'$
- für alle  $N' \subseteq N$  ist  $f^{-1}(N') = \{m \in M \mid f(m) \in N'\}$   
die Menge aller Ur-Bilder von Elementen aus  $N'$

## Beispiele

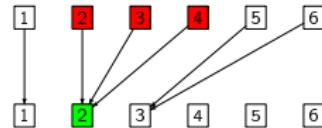
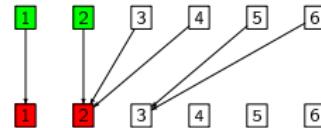
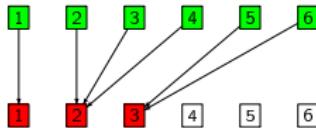
- $\text{id}_M(M') = M'$  und  $\text{id}_M^{-1}(M') = M'$  für alle  $M' \subseteq M$
- $\text{verdoppeln}(\mathbb{N}) = G$  und  $\text{verdoppeln}^{-1}(U) = \emptyset$

## Beispiel

- sei  $M = \{1, 2, 3, 4, 5, 6\}$  und  $f: M \rightarrow M$ , so dass  
 $f(m) = \lceil \sqrt{m} \rceil$  für alle  $m \in M$

Aufrunden  $\lceil \dots \rceil$

- $f(M) = \{1, 2, 3\}$
- $f(\{1, 2\}) = \{1, 2\}$
- $f^{-1}(\{2\}) = \{2, 3, 4\}$



- Äquivalenzrelationen und Zerlegungen
- Operationen auf Relationen
- Ordnungsrelationen
- Einführung Funktionen
- Definitions- und Bildbereich

Vierte Übungsserie ist bereits im OLAT.

# Diskrete Strukturen

## Vorlesung 5: Funktionen und Auswahlaxiom

Andreas Maletti

11. November 2014

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## heutige Vorlesung

- ① Eigenschaften von Funktionen
- ② Invertierung von Funktionen
- ③ Auswahlaxiom und Begriff: Axiom

Bitte Fragen direkt stellen!

Rückblick: Funktionen

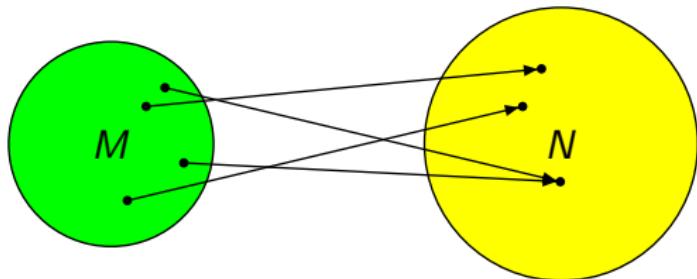
## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## Definition (§4.15)

Eine Relation  $R \subseteq M \times N$  ist eine **Funktion** gdw.

für jedes  $m \in M$  genau ein  $n \in N$  existiert, so dass  $(m, n) \in R$



## Eigenschaften von Funktionen

## §5.1 Definition

Eine Funktion  $f: M \rightarrow N$  ist

- **injektiv** gdw. falls alle verschiedenen Elemente von  $M$  auch verschiedene Bilder unter  $f$  haben

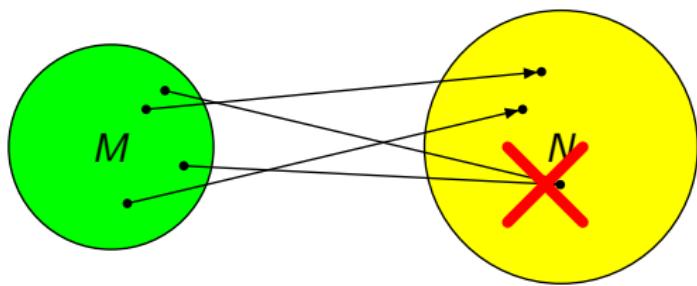
$$(\forall m, m' \in M). (m \neq m' \rightarrow f(m) \neq f(m'))$$

- **surjektiv** gdw.  $f(M) = N$   
jedes Element von  $N$  ist Bild eines Elements von  $M$

$$(\forall n \in N). (\exists m \in M). f(m) = n$$

- **bijektiv** gdw.  $f$  injektiv und surjektiv ist

nicht injektiv:



## §5.1 Definition

Eine Funktion  $f: M \rightarrow N$  ist

- **injektiv** gdw. falls alle verschiedenen Elemente von  $M$  auch verschiedene Bilder unter  $f$  haben

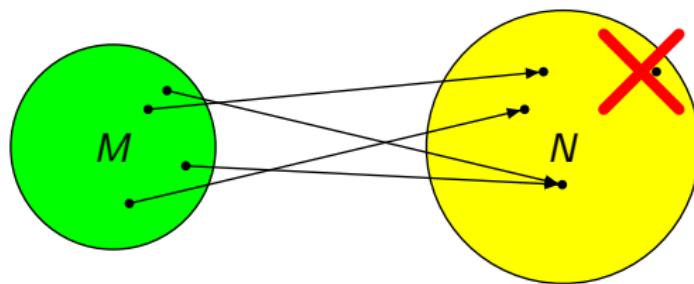
$$(\forall m, m' \in M). (m \neq m' \rightarrow f(m) \neq f(m'))$$

- **surjektiv** gdw.  $f(M) = N$   
jedes Element von  $N$  ist Bild eines Elements von  $M$

$$(\forall n \in N). (\exists m \in M). f(m) = n$$

- **bijektiv** gdw.  $f$  injektiv und surjektiv ist

nicht surjektiv:



## Beispiele

- $\text{id}_M: M \rightarrow M$  mit  $\text{id}_M(m) = m$  ist bijektiv
- verdoppeln:  $\mathbb{N} \rightarrow \mathbb{N}$  mit  $\text{verdoppeln}(n) = 2n$   
ist injektiv, aber **nicht** surjektiv (3 nicht erreichbar)
- $f: \mathbb{N} \rightarrow \mathbb{N}$  mit  $f(n) = \lceil \sqrt{n} \rceil$   
ist **nicht** injektiv, aber surjektiv (denn  $f(2) = f(3)$ )
- quadrieren:  $\mathbb{R} \rightarrow \mathbb{R}$  mit  $\text{quadrieren}(x) = x^2$   
ist **weder** injektiv noch surjektiv  
(negative Zahlen nicht erreichbar und  $(-2)^2 = 2^2$ )

## Notizen

- eine bijektive Funktion auf einer Menge  $M$  heißt auch  
**Permutation von  $M$**  (siehe Kombinatorik)
- wir importieren alle Operationen von Relationen  
z.B. zwei Funktionen  $f, g: M \rightarrow N$  sind **gleich** ( $f = g$ ) gdw.  
 $f(m) = g(m)$  für alle  $m \in M$   
dies entspricht der Gleichheit der Relationen

## §5.2 Theorem

Die Komposition zweier Funktionen ist wieder eine Funktion.

### Beweis.

Seien  $f: M \rightarrow N$  und  $g: N \rightarrow P$ . Dann ist  $(f ; g)(m) = g(f(m))$   
für alle  $m \in M$ .



## §5.3 Theorem

Seien  $f: M \rightarrow N$ ,  $g: N \rightarrow P$  und  $h: P \rightarrow Q$ .

- ①  $(f ; g) ; h = f ; (g ; h)$  (Assoziativitat der Komposition)
- ②  $f ; g$  ist injektiv, falls  $f$  und  $g$  injektiv sind

Beweis.

- ① Nach §5.2 sind beides Funktionen. Sei  $m \in M$  beliebig.

$$\begin{aligned} ((f ; g) ; h)(m) &= h((f ; g)(m)) = h(g(f(m))) \\ &= (g ; h)(f(m)) = (f ; (g ; h))(m) \end{aligned}$$

- ② Seien  $m, m' \in M$  mit  $m \neq m'$ . Da  $f$  injektiv ist, gilt  $f(m) \neq f(m')$ . Da auch  $g$  injektiv ist, gilt weiterhin

$$(f ; g)(m) = g(f(m)) \neq g(f(m')) = (f ; g)(m')$$



## §5.4 Theorem

Seien  $f: M \rightarrow N$  und  $g: N \rightarrow P$ .

- ①  $f ; g$  ist surjektiv, falls  $f$  und  $g$  surjektiv sind
- ②  $f ; g$  ist bijektiv, falls  $f$  und  $g$  bijektiv sind

### Beweis.

- ① Sei  $p \in P$  beliebig. Da  $g$  surjektiv ist, existiert  $n \in N$ , so dass  $g(n) = p$ . Weiterhin ist auch  $f$  surjektiv, wodurch  $m \in M$  existiert, so dass  $f(m) = n$ . Also ist

$$(f ; g)(m) = g(f(m)) = g(n) = p$$

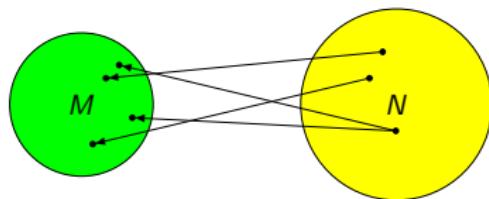
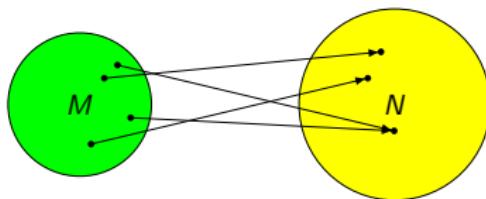
Also ist  $f ; g$  auch surjektiv.

- ② Dies ergibt sich direkt aus ① und §5.3②



## Notizen

- die Assoziativität der Komposition gilt auch für Relationen
- $f^{-1}$  ist i.A. nur eine Relation für  $f: M \rightarrow N$



## §5.5 Theorem

Sei  $f: M \rightarrow N$ . Für alle  $m \in M$  und  $n \in N$  gelten

- ①  $m \in f^{-1}(\{f(m)\})$
- ②  $f(f^{-1}(\{n\})) = \{n\}$

### Beweis.

- ① Wir setzen zunächst einfach die Definition ein:

$$\begin{aligned}f^{-1}(\{f(m)\}) &= \{m' \in M \mid f(m') \in \{f(m)\}\} \\&= \{m' \in M \mid f(m') = f(m)\}\end{aligned}$$

und damit  $m \in f^{-1}(\{f(m)\})$ .

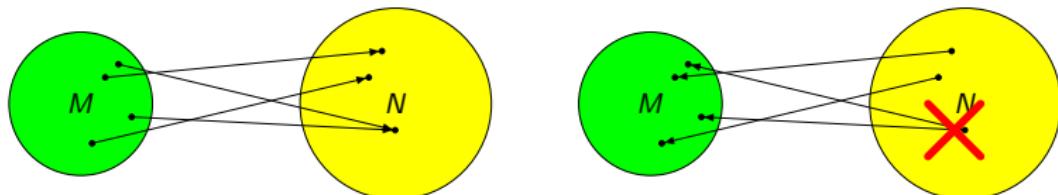
- ② Ebenso

$$\begin{aligned}f(f^{-1}(\{n\})) &= \{f(m') \mid m' \in f^{-1}(\{n\})\} \\&= \{f(m') \mid m' \in \{m'' \in M \mid f(m'') = n\}\} \\&= \{f(m') \mid m' \in M, f(m') = n\} = \{n\}\end{aligned}\quad \square$$

## Motivation

- manchmal möchte man eine Funktionsanwendung rückgängig machen können
- z.B. Verschlüsselung, Kompression, ...  
→ invertierbare Funktionen

Nicht invertierbar:



## §5.6 Definition (invertierbar)

Eine Funktion  $f: M \rightarrow N$  ist **invertierbar** gdw.  
eine Funktion  $g: N \rightarrow M$  existiert, so dass

$$f ; g = \text{id}_M \quad \text{und} \quad g ; f = \text{id}_N$$

## Beispiele

- $\text{id}_M$  ist offensichtlich invertierbar (vermittels  $\text{id}_M$ )
- verdoppeln ist **nicht** invertierbar

Welchen Wert soll die inverse Funktion 3 zuweisen?

- $f$  mit  $f(n) = \lceil \sqrt{n} \rceil$  ist **nicht** invertierbar

Welchen Wert soll die inverse Funktion 2 zuweisen?

## §5.7 Theorem

Eine Funktion  $f: M \rightarrow N$  ist invertierbar gdw. sie bijektiv ist

Beweis (1/2).

beidseitige Implikationen:

( $\rightarrow$ ) Sei  $f$  invertierbar, d.h. es existiert  $g: N \rightarrow M$ , so dass  
 $f ; g = \text{id}_M$  und  $g ; f = \text{id}_N$ .

- **Injektivität per Kontraposition:** Seien  $m, m' \in M$ , so dass  $f(m) = f(m')$ . Z.zg.  $m = m'$ . Es gilt

$$\begin{aligned}m &= \text{id}_M(m) = (f ; g)(m) = g(f(m)) \\&= g(f(m')) = (f ; g)(m') = \text{id}_M(m') = m'\end{aligned}$$

- **Surjektivität:** Sei  $n \in N$  beliebig. Dann ist  $f(g(n)) = (g ; f)(n) = \text{id}_N(n) = n$ . Also existiert nach §4.9 ein  $m \in M$ , so dass  $g(n) = m$  und  $f(m) = n$ .

Beweis (2/2).

beidseitige Implikationen:

( $\leftarrow$ ) Sei  $f$  bijektiv. Wir definieren die Relation  $g \subseteq N \times M$  durch  $g = f^{-1}$ . Zunächst zeigen wir, dass  $g$  eine Funktion ist.

- Sei  $n \in N$  beliebig. Da  $f$  surjektiv ist, existiert  $m \in M$  mit  $f(m) = n$ . Also  $(n, m) \in g$ .
- Seien  $(n, m) \in g$  und  $(n, m') \in g$ . Folglich gilt  $f(m) = n = f(m')$  und gemäß der Kontraposition der Injektivität von  $f$  folgt  $m = m'$ .

Z.zg.  $f ; g = \text{id}_M$  und  $g ; f = \text{id}_N$ . Für jedes  $m \in M$  und  $n \in N$  gelten

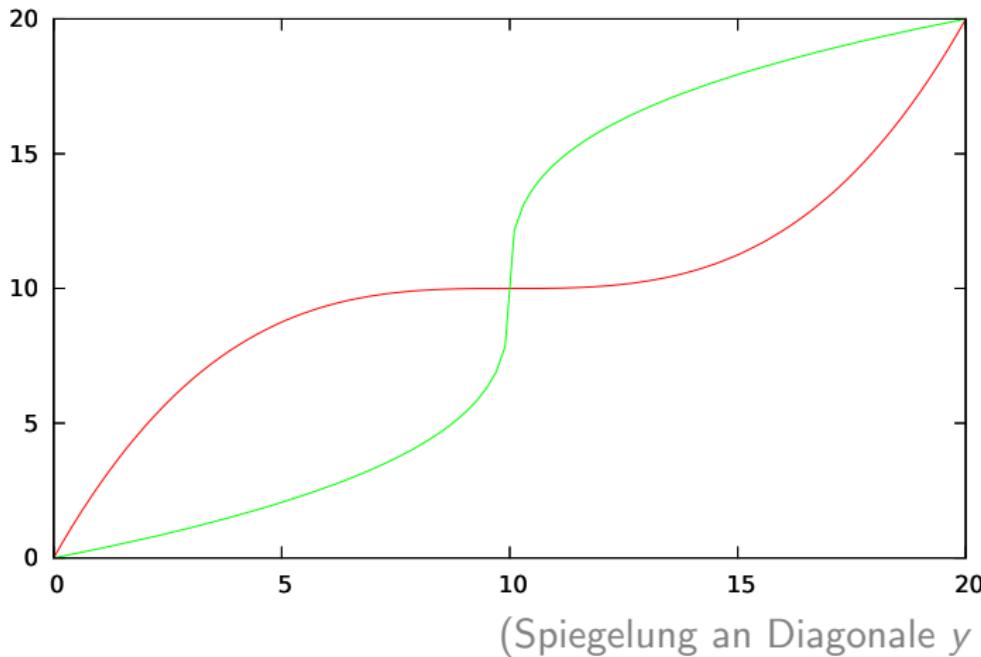
$$(f ; g)(m) = f^{-1}(f(m)) = m \quad \text{und}$$

$$(g ; f)(n) = f(f^{-1}(n)) = n$$

denn  $m \in f^{-1}(\{f(m)\})$  und  $f(f^{-1}(\{n\})) = \{n\}$  [§5.5]. □

## Notizen

- jede Verschlüsselungsfunktion  $f$  ist invertierbar
- aber die Berechnung einer inversen Funktion  $g$  ist "schwierig"



## §5.8 Theorem

Sei  $f: M \rightarrow N$  und seien  $g, g': N \rightarrow M$  mit

$$f ; g = \text{id}_M$$

$$f ; g' = \text{id}_M$$

$$g ; f = \text{id}_N$$

$$g' ; f = \text{id}_N$$

Dann gilt  $g = g'$

(Eindeutigkeit des Inversen)

Beweis.

*Direkt:*

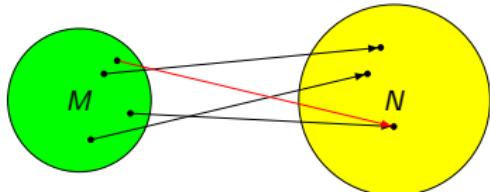
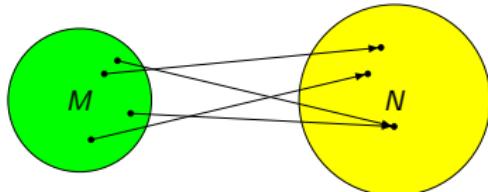
$$\begin{aligned}g &= g ; \text{id}_M = g ; (f ; g') \\&= (g ; f) ; g' = \text{id}_N ; g' = g'\end{aligned}$$

wobei wir die Assoziativität der Komposition (§5.3) nutzen. □

Auswahlaxiom

## Motivation

- betrachten wir §5.7 noch einmal ohne **injektiv**  
(abgeschwächte Aussage; nur eine Richtung)
- passen Beweis entsprechend an



## §5.9 Theorem [nutzt Auswahlaxiom]

Wenn eine Funktion  $f: M \rightarrow N$  surjektiv ist, dann existiert eine Funktion  $g: N \rightarrow M$ , so dass  $g ; f = \text{id}_N$

Beweis.

Sei  $n \in N$  beliebig. Da  $f$  surjektiv ist, existiert  $m \in M$  mit  $f(m) = n$ . Also  $f^{-1}(\{n\}) \neq \emptyset$ . Für jedes  $n \in N$  wähle ein  $m_n \in f^{-1}(\{n\})$ .

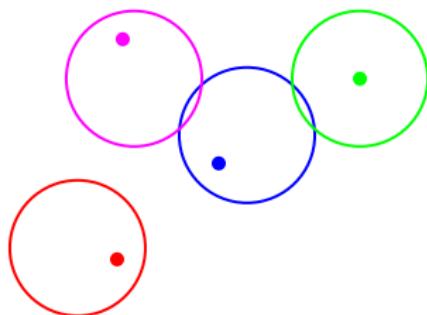
Wir definieren die Funktion  $g: N \rightarrow M$  durch  $g(n) = m_n$ .  
Z.zg.  $g ; f = \text{id}_N$ . Für alle  $n \in N$  gilt

$$(g ; f)(n) = f(g(n)) = f(m_n) = n = \text{id}_N(n)$$

denn  $f(f^{-1}(\{n\})) = \{n\}$  nach §5.5.

□

Illustration der nichtleeren Mengen  $f^{-1}(\{n\})$  mit Auswahl:



## Notizen

- diese offenbar einfache Auswahl ist **nicht** trivial
- ist aber allg. akzeptiert in der Mathematik
- Nutzung aber bitte kennzeichnen

### §5.10 Axiom (Auswahlaxiom; ZERMELO 1904)

Für jede Menge  $\mathcal{X}$  von nichtleeren Mengen gibt es eine Funktion  $c: \mathcal{X} \rightarrow \bigcup \mathcal{X}$ , so dass  $f(X) \in X$  für alle  $X \in \mathcal{X}$

### ERNST ZERMELO (\* 1871; † 1953)

- dtsch. Logiker und Mathematiker
- Begründer der axiomatischen Mengenlehre
- Schach hat eine endliche Lösung



© Konrad Jacobs

# Funktionen — Auswahlaxiom

Theorem (§5.9 jetzt nochmal mit Auswahlaxiom)

Wenn eine Funktion  $f: M \rightarrow N$  surjektiv ist, dann existiert eine Funktion  $g: N \rightarrow M$ , so dass  $g ; f = \text{id}_N$

Beweis.

Sei  $n \in N$  beliebig. Da  $f$  surjektiv ist, existiert  $m \in M$  mit  $f(m) = n$ . Also  $f^{-1}(\{n\}) \neq \emptyset$ . Sei  $\mathcal{M} = \{f^{-1}(\{n\}) \mid n \in N\}$ . Offensichtlich  $\emptyset \notin \mathcal{M}$  und  $\bigcup \mathcal{M} = M$ . Aufgrund des Auswahlaxioms existiert eine Funktion  $c: \mathcal{M} \rightarrow M$ , so dass  $c(M') \in M'$  für alle  $M' \in \mathcal{M}$ .

Wir definieren die Funktion  $g: N \rightarrow M$  durch  $g(n) = c(f^{-1}(\{n\}))$  für alle  $n \in N$ . Z.zg.  $g ; f = \text{id}_N$ . Für alle  $n \in N$  gilt

$$(g ; f)(n) = f(g(n)) = f(c(f^{-1}(\{n\}))) = n = \text{id}_N(n)$$

denn  $f(f^{-1}(\{n\})) = \{n\}$  nach §5.5. □

## Notizen

- **AC** = Auswahlaxiom (*axiom of choice*)
- **Axiom** ist eine Grundannahme (unbewiesen)
- man kann AC also glauben oder eben nicht

Begriff: Axiom

## §5.11 PEANO-Axiome der natürlichen Zahlen

Die **natürlichen Zahlen** sind ein System  $(N, s, z)$ , so dass

- ①  $z \in N$  und  $s: N \rightarrow N$  injektiv
- ②  $z \notin s(N)$
- ③ jede Teilmenge  $N' \subseteq N$ , so dass
  - $z \in N'$  und
  - $n \in N' \rightarrow s(n) \in N'$  für alle  $n \in N'$

gelten, erfüllt  $N' = N$

### GUISSEPPE PEANO (\* 1858; † 1932)

- ital. Mathematiker und Logiker
- Begründer der axiomatischen Mengenlehre
- Formalisierung der vollständigen Induktion



## Beispiel (§5.11)

Das System  $(\mathbb{N}, \text{nachfolger}, 0)$  mit  $\text{nachfolger}(n) = n + 1$  für alle  $n \in \mathbb{N}$  erfüllt die PEANO-Axiome:

- ①  $0 \in \mathbb{N}$  und  $\text{nachfolger}: \mathbb{N} \rightarrow \mathbb{N}$  ist injektiv ✓  
 $(n \neq n' \text{ impliziert } n + 1 \neq n' + 1)$
- ②  $0 \notin \text{nachfolger}(\mathbb{N})$  ✓  
 $(0 \neq n + 1 \text{ für alle } n \in \mathbb{N})$
- ③ jede Teilmenge  $N' \subseteq \mathbb{N}$ , so dass
  - $0 \in N'$  und
  - $n \in N' \rightarrow (n + 1) \in N'$  für alle  $n \in \mathbb{N}$gelten, erfüllt  $N' = \mathbb{N}$  ✓  
(Prinzip der vollständigen Induktion)

## Beispiel (§5.11)

Das System  $(\mathbb{Z}, \text{nachfolger}, 0)$  mit  $\text{nachfolger}(z) = z + 1$  für alle  $z \in \mathbb{Z}$  erfüllt die PEANO-Axiome **nicht**:

- ①  $0 \in \mathbb{Z}$  und  $\text{nachfolger}: \mathbb{Z} \rightarrow \mathbb{Z}$  ist injektiv ✓  
 $(z \neq z' \text{ impliziert } z + 1 \neq z' + 1)$
- ②  $0 \notin \text{nachfolger}(\mathbb{Z})$  ist falsch ✗  
 $(\text{da } -1 + 1 = 0)$
- ③ jede Teilmenge  $Z' \subseteq \mathbb{Z}$ , so dass
  - $0 \in Z'$  und
  - $z \in Z' \rightarrow (z + 1) \in Z'$  für alle  $z \in \mathbb{Z}$geltten, erfüllt  $Z' = \mathbb{Z}$  ist falsch ✗  
 $(\text{z.B. für } Z' = \mathbb{N})$

## Beispiel (§5.11)

Das System  $(\mathbb{R}_{\geq 0}, \text{nachfolger}, 0)$  mit  $\text{nachfolger}(r) = r + 1$  für alle  $r \in \mathbb{R}_{\geq 0}$  erfüllt die PEANO-Axiome **nicht**:

- ①  $0 \in \mathbb{R}_{\geq 0}$  und  $\text{nachfolger}: \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$  ist injektiv ✓  
 $(r \neq r' \text{ impliziert } r + 1 \neq r' + 1)$
- ②  $0 \notin \text{nachfolger}(\mathbb{R}_{\geq 0})$  ✓  
 $(\text{da } r + 1 \neq 0 \text{ für alle } r \in \mathbb{R}_{\geq 0})$
- ③ jede Teilmenge  $R' \subseteq \mathbb{R}_{\geq 0}$ , so dass
  - $0 \in R'$  und
  - $r \in R' \rightarrow (r + 1) \in R'$  für alle  $r \in \mathbb{R}_{\geq 0}$gelten, erfüllt  $R' = \mathbb{R}_{\geq 0}$  ist falsch ✗  
 $(\text{z.B. für } R' = \mathbb{N})$

## Notizen

- auch für die Mengenlehre gibt es Axiome
- **Klassiker:**
  - ZERMELO-FRAENKEL (ZF)
  - ZERMELO-FRAENKEL mit Auswahlaxiom (ZFC)
- basierend auf diesen Axiomen und der Logik  
kann man die klassische Theorie der nat. Zahlen entwickeln

ABRAHAM FRAENKEL (\* 1891; † 1965)

- dtsch.-isra. Mathematiker und Logiker
- Begründer der axiomatischen Mengenlehre
- ergänzte das Auswahlaxiom



Rückblick: Ordnungsrelationen

## Definition (§4.14)

Eine Relation  $\preceq$  auf  $M$  ist eine **Ordnungsrelation**  
gdw. sie reflexiv, antisymmetrisch und transitiv ist.

- $(\forall m \in M). m \preceq m$  reflexiv
- $(\forall m, m' \in M). ((m \preceq m' \wedge m' \preceq m) \rightarrow m = m')$  antisymmetrisch
- $(\forall m, m', m'' \in M). ((m \preceq m' \wedge m' \preceq m'') \rightarrow m \preceq m'')$  transitiv

Das Paar  $(M, \preceq)$  heißt dann **teilweise geordnete Menge**.

Ist  $\preceq$  linear, dann heißt  $(M, \preceq)$  auch **linear geordnete Menge**.

- $(\forall m, m' \in M). (m \preceq m' \vee m' \preceq m)$  linear

## §5.12 Definition (Teilkette)

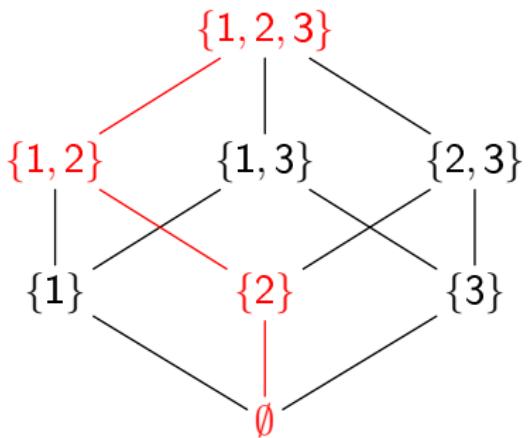
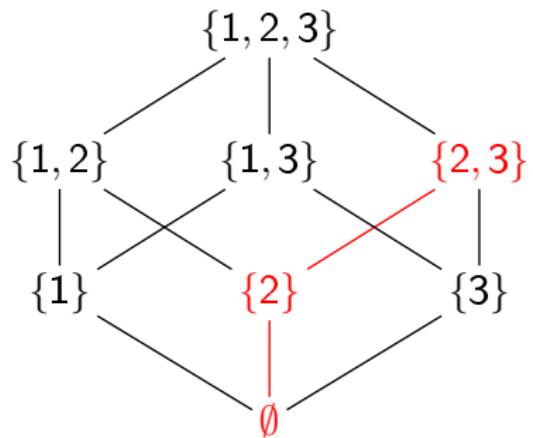
Sei  $(M, \preceq)$  eine teilweise geordnete Menge. Eine Teilmenge  $M' \subseteq M$  ist eine **Teilkette** von  $(M, \preceq)$  gdw.  $m' \preceq m''$  oder  $m'' \preceq m'$  für alle  $m', m'' \in M'$ .

(alternativ:  $(M', \preceq \cap (M' \times M'))$  ist linear geordnet)

## Beispiele

- $\mathbb{N}$  ist eine Teilkette von  $(\mathbb{Z}, \leq)$
- $\{\emptyset, \{1\}, \{1, 2\}\}$  ist eine Teilkette von  $(\mathcal{P}(\{1, 2\}), \subseteq)$
- $\{\{1\}, \{2\}\}$  ist **keine** Teilkette von  $(\mathcal{P}(\{1, 2\}), \subseteq)$

# Relationen — Ordnungsrelationen



## §5.13 Definition (obere Schranke, maximale und größte Elemente)

Sei  $(M, \preceq)$  eine teilweise geordnete Menge.

Ein Element  $m \in M$  ist

- eine **obere Schranke für  $M' \subseteq M$**  [bzgl.  $(M, \preceq)$ ]  
gdw.  $m' \preceq m$  für alle  $m' \in M'$   
(größer als alle Elemente aus  $M'$ )
- **maximal** [bzgl.  $(M, \preceq)$ ]  
gdw.  $m \not\preceq m'$  für alle  $m' \in M$  mit  $m' \neq m$   
(es gibt keine echt größeren Elemente)
- **das größte Element von  $M' \subseteq M$**  [bzgl.  $(M, \preceq)$ ]  
gdw.  $m \in M'$  und  $m$  obere Schranke für  $M'$  ist  
(obere Schranke von  $M'$ , die in  $M'$  liegt)

## Beispiele

- $\mathbb{N}$  hat **keine** obere Schranke bzgl.  $(\mathbb{Z}, \leq)$   
kein größtes Element in  $\mathbb{N}$ ; keine maximalen Elemente  
 $\{-1, 3\}$  hat obere Schranken (z.B. 4) und  
ein größtes Element 3
- bzgl.  $(\mathcal{P}(\{1, 2\}), \subseteq)$  ist  
 $\{1, 2\}$  das größte Element von  $M = \{\{1\}, \{1, 2\}\}$   
(auch obere Schranke von  $M$  und maximal)
- bzgl.  $(\mathcal{P}(\{1, 2\}), \subseteq)$  ist  
 $\{1, 2\}$  obere Schranke von  $M = \{\{1\}, \{2\}\}$   
( $M$  hat kein größtes Element)

## §5.14 Theorem (ZORNS Lemma)

Sei  $(M, \preceq)$  eine teilweise geordnete Menge, in der jede Teilkette eine obere Schranke hat. Dann hat  $(M, \preceq)$  ein maximales Element.

MAX AUGUST ZORN (\* 1906; † 1993)

- dtsch. Mathematiker
- Algebra, Gruppentheorie, Analysis
- vereinfachte Wohlordnungssatz



© Gerhard Hund

## §5.15 Definition (wohlgeordnet)

Eine **wohlgeordnete** Menge  $(M, \preceq)$  ist eine linear geordnete Menge, so dass jede nicht-leere Teilmenge  $M' \subseteq M$  ein größtes Element hat  
(traditionell: kleinstes Element)

## §5.16 Theorem (Wohlordnungssatz)

Jede Menge  $M$  kann wohlgeordnet werden;  
d.h. es existiert eine wohlgeordnete Menge  $(M, \preceq)$

## §5.17 Theorem (HAUSDORFF 1914)

Sei  $(M, \preceq)$  eine teilweise geordnete Menge.

Jede Teilkette ist in einer maximalen Teilkette enthalten.

(eine Teilkette ist maximal,  
wenn jede größere Teilmenge keine Teilkette mehr ist)

FELIX HAUSDORFF (\* 1868; † 1942)

- dtsch. Mathematiker
- Mengenlehre, Topologie, Funktionsanalysis
- Professor der Universität Leipzig



## §5.18 Theorem

Der Wohlordnungssatz impliziert das Auswahlaxiom (in ZF)

Beweis.

Sei  $\mathcal{M}$  eine Menge von Mengen, so dass  $\emptyset \notin \mathcal{M}$ . Des Weiteren sei  $M = \bigcup \mathcal{M}$ . Aufgrund des Wohlordnungssatzes existiert eine wohlgeordnete Menge  $(M, \preceq)$ . Für jedes  $M' \in \mathcal{M}$  definieren wir  $c: \mathcal{M} \rightarrow M$  durch

$$c(M') = m \quad \text{wobei } m \text{ das größte Element von } M' \text{ bzgl. } (M, \preceq) \text{ ist}$$
$$c(M') = \max_{\preceq} M'$$

Aufgrund der Wohlordnung existieren die größten Elemente (und diese sind eindeutig) und es gilt  $c(M') \in M'$ . □

## Notizen

- Auswahlaxiom ist unabhängig von ZF
- ZF konsistent  $\rightarrow$  ZFC konsistent [GÖDEL 1940]  
(Negation von AC lässt sich nicht aus ZF ableiten)
- ZF konsistent  $\rightarrow$  ZF( $\neg$ C) konsistent [COHEN 1963]  
(AC lässt sich nicht aus ZF ableiten)

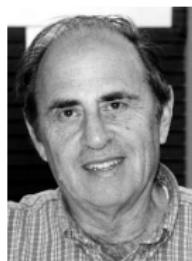
## KURT GÖDEL (\* 1906; † 1978)

- öster.-amerik. Logiker und Mathematiker
- prominentester Logiker des 20. Jhd.
- Unvollständigkeitstheoreme  
(siehe *Berechenbarkeit*)



## PAUL JOSEPH COHEN (\* 1934; † 2007)

- amerik. Mathematiker
- beherrschte viele Gebiete der Mathematik
- Unabhängigkeit von CH und AC



- Eigenschaften von Funktionen
- Invertierung von Funktionen
- Auswahlaxiom
- PEANO-Axiome der natürlichen Zahlen

# Diskrete Strukturen

## Vorlesung 6: Kardinalitäten

Andreas Maletti

18. November 2014

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## heutige Vorlesung

- ① Fixpunkte von Funktionen
- ② Kardinalität von Mengen
- ③ Grundwissen über Kardinalitäten
- ④ Endlichkeit & Abzählbarkeit

Bitte Fragen direkt stellen!

Ordnungen und Funktionen

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## Definition (§5.13 — spezielle Elemente in Ordnungsrelationen)

Sei  $(M, \preceq)$  eine teilweise geordnete Menge.

Ein Element  $m \in M$  ist

- eine **obere Schranke für  $M' \subseteq M$**  [bzgl.  $(M, \preceq)$ ]  
gdw.  $m' \preceq m$  für alle  $m' \in M'$   
(größer als alle Elemente aus  $M'$ )
- **maximal** [bzgl.  $(M, \preceq)$ ]  
gdw.  $m \not\preceq m'$  für alle  $m' \in M$  mit  $m' \neq m$   
(es gibt keine echt größeren Elemente)
- **das größte Element von  $M' \subseteq M$**  [bzgl.  $(M, \preceq)$ ]  
gdw.  $m \in M'$  und  $m$  obere Schranke für  $M'$  ist  
(obere Schranke für  $M'$ , die in  $M'$  liegt)

## Motivation

- Iteration ein wesentliches Prinzip der Programmierung
- Fixpunkte mathematische Variante von Iteration

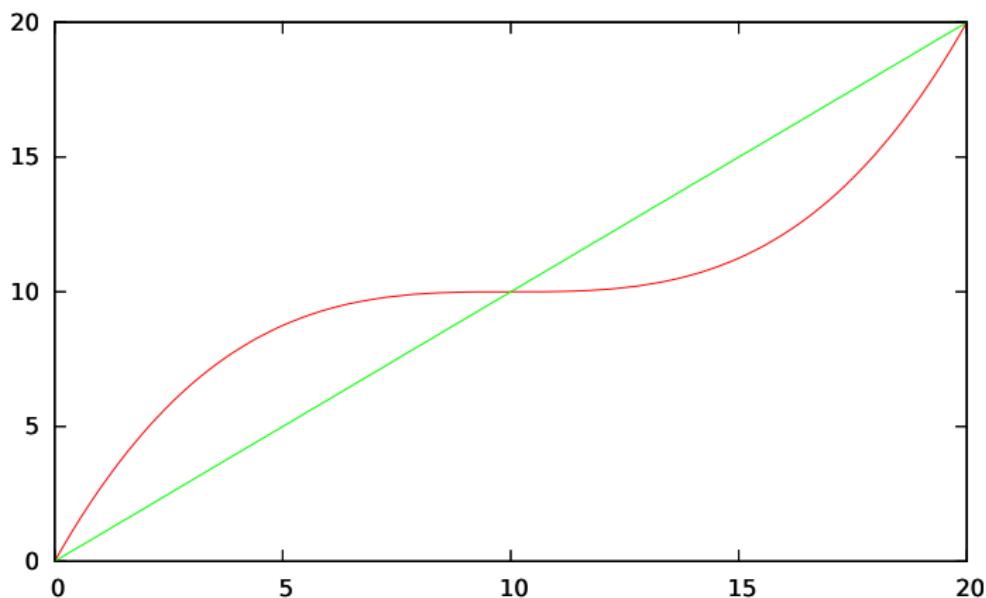
## §6.1 Definition (Fixpunkt)

Sei  $f: M \rightarrow M$  eine Funktion auf  $M$ . Ein **Fixpunkt von  $f$**  ist ein Element  $m \in M$ , so dass  $f(m) = m$ .

## Beispiele

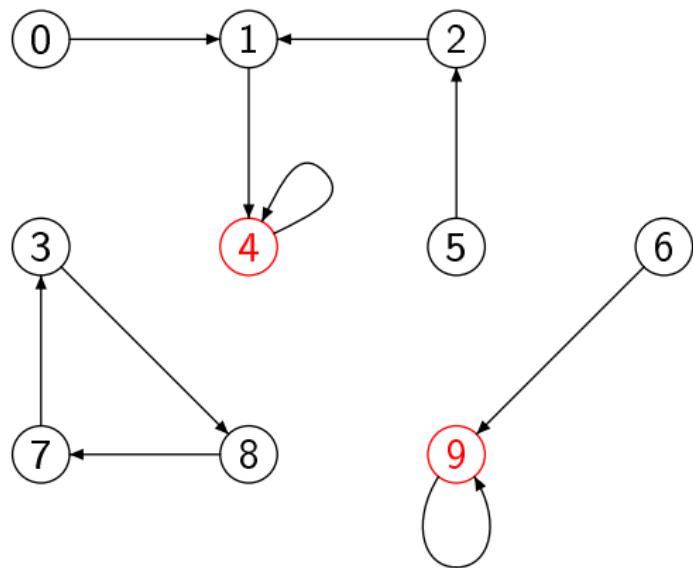
- **nachfolger**:  $\mathbb{N} \rightarrow \mathbb{N}$  hat **keine** Fixpunkte
- $f: \mathbb{N} \rightarrow \mathbb{N}$  mit  $f(n) = \lceil \sqrt{n} \rceil$  für alle  $n \in \mathbb{N}$  hat Fixpunkte 0, 1 und 2

# Funktionen — Fixpunkte



Fixpunkte = Schnittpunkte mit Diagonale  $y = x$

# Funktionen — Fixpunkte



(Fixpunkte haben Schleifen)

## §6.2 Theorem

Sei  $\mathcal{M} \subseteq \mathcal{P}(M)$  für eine Menge  $M$  und sei

$$\mathcal{S} = \{M' \subseteq M \mid M' \text{ ist obere Schranke für } \mathcal{M} \text{ bzgl. } \subseteq\}$$

die Menge aller oberen Schranken für  $\mathcal{M}$ .

Dann gilt  $\bigcup \mathcal{M} \subseteq \mathcal{S}$  für alle  $S \in \mathcal{S}$

(anders:  $\bigcup \mathcal{M}$  ist kleinste obere Schranke)

### Beweis.

Sei  $S \in \mathcal{S}$  eine obere Schranke für  $\mathcal{M}$  und sei  $m \in \bigcup \mathcal{M}$  beliebig.

Nach §3.4 existiert  $M' \in \mathcal{M}$ , so dass  $m \in M'$ .

Da  $S$  obere Schranke für  $\mathcal{M}$  ist, gilt  $M' \subseteq S$  und damit  $m \in S$ .  $\square$

## §6.3 Theorem (KNASTER-TARSKI Lemma)

Sei  $f: \mathcal{P}(M) \rightarrow \mathcal{P}(M)$  mit  $f(M') \subseteq f(M'')$  für alle  $M' \subseteq M'' \subseteq M$ . Dann hat  $f$  einen Fixpunkt.

Beweis.

Seien  $P = \{M'' \subseteq M \mid M'' \subseteq f(M'')\}$  und  $N = \bigcup P$ . Für jede Teilmenge  $M'' \in P$  gilt offensichtlich  $M'' \subseteq N$ . Nach Annahme gilt also  $f(M'') \subseteq f(N)$  und damit

$$M'' \subseteq f(M'') \subseteq f(N) ,$$

womit  $f(N)$  eine obere Schranke von  $P$  bzgl.  $(\mathcal{P}(M), \subseteq)$  ist.

Nach §6.2 ist  $N = \bigcup P \subseteq f(N)$ , denn  $f(N)$  ist eine obere Schranke von  $P$ . Also auch  $f(N) \subseteq f(f(N))$  nach Annahme, wodurch  $f(N) \in P$ . Demzufolge gilt auch  $f(N) \subseteq \bigcup P = N$  und zusammen mit  $N \subseteq f(N)$  erhalten wir  $N = f(N)$  und damit den Fixpunkt  $N$ .

□

## BRONISŁAW KNASTER (\* 1893; † 1980)

- poln. Mathematiker
- Topologie und faires Kuchenschneiden
- Doktorand von STEFAN MAZURKIEWICZ



© Konrad Jacobs

## ALFRED TARSKI (\* 1901; † 1983)

- poln.-amerik. Logiker und Mathematiker
- Modelltheorie und algebraische Logik
- Fixpunktsätze



© George M. Bergman

## Beispiele

- nachfolger:  $\mathbb{N} \rightarrow \mathbb{N}$  hat **keine** Fixpunkte
- für welche Teilmengen  $N \subseteq \mathbb{N}$  gilt  $\text{nachfolger}(N) = N$ ?  
für  $N = \emptyset$
- sei  $\text{nachfolger}' : \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ , so dass für alle  $N \subseteq \mathbb{N}$   
 $\text{nachfolger}'(N) = N \cup \{\text{nachfolger}(n) \mid n \in N\}$
- für welche Teilmengen  $N \subseteq \mathbb{N}$  gilt  $\text{nachfolger}'(N) = N$ ?  
für  $N \in \{\emptyset, \mathbb{N}\}$

## §6.4 Theorem

Sei  $f: M \rightarrow N$  und  $M' \subseteq M'' \subseteq M$

- ①  $f(M') \subseteq f(M'')$
- ②  $M \setminus M'' \subseteq M \setminus M'$

Beweis.

- ① Sei  $n \in f(M')$ . Dann existiert  $m \in M'$ , so dass  $f(m) = n$ . Da  $M' \subseteq M''$  gilt auch  $m \in M''$  und damit  $n \in f(M'')$ .
- ② Sei  $m \in M \setminus M''$ . Dann ist  $m \in M$ , aber  $m \notin M''$ . Da  $m \notin M''$  gilt auch  $m \notin M'$  (Kontraposition von  $M' \subseteq M''$ ) und somit  $m \in M \setminus M'$ .

□

## §6.5 Theorem (CANTOR-SCHRÖDER-BERNSTEIN-Theorem)

Seien  $f: M \rightarrow N$  und  $g: N \rightarrow M$  injektive Funktionen.

Dann existiert eine bijektive Funktion  $B: M \rightarrow N$ .

Beweis (1/3).

Wir definieren  $h: \mathcal{P}(M) \rightarrow \mathcal{P}(M)$ , so dass für alle  $M' \subseteq M$

$$h(M') = M \setminus g(N \setminus f(M'))$$

Vermittels §6.4 gilt  $h(M') \subseteq h(M'')$  für alle  $M' \subseteq M'' \subseteq M$ .

Damit existiert Fixpunkt  $F \subseteq M$  (d.h.  $h(F) = F$ ) nach §6.3 und

$$M \setminus F = M \setminus h(F) = M \setminus (M \setminus g(N \setminus f(F))) = g(N \setminus f(F))$$

Wir definieren  $B \subseteq M \times N$

$$B = \{(m, n) \in f \mid m \in F\} \cup \{(m, n) \in g^{-1} \mid m \in M \setminus F\}$$

und z.zg. ist, dass  $B$  die gewünschte bijektive Funktion ist.

## Beweis (2/3).

- **def. für jedes  $m \in M$ :** Falls  $m \in F$ , dann gilt  $(m, f(m)) \in B$ .  
Sonst ist  $m \in M \setminus F = g(N \setminus f(F))$ , also existiert  
 $n \in N \setminus f(F)$ , so dass  $g(n) = m$ , und damit  $(m, n) \in B$ .
- **Eindeutigkeit:** Seien  $(m, n) \in B$  und  $(m, n') \in B$ . Falls  
 $m \in F$ , dann gilt  $n = f(m) = n'$ . Andernfalls gilt  
 $g(n) = m = g(n')$  und aufgrund der (Kontraposition der)  
Injektivität von  $g$  gilt auch dann  $n = n'$ .

→  $B$  ist eine Funktion

$$B = \{(m, n) \in f \mid m \in F\} \cup \{(m, n) \in g^{-1} \mid m \in M \setminus F\}$$
$$M \setminus F = g(N \setminus f(F))$$

Beweis (3/3).

- **surjektiv:** Sei  $n \in N$ . Falls  $n \in f(F)$ , dann existiert  $m \in F$ , so dass  $f(m) = n$ . Damit gilt  $B(m) = n$ . Sonst  $n \in N \setminus f(F)$  und damit  $g(n) \in g(N \setminus f(F)) = M \setminus F$ . Also ist  $B(g(n)) = n$ .
- **injektiv:** (Kontrapos.) Seien  $m, m' \in M$  mit  $B(m) = B(m')$ . Z.zg.  $m = m'$ .
  - Sei  $B(m) \in f(F)$ . Existiere  $m'' \in \{m, m'\}$  mit  $m'' \in M \setminus F$ , dann existiert auch  $n \in N \setminus f(F)$  mit  $g(n) = m''$  da  $M \setminus F = g(N \setminus f(F))$ . Damit gilt  $B(m'') = n \in N \setminus f(F)$ , was jedoch  $B(m'') \in f(F)$  widerspricht. Also gilt  $m, m' \in F$ . Damit gilt jedoch auch  $m \neq m'$ , da  $f$  injektiv ist.
  - Sei  $B(m) \notin f(F)$ . Dann  $m, m' \in M \setminus F$ . Also gilt  $m = g(B(m)) = g(B(m')) = m'$ .

→  $B$  ist eine bijektive Funktion



$$B = \{(m, n) \in f \mid m \in F\} \cup \{(m, n) \in g^{-1} \mid m \in M \setminus F\}$$

$$M \setminus F = g(N \setminus f(F))$$

## ERNST SCHRÖDER (\* 1841; † 1902)

- dtsch. Mathematiker
- algebraische Logik
- Verfechter der formalen Logik



## FELIX BERNSTEIN (\* 1878; † 1956)

- dtsch. Mathematiker
- Grundlagen der Mengenlehre
- Doktorand von CANTOR
- Blutgruppenvererbung



Kardinalität

## Motivation

- bisher intuitive Größe von Mengen  
(Anzahl der Elemente oder  $\geq \infty$  für unendliche Mengen)  
→ **höchst ungenau**, da  $|\mathbb{N}| \geq \infty \leq |\mathbb{R}|$
- es gibt sogar unendlich viele “Unendlichkeiten”
- aber die **Kardinalitäten** (Mächtigkeiten) sind linear geordnet  
(nutzt Auswahlaxiom)

## §6.6 Definition

Zwei Mengen  $M$  und  $N$  sind **gleichmächtig** (kurz:  $|M| = |N|$ ) gdw. eine bijektive Funktion  $f: M \rightarrow N$  existiert

## Beispiele

- $|\emptyset| \neq |M|$  für alle nichtleeren Mengen  $M$
- $|\{1, 2, 3\}| = |\{6, 9, 11\}|$  via  $\{(1, 6), (2, 9), (3, 11)\}$
- $|\mathbb{Z}| = |\mathbb{N}|$  vermittels  $f: \mathbb{Z} \rightarrow \mathbb{N}$ ; für alle  $z \in \mathbb{Z}$  (Übung)

$$f(z) = \begin{cases} 2z & \text{falls } z \geq 0 \\ -(2z + 1) & \text{sonst} \end{cases}$$

( $\mathbb{Z}$  und  $\mathbb{N}$  sind gleichmächtig)

## Notizen

- Gleichmächtigkeit ist eine Äquivalenzrelation → Übung
- ihre Äquivalenzklassen heißen **Kardinalitäten**  
(auch: Mächtigkeiten oder Kardinalzahlen)
- die Kardinalitäten endlicher Mengen entsprechen den nat. Zahlen
- die Kardinalitäten unendlicher Mengen erkunden wir gleich

## §6.7 Theorem

$$|\mathbb{Q}| = |\mathbb{Z}|$$

( $\mathbb{Q}$  und  $\mathbb{Z}$  sind gleichmächtig)

Beweis.

Nach §6.5 reicht die Angabe zweier injektiver Funktionen  $f: \mathbb{Q} \rightarrow \mathbb{Z}$  und  $g: \mathbb{Z} \rightarrow \mathbb{Q}$ . Sei  $g(z) = z$  für alle  $z \in \mathbb{Z}$ . Dann ist  $g$  offensichtlich injektiv (aber nicht surjektiv).

Wir konstruieren  $f: \mathbb{Q} \rightarrow \mathbb{Z}$  für alle  $m, n \in \mathbb{Z}$  mit  $n \neq 0$ :

$$f\left(\frac{m}{n}\right) = \begin{cases} 2^{|m|} \cdot 3^{|n|} & \text{falls } \frac{m}{n} \geq 0 \\ -(2^{|m|} \cdot 3^{|n|}) & \text{sonst} \end{cases}$$

**injektiv:** (Kontrapos.) Seien  $m, m', n, n' \in \mathbb{Z}$  mit  $f\left(\frac{m}{n}\right) = f\left(\frac{m'}{n'}\right)$ .

Dann sind  $2^{|m|} \cdot 3^{|n|}$  und  $2^{|m'|} \cdot 3^{|n'|}$  offenbar Primfaktorzerlegungen von  $|f\left(\frac{m}{n}\right)| = |f\left(\frac{m'}{n'}\right)|$ . Nach dem Fundamentalsatz der Arithmetik ist die Zerlegung eindeutig, also gelten  $m = m'$  und  $n = n'$ .  $\square$

## §6.8 Theorem

$$|\mathbb{N}| \neq |\mathbb{R}|$$

( $\mathbb{N}$  und  $\mathbb{R}$  sind nicht gleichmächtig)

Beweis.

Indirekt. Sei  $|\mathbb{N}| = |\mathbb{R}|$ . Dann existiert eine bijektive Funktion  $b: \mathbb{N} \rightarrow \mathbb{R}$ . Schreibe Bilder als Dezimalzahlen:

$$b(0) = a_0, d_{00} d_{01} d_{02} \dots d_{0n}$$

$$b(1) = a_1, d_{10} d_{11} d_{12} \dots d_{1n}$$

$$b(2) = a_2, d_{20} d_{21} d_{22} \dots d_{2n}$$

...

$$b(n) = a_n, d_{n0} d_{n1} d_{n2} \dots d_{nn}$$

...

$$a_i \in \mathbb{Z}; d_{ij} \in \{0, 1, \dots, 9\}$$

Für jedes  $i \in \mathbb{N}$ , sei  $d_i \in \{0, 1, \dots, 9\}$ , so dass  $d_i \neq d_{ii}$ . Da  $b$  surjektiv ist, gibt es  $n \in \mathbb{N}$ , so dass  $b(n) = 0, d_1 d_2 d_3 \dots$  Dann gilt aber  $d_n = d_{nn}$  entgegen der Wahl von  $d_n \neq d_{nn}$ . Widerspruch! □

## Exkurs

- Gleichmächtigkeit  $\underline{\underline{=}} = \{(M, N) \mid |M| = |N|\}$   
ist eine Äquivalenzrelation
  - $\underline{\underline{=}}$  ist eine Teilmenge von  $\mathcal{M} \times \mathcal{M}$  für eine Menge  $\mathcal{M}$
- Was ist  $\mathcal{M}$ ?
- da wir beliebige Mengen vergleichen möchten,  
müsste dies die Menge  $\mathcal{M}$  aller Mengen sein

## §6.9 Problem (siehe §2.6)

Die Menge  $\mathcal{M}$  aller Mengen ist nicht wohldefiniert.

- für jede Menge  $M$  gilt entweder  $M \in \mathcal{M}$  oder  $M \notin \mathcal{M}$
- Sei  $\mathcal{M} \in \mathcal{M}$ . Dann gilt unsinnigerweise  $\mathcal{M} \neq \mathcal{M}$ ,  
denn jede Menge ist verschieden von ihren Elementen
- Sei  $\mathcal{M} \notin \mathcal{M}$ . Dann ist  $\mathcal{M}$  nicht die Menge aller Mengen,  
denn sie enthält die Menge  $\mathcal{M}$  nicht

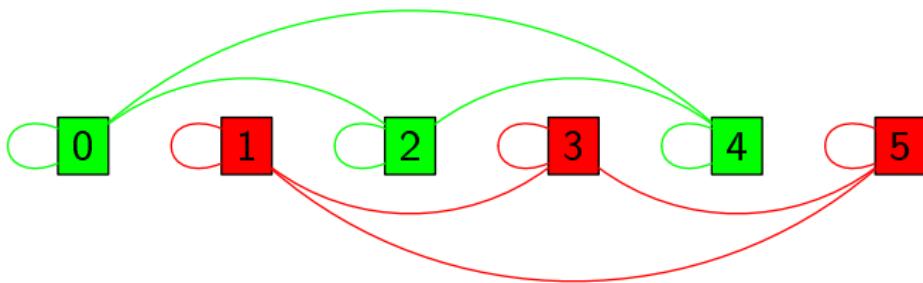
## Naive Mengenlehre

- Problem §6.9 zeigt Grenze unserer naiven Mengenlehre auf
- $\equiv$  hat die wesentlichen Eigenschaften einer Äquivalenzrelation
- aber keine geeignete Grundmenge
- wir ignorieren dies allerdings im Folgenden  
(genauer in der axiomatischen Mengenlehre)

Ordnung der Kardinalitäten

## Motivation

- man möchte evtl. Funktionen oder Relationen über Äquivalenzklassen definieren  
(z.B. Ordnung der Kardinalitäten)
- dies macht man oft mit Hilfe der Repräsentanten
- dabei muss man allerdings die Wohldefiniertheit nachweisen



## Beispiele

Sei  $\equiv$  obige Äquivalenzrelation

- ①  $[i] \prec [j]$  gdw.  $i < j$  ist **nicht** wohldefiniert,  
denn  $[1] \prec [2]$  aber  $[1] \not\prec [0]$  obwohl  $[2] = [0]$   
Definition ist nicht repräsentantenunabhängig
- ②  $[i] \prec [j]$  gdw. ungerade Zahl  $z \in \mathbb{Z}$  existiert, so dass  $i = j + z$   
ist wohldefiniert, denn **repräsentantenunabhängig** ( $\rightarrow$  Übung)

## §6.10 Definition

Die Menge  $N$  ist **mächtiger als** die Menge  $M$  (kurz:  $|M| \leq |N|$ )  
(genauer: die Mächtigkeit von  $N$  ist größer als die von  $M$ )  
gdw. eine injektive Funktion  $f: M \rightarrow N$  existiert.

## §6.11 Repräsentantenunabhängigkeit

Seien  $M, M', N, N'$  Mengen, so dass  $|M| = |M'|$  und  $|N| = |N'|$ .  
Es existiert eine injektive Funktion  $f: M \rightarrow N$   
gdw. eine injektive Funktion  $g: M' \rightarrow N'$  existiert.

Beweis.

*beidseitige Implikationen:*

- ( $\rightarrow$ ) Sei  $f: M \rightarrow N$  injektiv. Aufgrund der Annahme existieren  
 $f': M' \rightarrow M$  und  $f'': N \rightarrow N'$  bijektiv. Dann ist  
 $(f'; f; f''): M' \rightarrow N'$  injektiv nach §5.3.
- ( $\leftarrow$ ) analog



## Beispiele

- $|\mathbb{N}| \leq |\mathbb{Z}|$  vermittels  $\text{id}: \mathbb{N} \rightarrow \mathbb{Z}$  mit  $\text{id}(n) = n$  für alle  $n \in \mathbb{N}$
- $|\emptyset| \leq |\mathbb{N}|$  vermittels  $\emptyset$
- $|\{1, 2\}| \leq |\{2, 3, 4\}|$  vermittels  $f = \{(1, 4), (2, 2)\}$

## §6.12 Theorem

Sei  $M \subseteq N$ . Dann gilt  $|M| \leq |N|$ .

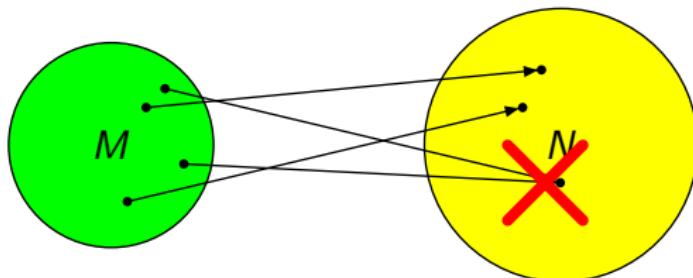
## Beweis.

Sei  $\text{id}: M \rightarrow N$ , so dass  $f(m) = m$  für alle  $m \in M$ .

Offensichtlich ist 'id' injektiv.

□

$f$  nicht injektiv:



## Notiz

für injektive Funktion  $f: M \rightarrow N$  muss es für jedes Element aus  $M$  ein eigenes Element  $f(m)$  in  $N$  geben

→ es gibt "mehr" Elemente in  $N$

## §6.13 Theorem (nutzt Auswahlaxiom)

Sei  $f: M \rightarrow N$  surjektiv. Dann gilt  $|N| \leq |M|$ .

Beweis.

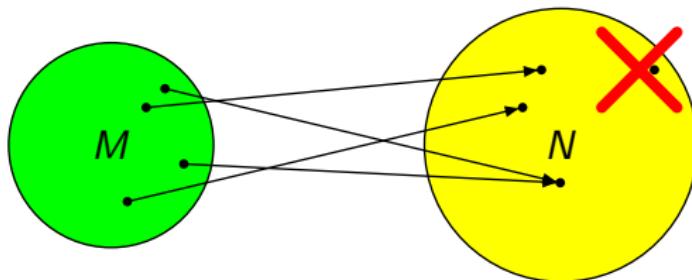
Da  $f$  surjektiv ist, existiert gemäß §5.9 eine Funktion  $g: N \rightarrow M$ , so dass  $g ; f = \text{id}_N$ . Z.zg.  $g$  ist injektiv. Kontraposition. Seien  $n, n' \in N$  mit  $g(n) = g(n')$ . Dann gilt

$$\begin{aligned}n &= \text{id}_N(n) = (g ; f)(n) = f(g(n)) \\&= f(g(n')) = (g ; f)(n') = \text{id}_N(n') = n'\end{aligned}$$

Da  $g$  injektiv ist, gilt  $|N| \leq |M|$ .

□

$f$  nicht surjektiv:



## Notiz

für surjektive Funktion  $f: M \rightarrow N$  muss für jedes Element aus  $N$  ein eigenes Element  $m \in M$  mit  $f(m) = n$  existieren

→ es gibt "mehr" Elemente in  $M$ , falls Auswahlaxiom gilt

## Definition (§4.14)

Eine Relation  $\preceq$  auf  $M$  ist eine **Ordnungsrelation** gdw. sie reflexiv, antisymmetrisch und transitiv ist.

- $(\forall m \in M). m \preceq m$  reflexiv
- $(\forall m, m' \in M). ((m \preceq m' \wedge m' \preceq m) \rightarrow m = m')$  antisymmetrisch
- $(\forall m, m', m'' \in M). ((m \preceq m' \wedge m' \preceq m'') \rightarrow m \preceq m'')$  transitiv

## §6.14 Theorem

$\leq$  ist eine Ordnungsrelation auf Kardinalitäten

Beweis.

- **reflexiv:** Für jede Menge  $M$  ist  $\text{id}_M: M \rightarrow M$  injektiv, also gilt  $|M| \leq |M|$ .
- **antisymmetrisch:** Seien  $f: M \rightarrow N$  und  $g: N \rightarrow M$  injektiv. Dann existiert  $h: M \rightarrow N$  bijektiv nach §6.5, also  $|M| = |N|$ .
- **transitiv:** Seien  $f: M \rightarrow N$  und  $g: N \rightarrow P$  injektiv. Dann ist  $(f; g): M \rightarrow P$  injektiv nach §5.3 und damit  $|M| \leq |P|$ .  $\square$

## §6.15 Theorem (Satz von HARTOGS)

$\leq$  ist eine lineare Ordnungsrelation auf Kardinalitäten  
gdw. das Auswahlaxiom gilt

FRIEDRICH MORITZ HARTOGS (\* 1874; † 1943)

- dtsch. Mathematiker
- Funktionentheorie
- wesentliche Beiträge zu Kardinalitäten



© Konrad Jacobs

## §6.16 Theorem

Für jede Funktion  $f: M \rightarrow M$  auf einer **endlichen** Menge  $M$  sind folgende Aussagen äquivalent:

- ①  $f$  ist bijektiv
- ②  $f$  ist surjektiv
- ③  $f$  ist injektiv

Beweis.

In der Übung ...



Notiz

- dies gilt nicht für unendliche Mengen
- **verdoppeln**:  $\mathbb{N} \rightarrow \mathbb{N}$  ist injektiv, aber nicht surjektiv

## §6.17 Definition (Endlichkeit)

Eine Menge  $M$  ist **endlich** gdw.

jede Funktion  $f: M \rightarrow M$  surjektiv ist gdw. sie injektiv ist.

### Notizen

- entspricht der natürlichen Vorstellung
- wir identifizieren 'endliche Kardinalitäten' mit  $\mathbb{N}$   
(jede endliche Kardinalität entspricht einer natürlichen Zahl)
- aber  $\mathbb{N}$  selbst ist nicht endlich

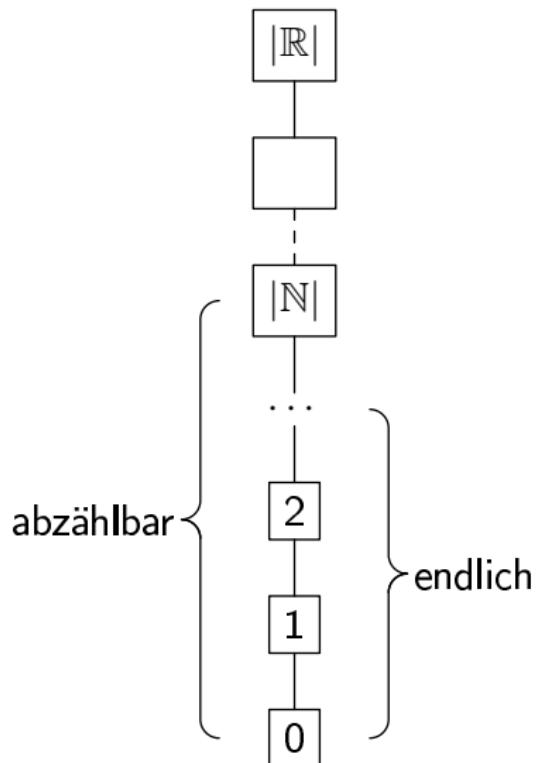
## §6.18 Definition (Abzählbarkeit)

Eine Menge  $M$  ist **abzählbar** gdw.  $|M| \leq |\mathbb{N}|$   
(d.h., sie höchstens die Kardinalität von  $\mathbb{N}$  hat)

## Beispiele

- endliche Mengen sind abzählbar
- $\mathbb{Z}$  und  $\mathbb{Q}$  sind abzählbar (§6.6 und §6.7)
- $\mathbb{R}$  ist **nicht** abzählbar (§6.8)

Gibt es unendlich viele unendliche Kardinalitäten?



## §6.19 Theorem (Satz von CANTOR)

Für jede Menge  $M$  gilt  $|M| \leq |\mathcal{P}(M)|$  und  $|M| \neq |\mathcal{P}(M)|$

Beweis.

Sei  $f: M \rightarrow \mathcal{P}(M)$ , so dass  $f(m) = \{m\}$ . Da  $f$  injektiv ist, gilt  $|M| \leq |\mathcal{P}(M)|$ .

indirekt. Sei  $g: M \rightarrow \mathcal{P}(M)$  surjektiv. Ferner sei

$$M' = \{m' \in M \mid m' \notin g(m')\}$$

und da  $g$  surjektiv ist, existiert  $m \in M$ , so dass  $g(m) = M'$ .

Es gilt folglich  $m \in g(m) = M'$  gdw.  $m \notin g(m)$ . Widerspruch!

Also gibt es keine surjektive Funktion  $g: M \rightarrow \mathcal{P}(M)$  und damit auch keine solche bijektive Funktion. Also  $|M| \neq |\mathcal{P}(M)|$

□

Wir schreiben auch  $m < m'$ , falls  $m \leq m'$  und  $m \neq m'$

## §6.20 Korollar

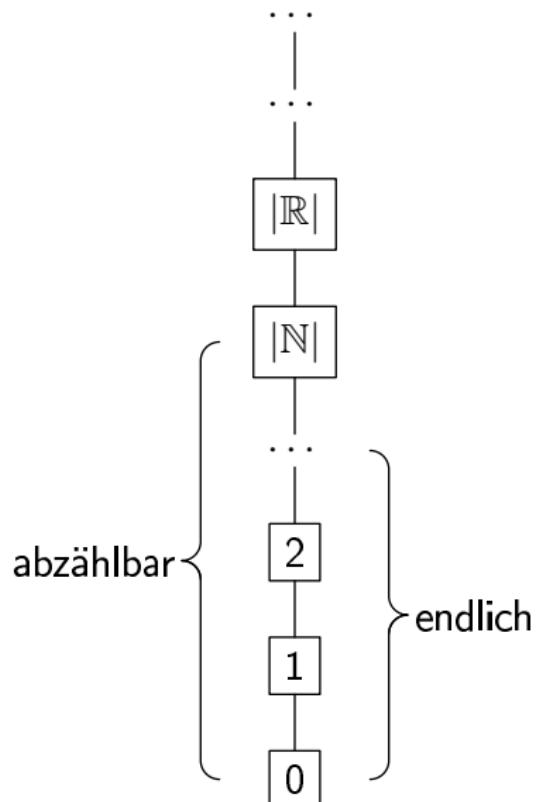
Es gibt unendlich viele unendliche Kardinalitäten

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots$$

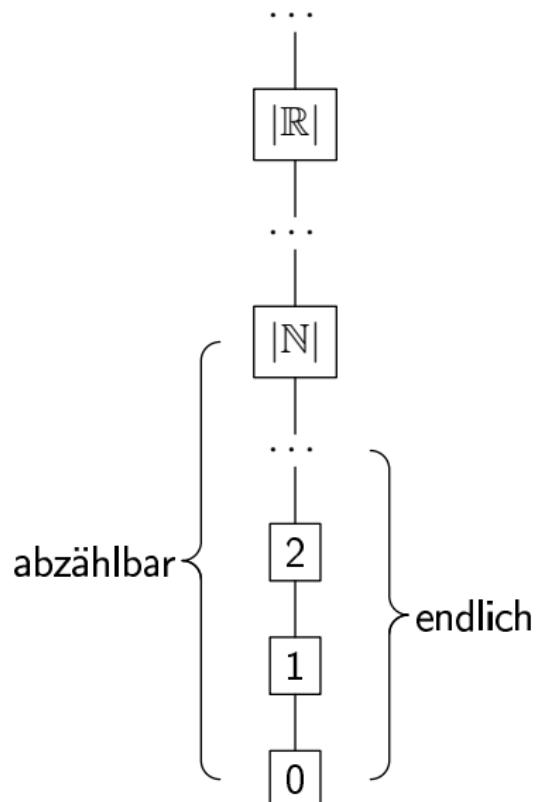
## Notizen

- außerdem gilt  $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$  → Übung
- Kontinuumshypothese (CH) von CANTOR:  
es gibt **keine** Menge  $M$ , so dass  $|\mathbb{N}| < |M| < |\mathbb{R}|$
- CH ist unabhängig von ZFC (GÖDEL, COHEN)

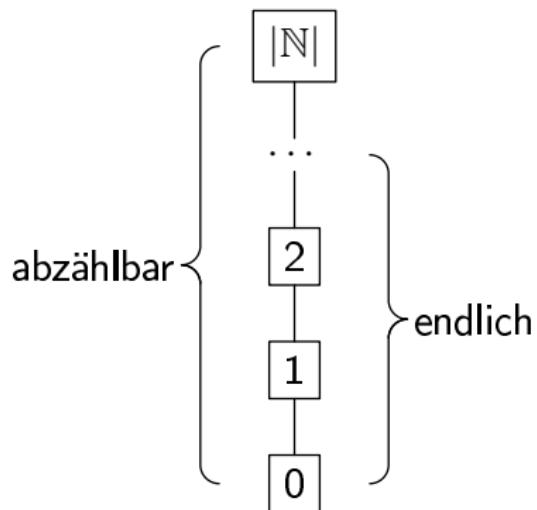
Kontinuumshypothese gilt:



Kontinuumshypothese gilt nicht:



In der **diskreten Mathematik** nur abzählbare Strukturen  
(sogar größtenteils endliche Strukturen)



- Fixpunkte von Funktionen
- Fixpunktsatz für  $(\mathcal{P}(M), \subseteq)$
- Kardinalität von Mengen
- Ordnung der Kardinalitäten
- Endliche und abzählbare Mengen → **diskrete Mathematik**

# Diskrete Strukturen

## Vorlesung 7: Kombinatorik

Andreas Maletti

25. November 2014

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## heutige Vorlesung

- ① Taubenschlagprinzip
- ② Grundlagen der Kombinatorik
- ③ Klassifikation und grundlegende Formeln
- ④ Binomialkoeffizienten

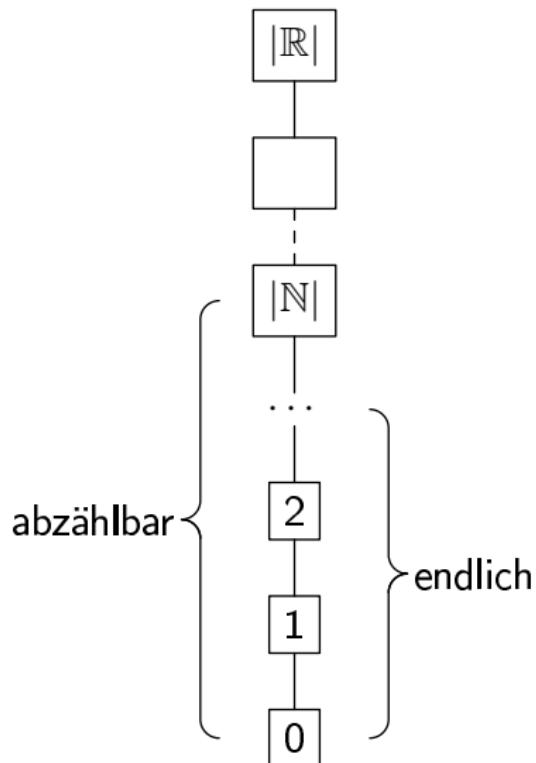
Bitte Fragen direkt stellen!

Kardinalität

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

Gibt es unendlich viele unendliche Kardinalitäten?



## Theorem (§6.19 — Satz von CANTOR)

Für jede Menge  $M$  gilt  $|M| \leq |\mathcal{P}(M)|$  und  $|M| \neq |\mathcal{P}(M)|$

Beweis.

Sei  $f: M \rightarrow \mathcal{P}(M)$ , so dass  $f(m) = \{m\}$ . Da  $f$  injektiv ist, gilt  $|M| \leq |\mathcal{P}(M)|$ .

indirekt. Sei  $g: M \rightarrow \mathcal{P}(M)$  surjektiv. Ferner sei

$$M' = \{m' \in M \mid m' \notin g(m')\}$$

und da  $g$  surjektiv ist, existiert  $m \in M$ , so dass  $g(m) = M'$ .

Es gilt folglich  $m \in g(m) = M'$  gdw.  $m \notin g(m)$ . Widerspruch!

Also gibt es keine surjektive Funktion  $g: M \rightarrow \mathcal{P}(M)$  und damit auch keine solche bijektive Funktion. Also  $|M| \neq |\mathcal{P}(M)|$

□

Wir schreiben auch  $m < m'$ , falls  $m \leq m'$  und  $m \neq m'$

## Korollar (§6.20)

Es gibt unendlich viele unendliche Kardinalitäten

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots$$

Kombinatorik

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## Fragestellung

- Wie viele **Kombinationen** / Varianten / Möglichkeiten gibt es für ...
- Wie sehen diese **Konfigurationen** aus?  
→ Lehre des Abzählens

## Beispiel

- Aufbau Email-Adresse an der Uni Leipzig

mai      14      zar  
Fakultät Imma-Jahr beliebige Kleinbuchstaben

- Wie viele Studenten können sich an unserer Fakultät pro Imma-Jahr maximal einschreiben?
- Anzahl der Kombinationen von 3 Kleinbuchstaben (ohne Umlaute, etc.)
- 26 mgl. Kleinbuchstaben für die erste Stelle  
26 mgl. Kleinbuchstaben für die zweite Stelle, ...
- insg.  $26^3 = 17.576$  Kombinationen (recht zukunftssicher)

## Beispiel

- Aufbau PIN (veraltet) einer EC- oder Kreditkarte

$$n_1 \ n_2 \ n_3 \ n_4$$

mit  $n_1 \in \{1, \dots, 9\}$  und  $n_2, n_3, n_4 \in \{0, \dots, 9\}$

(führende Nullen wurden in der ersten Generation ersetzt)

- Wie viele verschiedene (solche) PINs gibt es?
- 9 mgl. Ziffern für die erste Stelle  
10 mgl. Ziffern für die zweite Stelle, ...
- $9 \cdot 10^3 = 9.000$

## Erinnerung

- Kardinalitäten endlicher Mengen sind natürliche Zahlen  
→ wir können damit rechnen

## §7.1 Theorem

Seien  $M$  und  $N$  endliche Mengen. Dann gilt

$$|M \times N| = |M| \cdot |N|$$

Beweis.

in der Übung ...



## §7.2 Theorem (Taubenschlagprinzip von DIRICHLET)

Halten sich  $n+1$  Tauben in  $n$  Taubenschlägen auf,  
so existiert ein Taubenschlag mit mind. 2 Tauben

PETER GUSTAV DIRICHLET (\* 1805; † 1859)

- dtsch. Mathematiker
- Zahlentheorie und Analysis
- Frau = Schwester von FELIX MENDELSSOHN
- “nur” Ehrendoktor (sprach kein Latein)



## §7.3 Theorem

Seien  $M$  und  $N$  endliche Mengen mit  $N \neq \emptyset$  und  $f: M \rightarrow N$  eine Funktion. Dann existiert  $n \in N$  mit  $|f^{-1}(\{n\})| \geq \lceil \frac{|M|}{|N|} \rceil$   
(d.h., ein  $n \in N$  ist das Bild von mind.  $\lceil \frac{|M|}{|N|} \rceil$  Elementen)

Beweis.

Wähle  $n \in N$ , so dass  $|f^{-1}(\{n\})| \geq |f^{-1}(\{n'\})|$  für alle  $n' \in N$ .  
(Wähle Bild mit den meisten Urbildern)

Es gilt

$$|M| \leq \sum_{n' \in N} |f^{-1}(\{n'\})| \leq \sum_{n' \in N} |f^{-1}(\{n\})| = |N| \cdot |f^{-1}(\{n\})|$$

Also gilt auch  $|f^{-1}(\{n\})| \geq \frac{|M|}{|N|}$ . Da  $|f^{-1}(\{n\})|$  eine natürliche Zahl ist, gilt auch  $|f^{-1}(\{n\})| \geq \lceil \frac{|M|}{|N|} \rceil$ .

□

## Beispiele

- Ein Wort mit 6 Vokalen enthält mind. 1 Vokal mind. doppelt
- von 200 Studenten haben mind.  $\lceil \frac{200}{7} \rceil = 29$  am gleichen Wochentag ihren Geburtstag

## §7.4 Theorem

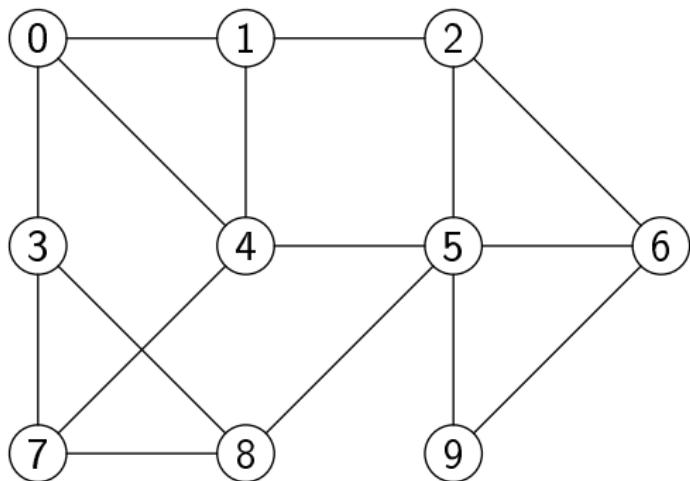
Sei  $M$  eine endliche Menge mit  $|M| \geq 6$  und  $R \subseteq M \times M$  eine symmetrische Relation. Dann existiert  $M' \subseteq M$ , so dass  $|M'| \geq 3$  und

- $(m', m'') \in R$  für alle  $m', m'' \in M'$  mit  $m' \neq m''$  oder
- $(m', m'') \notin R$  für alle  $m', m'' \in M'$  mit  $m' \neq m''$

## Beweis.

Sei  $m \in M$  beliebig. Nach §7.3 existieren mind. 3 verschiedene Elemente  $m_1, m_2, m_3 \in M \setminus \{m\}$  mit der gleichen Beziehung zu  $m$ .

- Sei  $(m, m_1), (m, m_2), (m, m_3) \in R$ . Existiert  $m', m'' \in \{m_1, m_2, m_3\}$  mit  $(m', m'') \in R$  und  $m' \neq m''$ , dann ist  $\{m, m', m''\}$  eine gesuchte Teilmenge. Andernfalls gilt  $(m', m'') \notin R$  für alle  $m', m'' \in \{m_1, m_2, m_3\}$  mit  $m' \neq m''$ , womit  $\{m_1, m_2, m_3\}$  eine gesuchte Teilmenge ist.
- Sei  $(m, m_1), (m, m_2), (m, m_3) \notin R$ . Analog. □



## Problem-Klassifikation

## Notizen

- kombinatorische Probleme oft zerlegbar in Einzelteile  
z.B. Stellen einer PIN, Stellen der Email-Adresse, etc.
- für Einzelteile Anzahl der Möglichkeiten meist einfach  
z.B. 10 Möglichkeiten für eine Stelle der PIN
- Klassifikation der Probleme
  - wie liefern Einzelteile Gesamtergebnis
  - Beschränkungen der Einzelteile untereinander

## §7.5 Klassifikation (Bildung des Gesamtergebnisses)

- **Zuordnung:** *Permutation, Variation*  
Reihenfolge bzw. Zuordnung der Einzelteile relevant  
z.B. PIN, Email-Adresse
- **Auswahl:** *Kombination*  
Reihenfolge bzw. Zuordnung der Einzelteile irrelevant  
z.B. Lotto-Zahlen, Übungsgruppenauswahl

## §7.6 Klassifikation (Interaktion der Einzelteile)

- **mit** Wiederholung: selbe Einzelteil mehrfach möglich  
z.B. PIN, Anagramme (Umsortierung der Buchstaben)
- **ohne:** Wiederholung: selbe Einzelteil nicht mehrfach  
z.B. Lotto-Zahlen, Gruppen-Auslosung der Fußball-WM

## Notizen

- betrachten Probleme jeden Typs unserer Klassifikation
- weitere Klassen denkbar
- insb. kompliziertere Interaktionen zwischen Einzelteilen vorstellbar

Variation mit Wiederholung

## Variation mit Wiederholung

- Reihenfolge relevant; Wiederholung möglich
- Wahl der Einzelteile unabhängig

## Beispiele

### ① PIN

- 1. Stelle aus  $\{0, 1, \dots, 9\}$
- ...
- 4. Stelle aus  $\{0, 1, \dots, 9\}$

### ② Email-Adresse `mai14zar@studserv.uni-leipzig.de`

- 6. Stelle aus  $\{a, \dots, z\}$
- 7. Stelle aus  $\{a, \dots, z\}$
- 8. Stelle aus  $\{a, \dots, z\}$

## §7.7 Definition

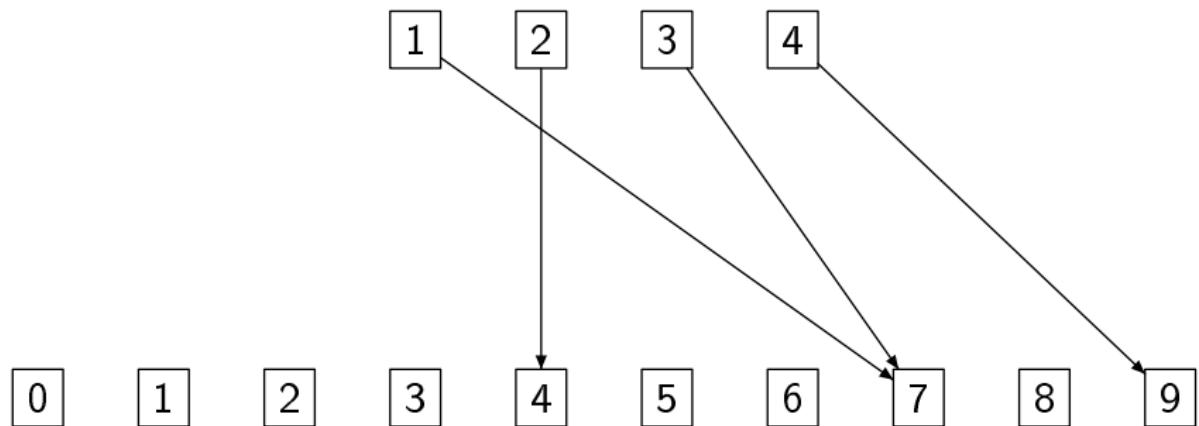
Seien  $M$  und  $N$  endliche Mengen.

Eine  **$N$ -Variation von  $M$**  ist eine Funktion

$$f: N \rightarrow M$$

## Beispiele

- PIN ist eine  $\{1, 2, 3, 4\}$ -Variation von  $\{0, 1, \dots, 9\}$
- Email-Adresse ist  $\{6, 7, 8\}$ -Variation von  $\{a, \dots, z\}$



## §7.8 Theorem

Für alle endlichen Mengen  $M$  und  $N$  gibt es  $m^n$   $N$ -Variationen von  $M$ , wobei  $m = |M|$  und  $n = |N|$  (und  $0^0 = 1$ )

Beweis.

per vollständiger Induktion über  $n$ .

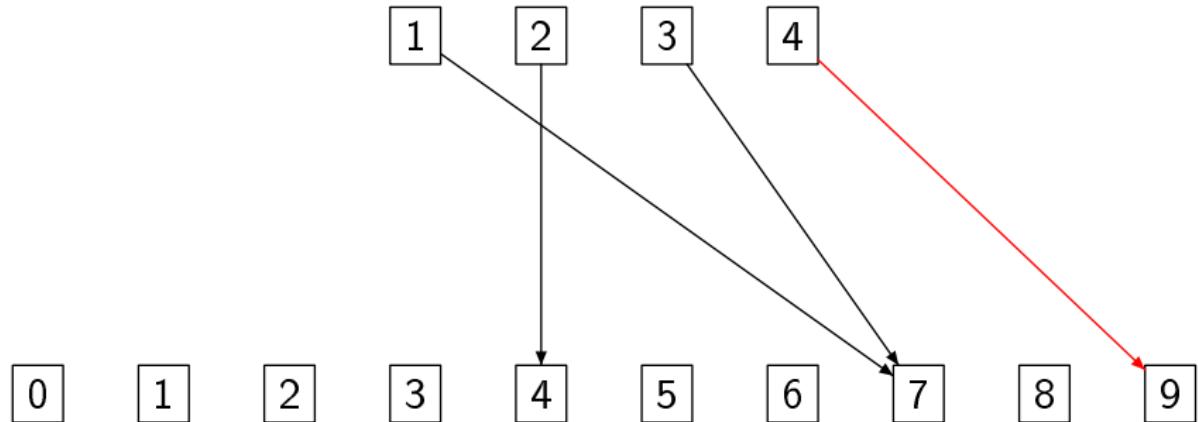
- **IA:** Sei  $n = |N| = 0$  und damit  $N = \emptyset$ . Dann existiert nur die Funktion  $\emptyset: N \rightarrow M$  und damit existiert  $1 = m^0$  Variation.
- **IS:** Sei  $N \neq \emptyset$  und wähle  $x \in N$  beliebig. Jede Funktion  $f: N \rightarrow M$  lässt sich darstellen als

$$f(n') = \begin{cases} g(n') & \text{falls } n' \neq x \\ m' & \text{sonst} \end{cases}$$

für eine Funktion  $g: (N \setminus \{x\}) \rightarrow M$  und  $m' \in M$ . Gemäß IH.  
gibt es  $m^{(n-1)}$  Wahlmöglichkeiten für  $g$  und  $|M| = m$  Möglichkeiten für  $m'$ . Damit erhalten wir  $m^{(n-1)} \cdot m = m^n$  mögliche  $N$ -Variationen von  $M$ .

□

# Kombinatorik — Variation



Variation ohne Wiederholung

## Variation ohne Wiederholung

- Reihenfolge relevant; Wiederholung nicht möglich
- Wahl der Einzelteile **nicht** unabhängig

## Beispiele

- ➊ Siegerehrung einer Sportveranstaltung mit 8 Teilnehmern
  - 1. Platz  $i_1$  aus  $\{1, \dots, 8\}$
  - 2. Platz  $i_2$  aus  $\{1, \dots, 8\} \setminus \{i_1\}$
  - 3. Platz  $i_3$  aus  $\{1, \dots, 8\} \setminus \{i_1, i_2\}$
- ➋ Stapel aus allen Skatkarten
  - oberste Karte  $k_1$  aus  $\{7\diamondsuit, \dots, A\clubsuit\}$
  - ...
  - unterste Karte  $k_{32}$  aus  $\{7\diamondsuit, \dots, A\clubsuit\} \setminus \{k_1, \dots, k_{31}\}$

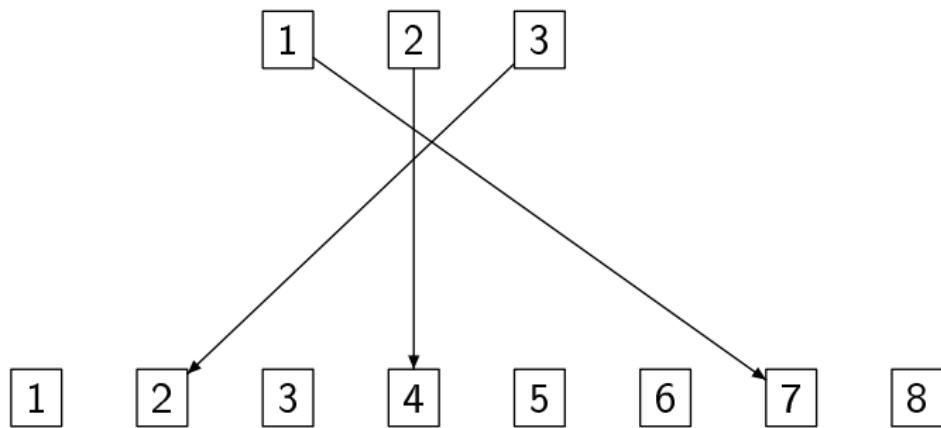
## §7.9 Definition

Seien  $M$  und  $N$  endliche Mengen.

Eine  **$N$ -Variation von  $M$  ohne Wiederholung**  
ist eine injektive Funktion  $f: N \rightarrow M$

## Beispiele

- Siegerehrung ist eine  $\{1, 2, 3\}$ -Variation von  $\{1, \dots, 8\}$  ohne Wiederholung
- Kartenstapel ist  $\{1, \dots, 32\}$ -Variation von  $\{7\diamond, \dots, A\clubsuit\}$  ohne Wiederholung



## §7.10 Theorem

Seien  $M$  und  $N$  endliche Mengen.

Falls  $m \geq n$ , gibt es  $\prod_{i=0}^{n-1} (m-i)$   $N$ -Variationen von  $M$  ohne Wiederholung, wobei  $m = |M|$  und  $n = |N|$ .

Sonst gibt es keine solchen Variationen.

### Beweis (1/2).

Sei zunächst  $m < n$ ; d.h.  $|M| < |N|$ . Dann existiert keine injektive Funktion  $f: N \rightarrow M$ , denn sonst wäre  $|N| \leq |M|$  nach §6.10.

Sei also  $m \geq n$ . Beweis per vollständiger Induktion über  $n$ .

- **IA:** Sei  $n = |N| = 0$  und damit  $N = \emptyset$ . Dann existiert nur die Funktion  $\emptyset: N \rightarrow M$ , die injektiv ist, und damit existiert  $1 = \prod_{i=0}^{-1} (m-i)$  Variation.

## Beweis (2/2).

- IS: Sei  $N \neq \emptyset$  und wähle  $x \in N$  beliebig. Jede injektive Funktion  $f: N \rightarrow M$  lässt sich darstellen als

$$f(n') = \begin{cases} g(n') & \text{falls } n' \neq x \\ m' & \text{sonst} \end{cases}$$

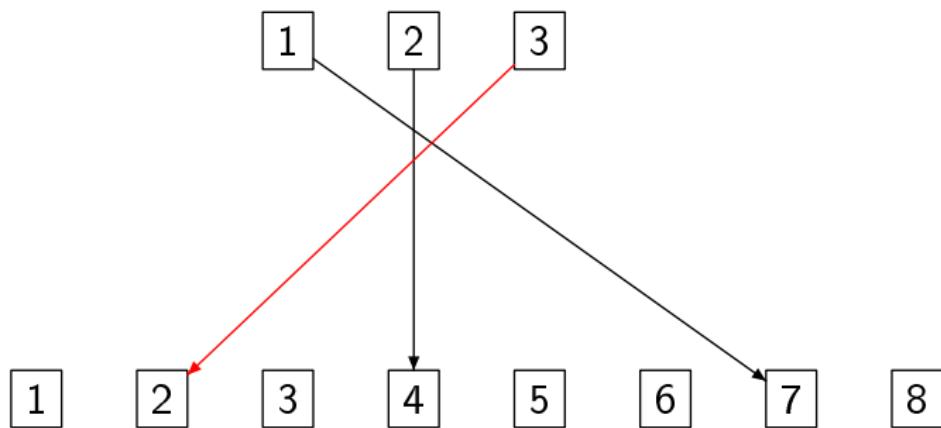
für eine injektive Funktion  $g: (N \setminus \{x\}) \rightarrow M$  und  
 $m' \in M \setminus g(N \setminus \{x\})$ .

(ein Bild von  $g$  kann nicht noch einmal gewählt werden).  
Gemäß IH. gibt es  $\prod_{i=0}^{n-2} (m-i)$  Wahlmöglichkeiten für  $g$  und  
 $|M| - (|N| - 1) = m - (n - 1)$  Möglichkeiten für  $m'$ . Damit erhalten wir

$$\prod_{i=0}^{n-2} (m-i) \cdot (m - (n - 1)) = \prod_{i=0}^{n-1} (m-i)$$

mögliche  $N$ -Variationen von  $M$  ohne Wiederholung. □

# Kombinatorik — Variation



## §7.11 Definition (Permutation)

Seien  $M$  und  $N$  endliche Mengen.

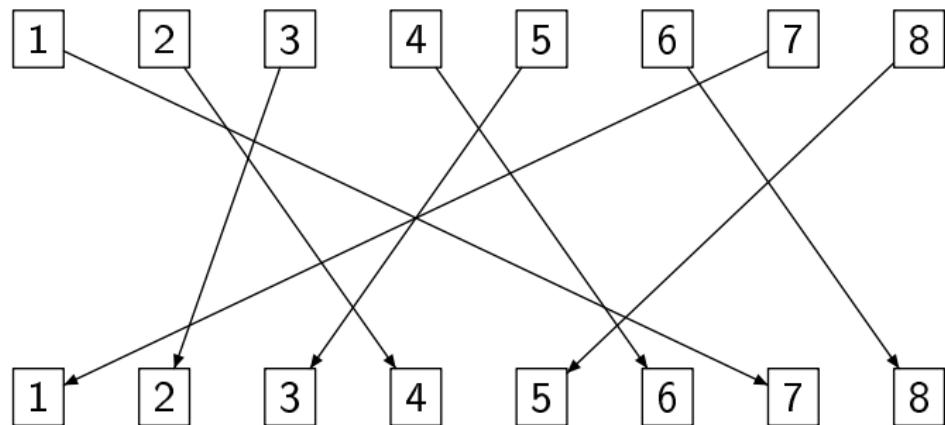
Jede  $N$ -Variation vom  $M$  ohne Wiederholung mit  $M = N$  heißt auch **Permutation von  $M$**

(anders: Permutation ist injektive Funktion  $f: M \rightarrow M$ )

### Beispiele

- $\text{id}_M$  ist eine Permutation von  $M$
- $\{(1, 2), (2, 3), (3, 1)\}$  ist eine Permutation von  $\{1, 2, 3\}$
- $\{(1, 1), (2, 3), (3, 1)\}$  ist **keine** Permutation

Permutation:



## §7.12 Theorem

Sei  $M$  eine endliche Menge. Jede Permutation von  $M$  ist bijektiv

### Beweis.

Sei  $f: M \rightarrow M$  eine Permutation von  $M$ . Da  $M$  endlich und  $f$  injektiv ist, ist  $f$  auch surjektiv nach §6.17. Also ist  $f$  bijektiv. □

## §7.13 Theorem

Sei  $M$  eine endliche Menge. Es gibt  $m!$  Permutationen von  $M$ , wobei  $m = |M|$

Beweis.

Da Permutationen spezielle Variationen ohne Wiederholung sind, wenden wir §7.10 an. Danach gibt es

$$\prod_{i=0}^{m-1} (m-i) = m \cdot (m-1) \cdot \dots \cdot \underbrace{(m-(m-1))}_{=1} = \prod_{i=1}^m m = m!$$

$M$ -Variationen von  $M$  ohne Wiederholung. □

## §7.13 Theorem

Seien  $M$  und  $N$  endliche Mengen. Falls  $m \geq n$ , gibt es  $\frac{m!}{(m-n)!}$   
 $N$ -Variationen von  $M$  ohne Wiederholung,  
wobei  $m = |M|$  und  $n = |N|$

Beweis.

Nach §7.10 wissen wir bereits, dass es

$$\begin{aligned}\prod_{i=0}^{n-1} (m-i) &= \prod_{i=0}^{n-1} (m-i) \cdot \frac{\prod_{i=n}^{m-1} (m-i)}{\prod_{i=n}^{m-1} (m-i)} \\ &= \frac{\prod_{i=0}^{m-1} (m-i)}{\prod_{i=n}^{m-1} (m-i)} = \frac{m!}{(m-n)!}\end{aligned}$$

solche Variationen gibt. □

Kombination ohne Wiederholung

## Kombination ohne Wiederholung

- Reihenfolge irrelevant; Wiederholung nicht möglich
- Wahl der Einzelteile **nicht** unabhängig

## Beispiele

### ① Lotto 6-aus-49

- Kugeln werden zwar der Reihe nach gezogen
- aber Ergebnis ist nur eine Menge  $M \subseteq \{1, \dots, 49\}$  mit  $|M| = 6$

### ② Handblatt beim Skat

- auch hier bekommt man die Karten zwar in einer Reihenfolge
  - aber diese ist im Weiteren irrelevant
- $H \subseteq \{7\diamondsuit, \dots, A\clubsuit\}$

## §7.14 Definition

Sei  $M$  eine endliche Menge und  $k \in \mathbb{N}$ .

Eine  **$k$ -Kombination von  $M$  ohne Wiederholung**  
ist eine Menge  $K \subseteq M$  mit  $|K| = k$

## Beispiele

- Lotto 6-aus-49 ist eine 6-Kombination von  $\{1, \dots, 49\}$  ohne Wiederholung
- 3-Karten-Handblatt ist eine 3-Kombination von  $\{7\lozenge, \dots, A\clubsuit\}$  ohne Wiederholung

# Kombinatorik — Kombination

1

2

3

4

5

6

7

8

## §7.15 Theorem

Seien  $M$  und  $N$  endliche Mengen.

Jede injektive Funktion  $f: N \rightarrow M$  mit  $|N| = |M|$  ist surjektiv

Beweis (indirekt).

Sei  $m \in M$ , so dass  $f(n) \neq m$  für alle  $n \in N$ . Dann ist  $f: N \rightarrow (M \setminus \{m\})$  auch eine injektive Funktion.

Daraus folgt  $|N| \leq |M| - 1$  nach §6.10 und damit  $|N| < |M|$ . Dies widerspricht jedoch  $|N| = |M|$ .

□

## §7.16 Definition

Seien  $M$  und  $N$  endliche Mengen

$$\equiv = \{(f, g) \mid f, g: N \rightarrow M \text{ injektiv}, f(N) = g(N)\}$$

Funktionen sind äquivalent gdw. sie gleichen Bildbereich haben

## Beispiele

- für  $f = \{(1, 2), (2, 3), (3, 1)\}$  gilt  $f \equiv \text{id}_{\{1, 2, 3\}}$
- für  $g = \{(1, 2), (2, 4), (3, 3)\}$  und  $g' = \{(1, 1), (2, 2), (3, 3)\}$  gilt  $g \not\equiv g'$

## §7.17 Theorem

$\equiv$  ist eine Äquivalenzrelation (reflexiv, symmetrisch, transitiv) und für alle injektiven  $f: N \rightarrow M$  gilt  $|[f]_{\equiv}| = |N|!$

Beweis (1/2).

Wir beginnen mit der Äquivalenzrelation:

- **reflexiv:** Für injektives  $f: N \rightarrow M$  gilt natürlich  $f(N) = f(N)$ , also  $f \equiv f$ .
- **symmetrisch:** Seien  $f, g: N \rightarrow M$  injektiv mit  $f \equiv g$ , also  $f(N) = g(N) = f(N)$  und damit  $g \equiv f$ .
- **transitiv:** Seien  $f, g, h: N \rightarrow M$  injektiv, so dass  $f \equiv g$  und  $g \equiv h$ . Also gilt

$$f(N) = g(N) = h(N)$$

und damit  $f \equiv h$ .

## Beweis (2/2).

Sei  $f: N \rightarrow M$  injektiv. Offenbar gilt  $|N| = |f(N)|$  nach §6.10 und §6.13. Damit ist  $f(N) \subseteq M$  also eine Teilmenge der Größe  $|N|$ .

Sei  $g: N \rightarrow f(N)$  eine andere injektive Funktion gleichen Typs. Da  $|N| = |f(N)|$  ist  $g$  surjektiv nach §7.15. Also gilt  $g(N) = f(N)$  und damit  $f \equiv g$ . Also ist jede injektive Funktion  $g: N \rightarrow f(N)$  äquivalent zu  $f$ . Nach §7.10 gibt es  $|N|!$  solche Funktionen.  $\square$

## §7.18 Theorem

Sei  $M$  eine endliche Menge und  $k \in \mathbb{N}$ .

Falls  $m \geq k$ , gibt es  $\frac{m!}{(m-k)! \cdot k!}$   $k$ -Kombinationen von  $M$  ohne Wiederholung, wobei  $m = |M|$ .

Sonst gibt es keine solchen Kombinationen.

## Beweis (1/2).

Sei zunächst  $m < k$ ; d.h.  $|M| < k$ . Dann existiert keine Teilmenge  $K \subseteq M$  mit  $|K| = k$ , denn sonst wäre  $k \leq |M|$  nach §6.12.

Beweis (2/2).

Sei also  $m \geq k$  und  $D = \{1, \dots, k\}$ . Für jede Teilmenge  $K \subseteq M$  mit  $|K| = k$  existiert eine injektive Funktion  $f: D \rightarrow M$  mit  $f(D) = K$ . Umgekehrt gilt  $|f(D)| = k$  für jede injektive Funktion  $f: D \rightarrow M$ . Somit treten genau die  $k$ -elementigen Teilmengen als (erreichte) Bildbereiche der injektiven Funktionen  $f: D \rightarrow M$  auf.

Gemäß §7.10 gibt es  $\frac{m!}{(m-k)!}$  injektive Funktionen  $f: D \rightarrow M$ .

Davon sind allerdings jeweils  $k!$  Funktionen äquivalent und haben damit die gleiche (erreichte) Bildmenge. Also existieren

$$\frac{m!}{(m-k)! \cdot k!}$$

verschiedene (erreichte) Bildmengen. □

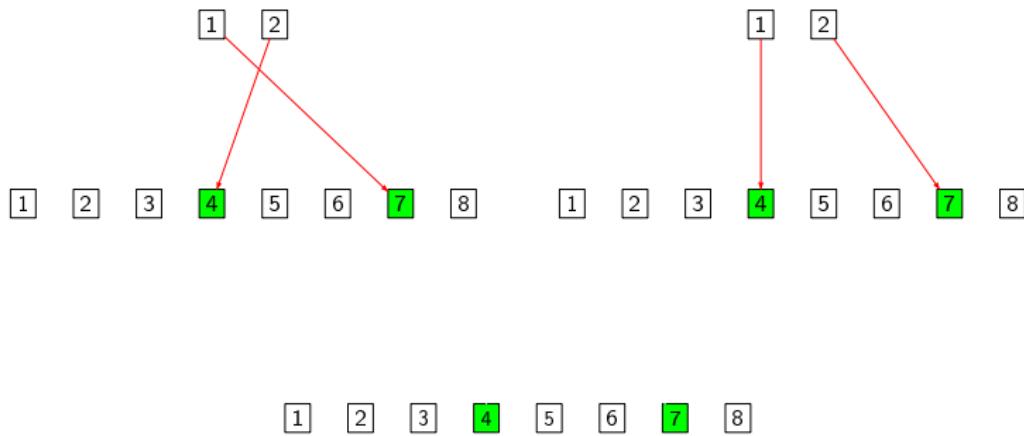
## §7.19 Definition

Für alle  $m \geq k$ , sei

$$\binom{m}{k} = \frac{m!}{(m - k)! \cdot k!}$$

der **Binomialkoeffizient  $k$  aus  $m$**

# Kombinatorik — Variation



Kombination mit Wiederholung

## Kombination mit Wiederholung

- Reihenfolge irrelevant; Wiederholung möglich
- Wahl der Einzelteile **nicht** unabhängig

## Übung

- formalisieren Sie diese Probleme
- berechnen Sie die Anzahl der Möglichkeiten
- Standardwerke zur Inspiration und Erfolgskontrolle

- Taubenschlagprinzip & kombinatorischer Beweis
- Grundlagen der Kombinatorik
- Problemklassifikation und grundlegende Zählformeln
- Binomialkoeffizienten

# Diskrete Strukturen

## Vorlesung 8: Kombinatorik & Stochastik

Andreas Maletti

9. Dezember 2014

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## heutige Vorlesung

- ① Rechnen mit Binomialkoeffizienten
- ② Grundlagen der Stochastik
- ③ Bedingte Wahrscheinlichkeiten

Bitte Fragen direkt stellen!

Kombinatorik

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## Klassifikation (§7.5 Bildung des Gesamtergebnisses)

- **Zuordnung:** *Permutation, Variation*  
Reihenfolge bzw. Zuordnung der Einzelteile relevant  
z.B. PIN, Email-Adresse
- **Auswahl:** *Kombination*  
Reihenfolge bzw. Zuordnung der Einzelteile irrelevant  
z.B. Lotto-Zahlen, Übungsgruppenauswahl

## Klassifikation (§7.6 Interaktion der Einzelteile)

- **mit** Wiederholung: selbe Einzelteil mehrfach möglich  
z.B. PIN, Anagramme (Umsortierung der Buchstaben)
- **ohne:** Wiederholung: selbe Einzelteil nicht mehrfach  
z.B. Lotto-Zahlen, Gruppen-Auslosung der Fußball-WM

## Theorem (Zusammenfassung)

Seien  $M$  und  $N$  endliche Mengen und  $k \in \mathbb{N}$ .

Weiterhin seien  $m = |M|$  und  $n = |N|$ . Es gibt

- $m^n$   $N$ -Variationen von  $M$  (mit Wiederholung)

Funktionen  $f: N \rightarrow M$

- $\frac{m!}{(m-n)!}$   $N$ -Variationen von  $M$  ohne Wiederholung  $(m \geq n)$   
injektive Funktionen  $f: N \rightarrow M$

- $m!$  Permutationen von  $M$

injektive Funktionen  $f: M \rightarrow M$

- $\frac{m!}{(m-k)! \cdot k!}$   $k$ -Kombinationen von  $M$  ohne Wdh.  $(m \geq k)$   
Teilmengen  $K \subseteq M$  mit  $|K| = k$

- ??  $k$ -Kombinationen von  $M$  (mit Wiederholung)

??

## Definition (Binomialkoeffizient)

Seien  $m, k \in \mathbb{N}$  mit  $m \geq k$ . Dann ist

$$\binom{m}{k} = \frac{m!}{(m-k)! \cdot k!}$$

## Binomialkoeffizienten

# Kombinatorik — Binomialkoeffizienten

## PASCALSches Dreieck

$\binom{0}{k}$					1			
$\binom{1}{k}$					1	1		
$\binom{2}{k}$				1	2	1		
$\binom{3}{k}$			1	3	3	1		
$\binom{4}{k}$		1	4	6	4	1		
$\binom{5}{k}$	1	5	10	10	5	1		
$\binom{6}{k}$	1	6	15	+ 20	15	6	1	
$\binom{7}{k}$	1	7	21	35	35	21	7	1

BLAISE PASCAL (\* 1623; † 1662)

- franz. Mathematiker, Physiker und Literat
- Vakuum; ortsgebundener Luftdruck
- Freund von CHEVALIER DE MÉRÉ



## §8.1 Theorem (PASCALSche Gleichung)

Für alle  $n, k \in \mathbb{N}$  mit  $1 \leq k \leq n$  gilt

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Beweis.

$$\begin{aligned}\binom{n}{k} &= \frac{n!}{k! \cdot (n-k)!} = \frac{\prod_{i=1}^n i}{k! \cdot \prod_{i=1}^{n-k} i} = \frac{\prod_{i=(n-k+1)}^n i}{k!} \\&= \frac{n \cdot \prod_{i=(n-k+1)}^{n-1} i}{k!} = \frac{(k+n-k) \cdot \prod_{i=(n-k+1)}^{n-1} i}{k!} \\&= \frac{k \cdot \prod_{i=(n-k+1)}^{n-1} i}{k!} + \frac{(n-k) \cdot \prod_{i=(n-k+1)}^{n-1} i}{k!} \\&= \binom{n-1}{k-1} + \binom{n-1}{k}\end{aligned}$$

□

## PASCALSches Dreieck

$\binom{0}{k}$					1				
$\binom{1}{k}$					1	1			
$\binom{2}{k}$				1	2	+ 1			
$\binom{3}{k}$			1	3	+ 3	1			
$\binom{4}{k}$		1	4	6	4	1			
$\binom{5}{k}$	1	5	10	= 10	5	1			
$\binom{6}{k}$	1	6	15	20	15	6	1		
$\binom{7}{k}$	1	7	21	35	35	21	7	1	

## §8.2 Theorem

Für alle  $n, k \in \mathbb{N}$  mit  $n \geq k$  gilt

$$\binom{n+1}{k+1} = \sum_{i=0}^n \binom{i}{k}$$

Beweis (1/2).

per vollständiger Induktion über  $n$ :

- **Induktionsanfang:** Sei  $n = 0$ . Dann gilt  $k = 0$  und damit

$$\binom{1}{1} = 1 = \binom{0}{0} = \sum_{i=0}^0 \binom{i}{k}$$

Beweis (2/2).

per vollständiger Induktion über  $n$ :

- **Induktionsschritt:**

$$\binom{n+2}{k+1} = \binom{n+1}{k} + \binom{n+1}{k+1}$$

§8.1

$$= \binom{n+1}{k} + \sum_{i=0}^n \binom{i}{k}$$

IH

$$= \sum_{i=0}^{n+1} \binom{i}{k}$$

□

## Notizen

- viele weitere Zusammenhänge
- mehr Spaß mit Binomialkoeffizienten in der Übung

Grundlagen Stochastik

## Intuition

- **Wahrscheinlichkeit** = erwartete Häufigkeit eines **Ereignisses** in Wiederholungen eines gleichartigen **Experiments**
- **Experiment** = Aktion, die eines mehrerer möglicher Ergebnisse produziert (**Elementarereignisse**)
- **Ereignis** = Teilmenge der Ergebnisse

## Beispiel

- **Experiment:** Würfeln (mit einem 6-seitigem Würfel)
- **Ereignisse:**
  - $E_1$ : eine gerade Zahl gewürfelt {2, 4, 6}
  - $E_2$ : eine 5 gewürfelt {5}
- **Wahrscheinlichkeiten:**
  - erwartete Häufigkeit von  $E_1$ : 50%
  - erwartete Häufigkeit von  $E_2$ : 17%

## Notizen

- wir folgen dem axiomatischen Ansatz von KOLMOGOROV
- zur Identifikation von diskreten Strukturen
- dieser Ansatz ist allgemeingültig  
(im diskreten Fall kann man dies vereinfachen)

ANDREJ KOLMOGOROV (\* 1903; † 1987)

- russ. Mathematiker
- Stochastik, Topologie,  
algorithmische Komplexitätstheorie
- Förderer begabter Jugendlicher



© Konrad Jacobs

## §8.3 Definition (Maßraum)

Seien  $\Sigma$  eine Menge und  $\mathcal{E} \subseteq \mathcal{P}(\Sigma)$ .

Dann ist  $(\Sigma, \mathcal{E})$  ein **Maßraum** gdw.

- $\Sigma \in \mathcal{E}$  (Grundmenge enthalten)
- $\Sigma \setminus E \in \mathcal{E}$  für alle  $E \in \mathcal{E}$  (abgeschlossen unter Komplement)
- $\bigcup_{i \in \mathbb{N}} E_i \in \mathcal{E}$  für alle  $E_0, E_1, \dots \in \mathcal{E}$  (abgeschlossen unter abzählbarer Vereinigung)

## Beispiele

- für jede Menge  $M$  sind  $(M, \{\emptyset, M\})$  und  $(M, \mathcal{P}(M))$  Maßräume
- für jede Menge  $M$  und Teilmenge  $N \subseteq M$  ist  $(M, \{\emptyset, N, N^c, M\})$  ein Maßraum

## §8.4 Theorem

Sei  $(\Sigma, \mathcal{E})$  ein Maßraum.

Dann gilt auch  $\bigcap_{i \in \mathbb{N}} E_i \in \mathcal{E}$  für alle  $E_0, E_1, \dots \in \mathcal{E}$

Beweis.

*Direkt.* Seien  $E_0, E_1, \dots \in \mathcal{E}$ . Dann ist

$$\bigcap_{i \in \mathbb{N}} E_i = \left( \left( \bigcap_{i \in \mathbb{N}} E_i \right)^c \right)^c = \left( \bigcup_{i \in \mathbb{N}} E_i^c \right)^c$$

Da  $E_i^c \in \mathcal{E}$  (Abschluss unter Komplement)

und  $\bigcup_{i \in \mathbb{N}} E_i^c \in \mathcal{E}$  (Abschluss unter abzählbarer Vereinigung),  
ist auch  $\bigcap_{i \in \mathbb{N}} E_i \in \mathcal{E}$  (Abschluss unter Komplement). □

## §8.5 Begriffe

Sei  $(\Sigma, \mathcal{E})$  ein Maßraum

- jedes Element  $\sigma \in \Sigma$  heißt **elementares Ereignis**
- jedes Element  $E \in \mathcal{E}$  heißt **Ereignis**
- $\Sigma$  ist **Elementarereignismenge**
- $\mathcal{E}$  ist **Ereignismenge**

## Beispiel

Würfeln (mit 6-seitigem Würfel):

- Elementarereignisse  $\Sigma = \{1, 2, 3, 4, 5, 6\}$
- Ereignismenge  $\mathcal{E} = \mathcal{P}(\Sigma)$
- Maßraum  $(\Sigma, \mathcal{E})$
- $\{1, 3\} \in \mathcal{E}$  ist Ereignis ("1 oder 3")
- $\emptyset \in \mathcal{E}$  ist Ereignis (unmögliches Ereignis)
- $\Sigma \in \mathcal{E}$  ist Ereignis (sicheres Ereignis)

## Notizen

- diskrete Stochastik = Elementarereignismenge  $\Sigma$  abzählbar  
aber Ereignismenge  $\mathcal{E}$  evtl. nicht abzählbar  
Bsp.  $\Sigma = \mathbb{N}$  abzählbar und  $\mathcal{E} = \mathcal{P}(\mathbb{N})$  nicht abzählbar
- hier oft endliche Elementarereignismengen  $\Sigma$
- Maßraum unter BOOLEschen Operationen  
(Vereinigung, Schnitt, Komplement) abgeschlossen
- gilt sogar für abzählbare Vereinigungen und Schnitte

## GEORGE BOOLE (\* 1815; † 1864)

- engl. Philosoph und Mathematiker
- symbolische Aussagenlogik
- nur Grundschulausbildung



## §8.6 Definition (Wahrscheinlichkeitsmaß)

Sei  $(\Sigma, \mathcal{E})$  ein Maßraum und  $p: \mathcal{E} \rightarrow [0, 1]$ .

Dann ist  $(\Sigma, \mathcal{E}, p)$  ein **Wahrscheinlichkeitsmaß** gdw.

- $p(\Sigma) = 1$  (sicheres Ereignis tritt immer ein)
- $p(\bigcup_{i \in \mathbb{N}} E_i) = \sum_{i \in \mathbb{N}} p(E_i)$   
für alle paarweise disjunkten  $E_0, E_1, \dots \in \mathcal{E}$   
(Wahrscheinlichkeiten additiv für disjunkte Ereignisse)

## Beispiele

für den Maßraum des Würfels

- liefert folgendes  $p$  ein Wahrscheinlichkeitsmaß

$$p(E) = \frac{|E|}{6}$$

- $p(E) = 1$  für alle  $E \in \mathcal{E}$  **kein** Wahrscheinlichkeitsmaß

## §8.7 Theorem

Für jedes Wahrscheinlichkeitsmaß  $(\Sigma, \mathcal{E}, p)$  gelten:

- ①  $p(\emptyset) = 0$
- ②  $p(E^c) = 1 - p(E)$  für alle  $E \in \mathcal{E}$
- ③  $p(E) \leq p(E')$  für alle Ereignisse  $E, E' \in \mathcal{E}$  mit  $E \subseteq E'$
- ④  $p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$   
für alle Ereignisse  $E_1, E_2 \in \mathcal{E}$

Beweis (1/2).

- ①  $1 = p(\Sigma) = p(\emptyset \cup \Sigma) = p(\emptyset) + p(\Sigma) = p(\emptyset) + 1.$   
Es folgt  $p(\emptyset) = 0$
- ②  $1 = p(\Sigma) = p(E \cup E^c) = p(E) + p(E^c).$   
Es folgt  $p(E^c) = 1 - p(E)$
- ③  $p(E') = p(E \cup (E' \cap E^c)) = p(E) + p(E' \cap E^c).$   
Da  $p(E' \cap E^c) \geq 0$  folgt  $p(E') \geq p(E)$

## Beweis (2/2).

- ④ Seien  $E_1$  und  $E_2$  Ereignisse. Dann gilt

$$\begin{aligned} p(E_1 \cup E_2) &= p(E_1 \cup (E_2 \cap E_1^c)) = p(E_1) + p(E_2 \cap E_1^c) \\ &= p(E_1) + p(((E_2 \cap E_1^c)^c)^c) \\ &= p(E_1) + p((E_2^c \cup E_1)^c) \\ &= p(E_1) + 1 - p(E_2^c \cup E_1) \\ &= p(E_1) + 1 - p(E_2^c \cup (E_1 \cap E_2)) \\ &= p(E_1) + 1 - p(E_2^c) - p(E_1 \cap E_2) \\ &= p(E_1) + p(E_2) - p(E_1 \cap E_2) \end{aligned}$$

□

## §8.8 Definition

Sei  $(\Sigma, \mathcal{E}, p)$  ein Wahrscheinlichkeitsmaß mit endlichem  $\Sigma$ .

Dann ist  $(\Sigma, \mathcal{E}, p)$  **gleichverteilt** gdw.

$p(E) = \frac{|E|}{|\Sigma|}$  für alle Ereignisse  $E \in \mathcal{E}$ .

## Beispiele

- Wahrscheinlichkeitsmaß des Würfels ist gleichverteilt
- Wurf von zwei gleichen Münzen  $(K = \text{Kopf}; Z = \text{Zahl})$

$$\Sigma = \{\{K\}, \{Z\}, \{K, Z\}\} \quad \mathcal{E} = \mathcal{P}(\Sigma)$$

mit  $p(\{\{K\}\}) = p(\{\{Z\}\}) = 0,25$  und  $p(\{\{K, Z\}\}) = 0,5$   
ist **nicht** gleichverteilt

## Erste Beispiele

## Frage [GALILEO, Anfang 17. Jhd.]

Kommt beim Würfeln mit 3 Würfeln

die Augensumme 10 häufiger vor als die Augensumme 9?

## Geschichtliche Anmerkungen

- 4.040 Münzwürfe (2.048 Kopf) [BUFFON, 18. Jhd.]
- 26.306 Würfe von 12 Würfeln [WELDON, 1894]  
(85h bei 1 Wurf/s)
- 100.000 Würfe eines Würfels [WOLF,  $\approx$  1894]  
(27h bei 1 Wurf/s)

## GALILEO GALILEI (\* 1564; † 1642)

- ital. Mathematiker, Physiker, Astronom
- änderte unser Weltbild
- “kleinere” Dispute mit der kath. Kirche



## Lösung

- es gibt mehrere Möglichkeiten, dies zu modellieren
- $\Sigma = \{1, \dots, 6\} \times \{1, \dots, 6\} \times \{1, \dots, 6\}$   
(Ergebnis drei unterscheidbarer Würfel)
- $\mathcal{E} = \mathcal{P}(\Sigma)$  und Gleichverteilung  $p$
- An welchen Ereignissen sind wir interessiert?

$$\begin{aligned} E_9 &= \{(1, 2, 6), (1, 3, 5), (1, 4, 4), (1, 5, 3), (1, 6, 2), \\ &= \{(2, 1, 6), (2, 2, 5), (2, 3, 4), (2, 4, 3), (2, 5, 2), (2, 6, 1), \\ &= \{(3, 1, 5), (3, 2, 4), (3, 3, 3), (3, 4, 2), (3, 5, 1), \\ &= \{(4, 1, 4), (4, 2, 3), (4, 3, 2), (4, 4, 1), \\ &= \{(5, 1, 3), (5, 2, 2), (5, 3, 1), (6, 1, 2), (6, 2, 1)\} \end{aligned}$$

$$|E_{10}| = 27$$

- also gilt:  $p(E_9) = \frac{25}{216}$  und  $p(E_{10}) = \frac{27}{216}$

## Frage [TVERSKY, 1982]

- In Krankenhaus 1 werden jeden Tag **45 Kinder** entbunden, und in Krankenhaus 2 sind es **15 Kinder** pro Tag.
- Über das gesamte Jahr liegt der Anteil der Jungen an den entbundenen Kindern in beiden Krankenhäusern bei **50%**.
- In welchem Krankenhaus wird die Anzahl der Tage, an denen mehr als 60% Jungen geboren werden, größer sein?

## Lösung

in der Übung

## Frage [CHEVALIER DE MÉRÉ, PASCAL, FERMAT, 1654]

Wie wahrscheinlich ist mind. eine 6 bei 4 Würfen eines Würfels?

### CHEVALIER DE MÉRÉ (\* 1607; † 1684)

- franz. Schriftsteller und Spieler
- eigentlich ANTOINE GOMBAUD
- Unzulänglichkeiten der Mathematik

### PIERRE DE FERMAT (\* 1601; † 1665)

- franz. Mathematiker und Jurist
- analytische Geometrie und Optik
- bekannt für Randnotizen



## §8.9 Definition (Unabhängigkeit)

Sei  $(\Sigma, \mathcal{E}, p)$  ein Wahrscheinlichkeitsmaß und  $E_1, E_2 \in \mathcal{E}$ .

Die Ereignisse  $E_1$  und  $E_2$  sind **unabhängig** gdw.

$$p(E_1 \cap E_2) = p(E_1) \cdot p(E_2)$$

### Beispiel

gleichverteiltes Wahrscheinlichkeitsmaß  $(\Sigma, \mathcal{P}(\Sigma), p)$  mit

$$\Sigma = \{1, \dots, 6\}^4$$

- $E_{1i} = \{(i, j_1, j_2, j_3) \mid j_1, j_2, j_3 \in \{1, \dots, 6\}\}$        $i$  bei 1. Wurf
- ...
- $E_{4i} = \{(j_1, j_2, j_3, i) \mid j_1, j_2, j_3 \in \{1, \dots, 6\}\}$        $i$  bei 4. Wurf
- für alle  $1 \leq i, i' \leq 6$  sind  $E_{1i}$  und  $E_{2i'}$  unabhängig, denn

$$p(E_{1i} \cap E_{2i'}) = \frac{36}{1.296} = \frac{1}{36} = \frac{1}{6} \cdot \frac{1}{6} = \frac{216}{1.296} \cdot \frac{216}{1.296} = p(E_{1i}) \cdot p(E_{2i'})$$

## Lösung

Wir sind am Ereignis

$$E = \{(i_1, i_2, i_3, i_4) \mid 1 \leq i_1, i_2, i_3, i_4 \leq 6, \{i_1, i_2, i_3, i_4\} \}$$

interessiert. Wir betrachten zunächst  $E^c = \{1, \dots, 5\}^4$ . Aufgrund der Unabhängigkeit gilt  $p(E^c) = (\frac{5}{6})^4 = 0,48$ . Folglich gilt  $p(E) = 1 - p(E^c) = 0,52$ .

## Frage [CHEVALIER DE MÉRÉ, PASCAL, FERMAT, 1654]

Wie viele Würfe von 2 Würfeln braucht man, um mind. einmal ein 6er-Paar mit Wahrscheinlichkeit mind. 50% zu werfen?

### Notizen

- PASCAL und FERMAT errechneten Lösung 24
- Spieler DE MÉRÉ bestand darauf mit 24 Würfen zu verlieren  
(Unzulänglichkeit der Mathematik)

## Frage (IBM-PIN Ableitungsmethode [veraltet])

- Umwandlung der Konto- oder Kreditkartennummer ins Hexadezimalsystem (16 Stellen; 64 Bits)
- Verschlüsselung mit Bankschlüssel
- Reduktion auf die ersten 4 Stellen
- Ersetzung A  $\mapsto$  0, B  $\mapsto$  1, C  $\mapsto$  2, D  $\mapsto$  3, E  $\mapsto$  4 und F  $\mapsto$  5
- Ersetzung 0  $\mapsto$  1 angewandt auf 1. Stelle

Wie wahrscheinlich ist die PIN 1234?

## Notiz

- nach Verschlüsselung kann von Gleichverteilung der Ergebnisse ausgegangen werden

## Lösung

- Elementarereignisse  $\Sigma = \{0, \dots, 9, A, \dots, F\}^4$  und Ereignisse  $\mathcal{E} = \mathcal{P}(\Sigma)$
- gleichverteiltes Wahrscheinlichkeitsmaß
- relevantes Ereignis

$$E = \{d_1 d_2 d_3 d_4 \mid d_1 \in \{0, 1, A, B\}, d_2 \in \{2, C\}, \\ d_3 \in \{3, D\}, d_4 \in \{4, E\}\}$$

- $p(E) = \frac{4 \cdot 2 \cdot 2 \cdot 2}{16 \cdot 16 \cdot 16 \cdot 16} = \frac{1}{4 \cdot 8 \cdot 8 \cdot 8} = \frac{1}{2.048}$
- entspricht 0,05% statt der “erwarteten” 0,01%
- System extrem anfällig; wird nicht länger verwendet  
( $\leq 20$  Versuche genügten im Mittel, um PIN zu erraten)

Bedingte Wahrscheinlichkeiten

## Motivation

Ihr Kühlschrank funktioniert nicht mehr

Ursache	Wahrscheinlichkeit
nicht eingesteckt	0,4
Sicherung raus	0,2
Motor kaputt	0,1
Kühlmittelleck	0,1
Stromkabel kaputt	0,1
Sabotage durch Aliens	0,05
...	...

Beobachtung: Das Licht im Inneren funktioniert noch

## Motivation

Ihr Kühlschrank funktioniert nicht mehr

Ursache	Wahrscheinlichkeit
nicht eingesteckt	0
Sicherung raus	0
Motor kaputt	0,1
Kühlmittelleck	0,1
Stromkabel kaputt	0
Sabotage durch Aliens	0,05
...	...

Beobachtung: Das Licht im Inneren funktioniert noch

## §8.10 Definition

Seien  $(\Sigma, \mathcal{E}, p)$  ein Wahrscheinlichkeitsmaß und  $E, E' \in \mathcal{E}$  Ereignisse mit  $p(E') \neq 0$ .

Dann ist  $p(E|E')$  die Wahrscheinlichkeit von  $E$  unter Bedingung  $E'$   
(auch: Wahrscheinlichkeit von  $E$  gegeben  $E'$ )  
und es gilt:

$$p(E|E') = \frac{p(E \cap E')}{p(E')}$$

## §8.11 Theorem

Seien  $(\Sigma, \mathcal{E}, p)$  ein Wahrscheinlichkeitsmaß und  $E, E' \in \mathcal{E}$  Ereignisse mit  $p(E') \neq 0$ . Folgende Aussagen sind äquivalent:

- ①  $E$  und  $E'$  sind unabhängig
- ②  $p(E|E') = p(E)$

### Beweis.

Wir beweisen beide Richtungen.

- ① → ②: Sei also  $p(E \cap E') = p(E) \cdot p(E')$ . Damit gilt

$$p(E|E') = \frac{p(E \cap E')}{p(E')} = \frac{p(E) \cdot p(E')}{p(E')} = p(E)$$

- ② → ①: Sei  $p(E|E') = p(E)$ . Dann gilt

$$p(E) = p(E|E') = \frac{p(E \cap E')}{p(E')} \quad \text{also} \quad p(E \cap E') = p(E) \cdot p(E')$$

□

## §8.12 Theorem (Formel von BAYES)

Seien  $(\Sigma, \mathcal{E}, p)$  ein Wahrscheinlichkeitsmaß und  $E, E' \in \mathcal{E}$  Ereignisse mit  $p(E) \neq 0$  und  $p(E') \neq 0$ .

$$p(E|E') = \frac{p(E'|E) \cdot p(E)}{p(E')}$$

Beweis.

Direkt:

$$p(E|E') = \frac{p(E \cap E')}{p(E')} = \frac{p(E \cap E') \cdot p(E)}{p(E') \cdot p(E)} = \frac{p(E'|E) \cdot p(E)}{p(E')}$$

□

THOMAS BAYES (\* 1701; † 1761)

- engl. Statistiker und Pfarrer
- begründete eine neue Interpretation
- Formel von BAYES erst nach Tod publiziert



## Frage

- Eine Firma entwickelt einen Test für einen Krebs, an dem nur 0,1% aller Menschen leiden.
- Der Test hat 99% Sensitivität und 95% Spezifität.
  - Sensitivität:  $p(\text{positiv}|\text{Krebs}) = 0,99$
  - Spezifität:  $p(\text{negativ}|\text{gesund}) = 0,95$
- Wie hoch ist die Wahrscheinlichkeit für eine Erkrankung mit diesem Krebs bei einem positiven Testergebnis?

## Lösung

- Elementarereignisse:  $\Sigma = \{(k, +), (k, -), (g, +), (g, -)\}$   
 $k = \text{krank}, g = \text{gesund}, +/ - \text{ Ergebnis des Tests}$
- Ereignisse  $\mathcal{E} = \mathcal{P}(\Sigma)$ 
  - $E_{\text{krank}} = \{(k, +), (k, -)\}$  und  $E_{\text{gesund}} = \{(g, +), (g, -)\}$
  - $E_+ = \{(k, +), (g, +)\}$  und  $E_- = \{(k, -), (g, -)\}$
- $p(E_{\text{krank}}) = 0,001$
- $p(E_+ | E_{\text{krank}}) = 0,99$  und  $p(E_- | E_{\text{gesund}}) = 0,95$
- Berechnung:

$$\begin{aligned} p(E_{\text{krank}} | E_+) &= \frac{p(E_+ | E_{\text{krank}}) \cdot p(E_{\text{krank}})}{p(E_+)} && (\S 8.12) \\ &= \frac{p(E_+ | E_{\text{krank}}) \cdot p(E_{\text{krank}})}{p(E_+ | E_{\text{krank}}) \cdot p(E_{\text{krank}}) + p(E_+ | E_{\text{gesund}}) \cdot p(E_{\text{gesund}})} \\ &= \frac{0,99 \cdot 0,001}{0,99 \cdot 0,001 + 0,05 \cdot 0,999} = 0,019 \end{aligned}$$

## Notizen

- nur 2% aller positiv getesteten Personen sind krank
- Tests für seltene Krankheiten schwierig
- **aber** kann zum Ausschluss dienen

$$p(E_{\text{gesund}}|E_-) = 0.999989 \quad (99,999\%)$$

- Rechnen mit Binomialkoeffizienten
- Grundlagen der Stochastik
- Unabhängigkeit
- Bedingte Wahrscheinlichkeiten

# Diskrete Strukturen

## Vorlesung 9: Verbände

Andreas Maletti

16. Dezember 2014

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## heutige Vorlesung

- ① kleinste obere Schranke und größte untere Schranke
- ② Einführung Verbände
- ③ Eigenschaften von Verbänden
- ④ Korrespondenz Ordnungsstruktur & algebraische Darstellung

Bitte Fragen direkt stellen!

Organisation

## Prüfung

am **20.02.2015** um 09:00 Uhr im HS 3 und im AudiMax

## Tutorium

- ANDREAS MALETTI: 19. Dezember (Fr.), 15 Uhr **im Hs. 5**
- CHRISTOPH GAMM: 9. Januar (Fr.), 15 Uhr **im Hs. 5**
- DOREEN HEUSEL: 16. Januar (Fr.), 15 Uhr **im Hs. 5**
- THOMAS WEIDNER: 23. Januar (Fr.), 15 Uhr **im Hs. 5**
- CLAUDIO RÖHL: 29. Januar (Do.), 17 Uhr
- ANDREAS MALETTI: 6. Februar (Fr.), 15 Uhr **im Hs. 5**

## Supremum und Infimum

## Inhalt

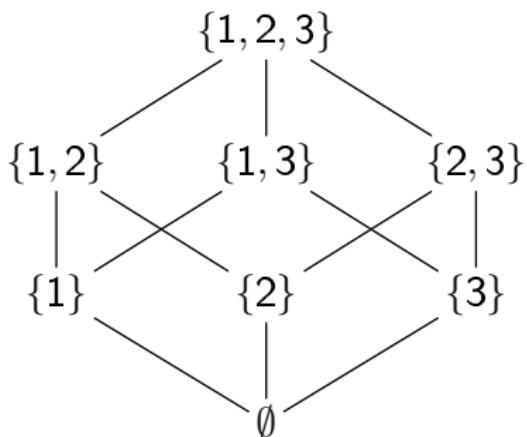
- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ **Algebraische Strukturen**
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## Definition (§4.14 — Ordnungsrelation)

Eine Relation  $\preceq$  auf  $M$  ist eine **Ordnungsrelation**  
gdw. sie reflexiv, antisymmetrisch und transitiv ist.

Das Paar  $(M, \preceq)$  heißt dann **teilweise geordnete Menge**.

Ist  $\preceq$  linear, dann heißt  $(M, \preceq)$  auch **linear geordnete Menge**.



## Definition (§5.6)

Sei  $(M, \preceq)$  eine teilweise geordnete Menge und  $M' \subseteq M$ . Ein Element  $m \in M$  ist

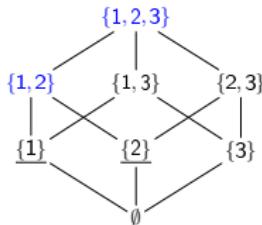
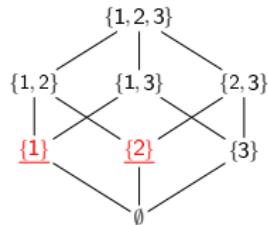
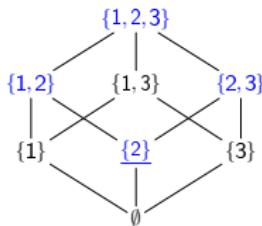
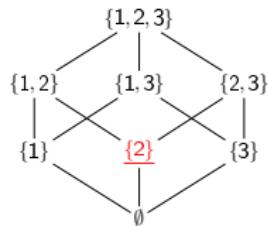
- eine **obere Schranke für  $M'$**  gdw.  $m' \preceq m$  für alle  $m' \in M'$   
(größer als alle Elemente aus  $M'$ )
- **das größte Element von  $M'$**  gdw.  $m \in M'$  und  $m \in \uparrow M'$  ist  
(obere Schranke von  $M'$ , die in  $M'$  liegt)
- **maximal in  $M'$**  gdw.  $m \in M'$  und  $m \not\prec m'$  für alle  $m' \in M'$   
(es gibt keine echt größeren Elemente in  $M'$ )

## Notation

Sei  $(M, \preceq)$  eine teilweise geordnete Menge und  $M' \subseteq M$

$$\uparrow M' = \{m \in M \mid (\forall m' \in M').(m' \preceq m)\}$$

Menge der oberen Schranken von  $M'$



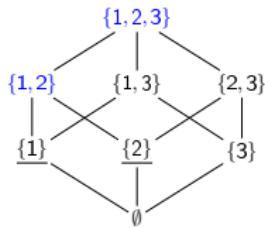
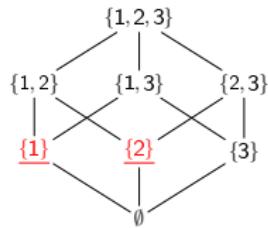
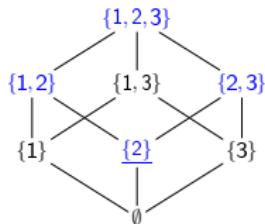
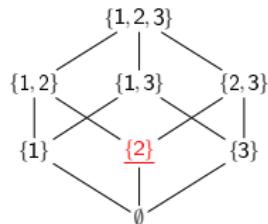
## Beispiele

- obere Schranken von  $\{\{2\}\}$ :

$$\uparrow\{\{2\}\} = \{\{2\}, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}\}$$

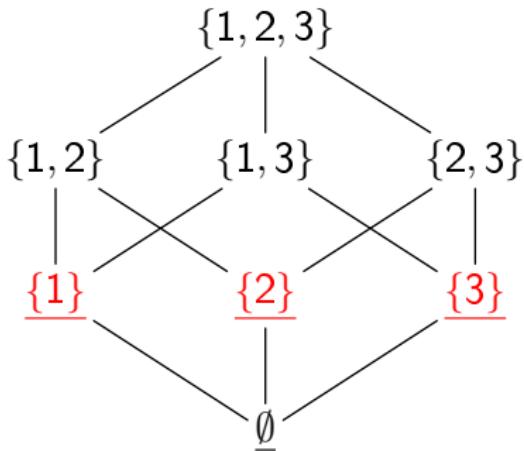
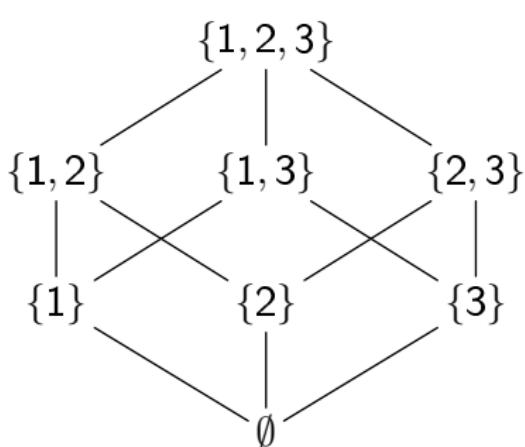
- obere Schranken von  $\{\{1\}, \{2\}\}$ :

$$\uparrow\{\{1\}, \{2\}\} = \{\{1, 2\}, \{1, 2, 3\}\}$$



## Beispiele

- größte Element von  $\{\{2\}\}$  ist  $\{2\}$
- größte Element von  $\{\{1\}, \{2\}\}$  existiert nicht



## Beispiele

- nur  $\{1, 2, 3\}$  ist maximal in  $\mathcal{P}(\{1, 2, 3\})$
- $\{1\}$ ,  $\{2\}$  und  $\{3\}$  sind maximal in  $\{\emptyset, \{1\}, \{2\}, \{3\}\}$
- $(\mathbb{N}, \leq)$  hat **kein** maximales Element in  $\mathbb{N}$

## §9.1 Zusammenhänge

Sei  $(M, \preceq)$  eine teilweise geordnete Menge und  $M' \subseteq M$  beliebig.

- Jede obere Schranke für  $M'$  ist maximal in  $M$  X
- Jede obere Schranke für  $M'$  ist maximal in  $M'$  X
- Jede obere Schranke für  $M$  ist maximal in  $M$  ✓
- Jede obere Schranke für  $M$  ist das größte Element von  $M'$  X
- Jede obere Schranke für  $M$  ist das größte Element von  $M$  ✓
- Jedes maximale Element in  $M'$  ist obere Schranke für  $M'$  X
- Jedes maximale Element in  $M$  ist obere Schranke für  $M$  X
- Das größte Element von  $M'$  ist maximal in  $M'$  ✓
- Das größte Element von  $M'$  ist obere Schranke für  $M'$  ✓

## Definition (Analog zu §5.6)

Sei  $(M, \preceq)$  eine teilweise geordnete Menge und  $M' \subseteq M$ . Ein Element  $m \in M$  ist

- eine **untere Schranke für  $M'$**  gdw.  $m \preceq m'$  für alle  $m' \in M'$   
(kleiner als alle Elemente aus  $M'$ )
- **das kleinste Element von  $M'$**  gdw.  $m \in M'$  und  $m \in \downarrow M'$   
(untere Schranke von  $M'$ , die in  $M'$  liegt)
- **minimal in  $M'$**  gdw.  $m \in M'$  und  $m' \not\preceq m$  für alle  $m' \in M'$   
(es gibt keine echt kleineren Elemente in  $M'$ )

## Notation

Sei  $(M, \preceq)$  eine teilweise geordnete Menge und  $M' \subseteq M$

$$\downarrow M' = \{m \in M \mid (\forall m' \in M').(m \preceq m')\}$$

Menge der unteren Schranken von  $M'$

## Notizen

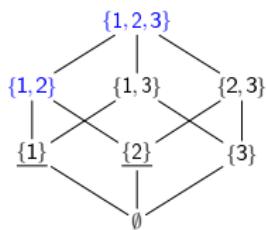
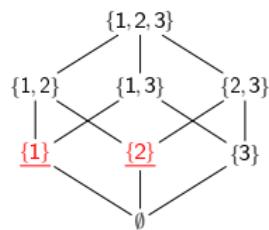
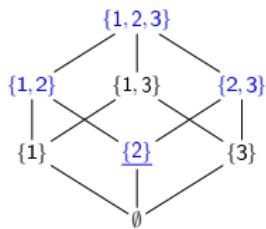
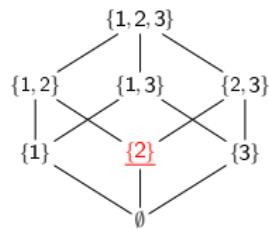
- es gibt höchstens ein größtes (bzw. kleinstes) Element von  $M'$  (einfacher Beweis unter Nutzung von Antisymmetrie)
- **aber** es kann mehrere maximale (bzw. minimale) Elemente in  $M'$  geben
- die Zusammenhänge gelten analog für untere Schranken, minimale und kleinste Elemente
- $\uparrow\emptyset = \downarrow\emptyset = M$

## §9.2 Definition

Sei  $(M, \preceq)$  eine teilweise geordnete Menge und  $M' \subseteq M$ .

- Das **Supremum von  $M'$**  ist das kleinste Element von  $\uparrow M'$   
(kleinste obere Schranke für  $M'$ )
- Das **Infimum von  $M'$**  ist das größte Element von  $\downarrow M'$   
(größte untere Schranke für  $M'$ )
- Sollten solche Elemente nicht existieren,  
dann existiert auch das Supremum/Infimum nicht
- Falls sie existieren, dann schreiben wir auch
  - $\sup M'$  für das Supremum von  $M'$
  - $\inf M'$  für das Infimum von  $M'$

# Verbände — Supremum und Infimum



## Beispiele

- Supremum von  $\{\{2\}\}$  ist  $\{2\} = \sup\{\{2\}\}$
- Supremum von  $\{\{1\}, \{2\}\}$  ist  $\{1, 2\} = \sup\{\{1\}, \{2\}\}$

## §9.3 Theorem

Sei  $(\mathcal{M}, \subseteq)$  eine teilweise geordnete Menge mit  $\mathcal{M} \subseteq \mathcal{P}(M)$  für eine Menge  $M$ . Für jede Teilmenge  $\mathcal{M}' \subseteq \mathcal{M}$  mit  $\bigcup \mathcal{M}' \in \mathcal{M}$  gilt  $\bigcup \mathcal{M}' = \sup \mathcal{M}'$ .

### Beweis.

Wir zeigen zunächst, dass  $\bigcup \mathcal{M}'$  eine obere Schranke für  $\mathcal{M}'$  ist. Sei  $M' \in \mathcal{M}'$  beliebig. Dann gilt  $M' \subseteq \bigcup \mathcal{M}'$ , womit  $\bigcup \mathcal{M}'$  obere Schranke ist.

Nach §6.2 ist  $\bigcup \mathcal{M}'$  die kleinste obere Schranke. Also ist  $\bigcup \mathcal{M}'$  das Supremum von  $\mathcal{M}'$ . □

## Notation

- wir schreiben auch  $m_1 \vee m_2$  statt  $\sup\{m_1, m_2\}$
- wir schreiben auch  $m_1 \wedge m_2$  statt  $\inf\{m_1, m_2\}$
- warum wir hier auch  $\vee$  und  $\wedge$  verwenden, wird gleich klar

Verbände

## §9.4 Definition (Verband)

Eine teilweise geordnete Menge  $(M, \preceq)$  heißt **Verband** gdw.  
für alle  $m_1, m_2 \in M$

- das Supremum von  $\{m_1, m_2\}$  und  $(m_1 \vee m_2)$
- das Infimum von  $\{m_1, m_2\}$   $(m_1 \wedge m_2)$

existieren. Weiterhin heißt  $(M, \preceq)$  **vollständiger Verband** gdw.  
sogar die Suprema und Infima beliebiger Teilmengen  $M' \subseteq M$   
existieren.

## Notizen

- jeder vollständige Verband ist ein Verband
- jeder vollständige Verband  $(M, \preceq)$  hat
  - das größte Element  $\inf \emptyset$  in  $M$  und  $(\downarrow \emptyset = M)$
  - das kleinste Element  $\sup \emptyset$  in  $M$   $(\uparrow \emptyset = M)$

## Beispiele

- $(\{0, 1\}, R)$  mit  $R = \{(0, 0), (0, 1), (1, 1)\}$   
ist ein vollständiger Verband mit

- $\sup B = 1$  gdw.  $1 \in B$  (entspricht 'oder')
- $\inf B = 1$  gdw.  $0 \notin B$  (entspricht 'und')

größtes Element 1 und kleinstes Element 0

- $(\mathcal{P}(M), \subseteq)$  für Menge  $M$  ist vollständiger Verband mit

- $\sup \mathcal{M} = \bigcup \mathcal{M}$  (siehe §9.3)
- $\inf \mathcal{M} = \bigcap \mathcal{M}$  (analog zu §9.3)

größtes Element  $M$  und kleinstes Element  $\emptyset$

## §9.5 Definition (Distributivitat)

Ein Verband  $(M, \preceq)$  ist **distributiv** gdw. fur alle  $m_1, m_2, m_3 \in M$

$$m_1 \wedge (m_2 \vee m_3) = (m_1 \wedge m_2) \vee (m_1 \wedge m_3)$$

$$m_1 \vee (m_2 \wedge m_3) = (m_1 \vee m_2) \wedge (m_1 \vee m_3)$$

## Beispiele

- $(\{0, 1\}, R)$  mit  $R = \{(0, 0), (0, 1), (1, 1)\}$   
ist ein vollstandiger und distributiver Verband
- $(\mathcal{P}(M), \subseteq)$  fur Menge  $M$   
ist ein vollstandiger und distributiver Verband

## §9.6 Theorem

Jede linear geordnete Menge  $(M, \preceq)$  ist ein distributiver Verband

Beweis (1/2).

Wir müssen die Eigenschaften eines Verbandes und die Distributivität beweisen.

- **Supremum:** Für alle  $m_1, m_2 \in M$  gilt entweder  $m_1 \preceq m_2$  oder  $m_2 \preceq m_1$ . Ohne Beschränkung der Allgemeinheit (oBdA) sei  $m_1 \preceq m_2$ . Dann ist  $m_2$  obere Schranke für  $\{m_1, m_2\}$ . Sei  $m$  eine andere obere Schranke für  $\{m_1, m_2\}$ . Dann gilt  $m_2 \preceq m$  und damit ist  $m_2$  die kleinste obere Schranke für  $\{m_1, m_2\}$ .
- **Infimum:** analog

## Beweis (2/2).

Wir müssen die Eigenschaften eines Verbandes und die Distributivitat beweisen.

- **Distributivitat:** Seien  $m_1, m_2, m_3 \in M$ . Seien  $m = (m_1 \wedge m_2) \vee (m_1 \wedge m_3)$  und  $m' = (m_1 \vee m_2) \wedge (m_1 \vee m_3)$ .

Ordnung	$m_1 \wedge (m_2 \vee m_3)$	$m$	$m_1 \vee (m_2 \wedge m_3)$	$m'$
$m_1 \preceq m_2 \preceq m_3$	$m_1$	$m_1$	$m_2$	$m_2$
$m_1 \preceq m_3 \preceq m_2$	$m_1$	$m_1$	$m_3$	$m_3$
$m_2 \preceq m_1 \preceq m_3$	$m_1$	$m_1$	$m_1$	$m_1$
$m_2 \preceq m_3 \preceq m_1$	$m_3$	$m_3$	$m_1$	$m_1$
$m_3 \preceq m_1 \preceq m_2$	$m_1$	$m_1$	$m_1$	$m_1$
$m_3 \preceq m_2 \preceq m_1$	$m_2$	$m_2$	$m_1$	$m_1$



## Notizen

- $(\mathbb{N}, \leq)$ ,  $(\mathbb{Z}, \leq)$ ,  $(\mathbb{Q}, \leq)$ ,  $(\mathbb{R}, \leq)$  sind distributive Verbände  
[siehe §9.6]
- aber **nicht** vollständig, denn  $\sup \mathbb{N}$  existiert nicht

## §9.7 Theorem

Für jeden Verband  $(M, \preceq)$  und alle  $m_1, m_2, m_3 \in M$  gelten

- $m_1 \vee m_1 = m_1$  und  $m_1 \wedge m_1 = m_1$  Idempotenz
- $m_1 \vee m_2 = m_2 \vee m_1$  und  $m_1 \wedge m_2 = m_2 \wedge m_1$  Kommutativität
- $m_1 \vee (m_2 \vee m_3) = (m_1 \vee m_2) \vee m_3$  und  
 $m_1 \wedge (m_2 \wedge m_3) = (m_1 \wedge m_2) \wedge m_3$  Assoziativität
- $m_1 \vee (m_1 \wedge m_2) = m_1$  und  $m_1 \wedge (m_1 \vee m_2) = m_1$  Absorption

Beweis.

in der Übung



## §9.8 Theorem

Sei  $(M, \preceq)$  ein Verband. Für jede endliche Teilmenge  $M' \subseteq M$  existieren  $\sup M'$  und  $\inf M'$ .

Beweis.

Sei  $M' = \{m_1, \dots, m_n\}$ . Wir zeigen, dass

$$\sup M' = m_1 \vee \cdots \vee m_n \quad \text{und} \quad \inf M' = m_1 \wedge \cdots \wedge m_n$$

Wir zeigen dies für das Supremum (analog für Infimum).

- Offensichtlich ist  $m_1 \vee \cdots \vee m_n$  obere Schranke für  $M'$ .
- Sei  $m$  eine obere Schranke für  $M'$ . Dann ist  $m$  obere Schranke für  $\{m_1, m_2\}$  und damit  $m_1 \vee m_2 \preceq m$ . Also ist  $m$  auch obere Schranke für  $\{m_1 \vee m_2, m_3\}$  und damit  $(m_1 \vee m_2) \vee m_3 \preceq m$  ... Letztlich gilt damit auch  $m_1 \vee \cdots \vee m_n \preceq m$ , womit  $m_1 \vee \cdots \vee m_n$  die kleinste obere Schranke ist.

□

## §9.9 Korollar

Jeder Verband  $(M, \preceq)$  mit endlichem  $M$  ist vollständig

## Definition (§8.3)

Sei  $\mathcal{E} \subseteq \mathcal{P}(\Sigma)$  für Menge  $\Sigma$ . Dann ist  $(\Sigma, \mathcal{E})$  ein **Maßraum** gdw.

- $\Sigma \in \mathcal{E}$  (Grundmenge enthalten)
- $\Sigma \setminus E \in \mathcal{E}$  für alle  $E \in \mathcal{E}$  (abgeschlossen unter Komplement)
- $\bigcup_{i \in \mathbb{N}} E_i \in \mathcal{E}$  für alle  $E_0, E_1, \dots \in \mathcal{E}$   
(abgeschlossen unter abzählbarer Vereinigung)

## Theorem (§8.4)

Für jeden Maßraum  $(\Sigma, \mathcal{E})$  gilt  $\bigcap_{i \in \mathbb{N}} E_i \in \mathcal{E}$  für alle  $E_0, E_1, \dots \in \mathcal{E}$

## §9.10 Theorem (nutzt Auswahlaxiom)

Jeder Maßraum  $(\Sigma, \mathcal{E})$  liefert einen distributiven Verband  $(\mathcal{E}, \subseteq)$ .  
Ist  $\Sigma$  abzählbar, dann ist  $(\mathcal{E}, \subseteq)$  sogar vollständig.

### Beweis (1/2).

Wir wissen, dass  $E_1 \cup E_2 \in \mathcal{E}$  und  $E_1 \cap E_2 \in \mathcal{E}$  [§8.4] und dies sind Supremum und Infimum von  $\{E_1, E_2\}$ . Aufgrund der Rechenregeln der Mengenlehre gilt die Distributivität.

Beweis (2/2).

Sei  $\mathcal{E}' \subseteq \mathcal{E}$  ( $\mathcal{E}'$  ist evtl. nicht abzählbar). Wir wissen bereits, dass  $\sup \mathcal{E}' = \bigcup \mathcal{E}'$  in  $(\mathcal{P}(\Sigma), \subseteq)$ .

(d.h.,  $\bigcup \mathcal{E}'$  ist kleinste obere Schranke für  $\mathcal{E}'$ )

Wir müssen aber noch zeigen, dass  $\bigcup \mathcal{E}' \in \mathcal{E}$ .

Sei  $\Sigma$  abzählbar. Für jedes  $\sigma \in \Sigma$ , seien

$$\mathcal{E}_\sigma = \{E \in \mathcal{E}' \mid \sigma \in E\} \quad \text{und} \quad \mathfrak{E} = \{\mathcal{E}_\sigma \mid \sigma \in \Sigma\} \setminus \{\emptyset\}$$

Gemäß Auswahlaxiom existiert  $c: \mathfrak{E} \rightarrow \bigcup_{\sigma \in \Sigma} \mathcal{E}_\sigma$ , so dass  $c(\mathcal{E}'') \in \mathcal{E}''$  für alle  $\mathcal{E}'' \in \mathfrak{E}$ . Also  $c(\mathcal{E}_\sigma) \in \mathcal{E}_\sigma$  für alle  $\sigma \in \Sigma$  mit  $\mathcal{E}_\sigma \neq \emptyset$ . Also gilt  $c(\mathcal{E}_\sigma) \in \mathcal{E}'$ .

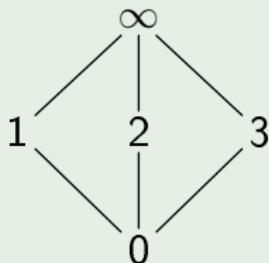
Des Weiteren gilt  $\bigcup \mathcal{E}' = \bigcup_{\sigma \in \Sigma, \mathcal{E}_\sigma \neq \emptyset} c(\mathcal{E}_\sigma)$  (siehe Übung). Da  $c(\mathcal{E}_\sigma) \in \mathcal{E}' \subseteq \mathcal{E}$  für alle  $\sigma \in \Sigma$  mit  $\mathcal{E}_\sigma \neq \emptyset$  und  $\mathcal{E}$  unter abzählbarer Vereinigung abgeschlossen ist, ist auch

$$\bigcup_{\sigma \in \Sigma, \mathcal{E}_\sigma \neq \emptyset} c(\mathcal{E}_\sigma) = \bigcup \mathcal{E}' \in \mathcal{E}. \quad (\text{analog für Infimum})$$

□

## weitere Beispiele

- vollständiger Verband, der nicht distributiv ist



denn  $1 \vee (2 \wedge 3) = 1 \vee 0 = 1$

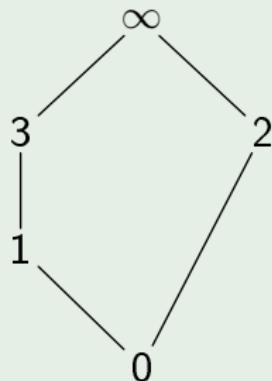
aber  $(1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (\infty \vee 3) = \infty \wedge \infty = \infty$

- $(\mathcal{M}, \subseteq)$  mit  $\mathcal{M} = \{N \subseteq \mathbb{N} \mid N \text{ endlich}\}$  ist distributiver Verband, der nicht vollständig ist

(kein größtes Element)

## weitere Beispiele

- vollständiger Verband, der nicht distributiv ist



$$\text{denn } 1 \vee (2 \wedge 3) = 1 \vee 0 = 1$$

$$\text{aber } (1 \vee 2) \wedge (1 \vee 3) = \infty \wedge (1 \vee 3) = \infty \wedge 3 = 3$$

Korrespondenz

## Motivation

- wir können auch “Mengen” von komplizierten Objekten betrachten
- Beispiele

$$\text{Verb} = \{(M, \preceq) \mid (M, \preceq) \text{ Verband}\}$$

$$\text{Zerl} = \{(M, \mathcal{M}) \mid \mathcal{M} \text{ Zerlegung von } M\}$$

$$\ddot{\text{A}}\text{q} = \{(M, \equiv) \mid \equiv \text{ Äquivalenzrelation auf } M\}$$

## §9.11 Theorem

Die Funktion  $f: \ddot{\text{Aq}} \rightarrow \text{Zerl}$  mit

$$f((M, \equiv)) = (M, (M/\equiv))$$

für alle  $(M, \equiv) \in \ddot{\text{Aq}}$  ist bijektiv

### Beweis.

Für jede Äquivalenzrelation  $\equiv$  auf  $M$  ist  $(M/\equiv)$  eine Zerlegung von  $M$  gemäß §4.6. Also gilt  $f((M, \equiv)) \in \text{Zerl}$ .

Des Weiteren gibt es nach §4.7 eine Funktion  $g: \text{Zerl} \rightarrow \ddot{\text{Aq}}$ , so dass  $f ; g = \text{id}_{\ddot{\text{Aq}}}$  und  $g ; f = \text{id}_{\text{Zerl}}$  (siehe §4.8).

Damit ist  $f$  invertierbar und deshalb nach §5.7 bijektiv. □

## Kurzeinführung

- **algebraische Struktur** ist eine Menge  $M$  zusammen mit Relationen, Funktionen, und Konstanten auf  $M$
- häufig unterliegen diese weiteren Einschränkungen

## Beispiele

- $(\mathbb{N}, \text{nachfolger}, 0)$  ist eine algebraische Struktur mit
  - einer Funktion nachfolger:  $\mathbb{N} \rightarrow \mathbb{N}$  und
  - einer Konstante  $0 \in \mathbb{N}$
- PEANO-Axiome beschreiben algebraische Strukturen  $(N, s, z)$  mit (siehe §5.11)
  - einer Funktion  $s: N \rightarrow N$  und (speziell: injektiver Funktion)
  - einer Konstante  $z \in N$  (mit weiteren Eigenschaften)
- jede teilweise geordnete Menge  $(M, \preceq)$  ist eine algebraische Struktur mit
  - einer Relation  $\preceq \subseteq M \times M$  (speziell: einer Ordnungsrelation)

## Theorem (§9.7)

Für jeden Verband  $(M, \preceq)$  und alle  $m_1, m_2, m_3 \in M$  gelten

- $m_1 \vee m_1 = m_1$  und  $m_1 \wedge m_1 = m_1$  Idempotenz
- $m_1 \vee m_2 = m_2 \vee m_1$  und  $m_1 \wedge m_2 = m_2 \wedge m_1$  Kommutativität
- $m_1 \vee (m_2 \vee m_3) = (m_1 \vee m_2) \vee m_3$  und  $m_1 \wedge (m_2 \wedge m_3) = (m_1 \wedge m_2) \wedge m_3$  Assoziativität
- $m_1 \vee (m_1 \wedge m_2) = m_1$  und  $m_1 \wedge (m_1 \vee m_2) = m_1$  Absorption

## Notizen

- für jeden Verband  $(M, \preceq)$  (selbst eine algebraische Struktur) existiert also eine algebraische Struktur  $(M, \vee, \wedge)$  mit den obigen Beschränkungen an die Funktionen  $\vee, \wedge: M \times M \rightarrow M$

## §9.12 Theorem

Sei  $M$  eine Menge und  $\sqcup, \sqcap: M \times M \rightarrow M$  zwei Funktionen, so dass für alle  $m_1, m_2, m_3 \in M$

- $m_1 \sqcup m_1 = m_1$  und  $m_1 \sqcap m_1 = m_1$  Idempotenz
- $m_1 \sqcup m_2 = m_2 \sqcup m_1$  und  $m_1 \sqcap m_2 = m_2 \sqcap m_1$  Kommutativität
- $m_1 \sqcup (m_2 \sqcup m_3) = (m_1 \sqcup m_2) \sqcup m_3$  und  $m_1 \sqcap (m_2 \sqcap m_3) = (m_1 \sqcap m_2) \sqcap m_3$  Assoziativität
- $m_1 \sqcup (m_1 \sqcap m_2) = m_1$  und  $m_1 \sqcap (m_1 \sqcup m_2) = m_1$  Absorption

Dann ist  $(M, \preceq)$  ein Verband, wobei

$$\preceq = \{(m, m') \in M \times M \mid m = m \sqcap m'\}$$

## Beweis (1/2).

Für alle  $m, m' \in M$  ist also  $m \preceq m'$  gdw.  $m = m \sqcap m'$ . Wir weisen zunächst die Eigenschaften einer Ordnungsrelation nach:

- **reflexiv:** Für jedes  $m \in M$  gilt  $m = m \sqcap m$  (Idempotenz) also auch  $m \preceq m$ .
- **antisymmetrisch:** Seien  $m \preceq m'$  und  $m' \preceq m$ . D.h.  $m = m \sqcap m'$  und  $m' = m' \sqcap m$ . Mit Hilfe der Kommutativität gilt dann

$$m = m \sqcap m' = m' \sqcap m = m'$$

- **transitiv:** Seien  $m \preceq m'$  und  $m' \preceq m''$ . D.h.  $m = m \sqcap m'$  und  $m' = m' \sqcap m''$ . Unter Nutzung der Assoziativität erhalten wir

$$m = m \sqcap m' = m \sqcap (m' \sqcap m'') = (m \sqcap m') \sqcap m'' = m \sqcap m''$$

und damit  $m \preceq m''$ .

## Beweis (2/2).

Für alle  $m, m' \in M$  ist also  $m \preceq m'$  gdw.  $m = m \sqcap m'$ . Wir weisen nun noch die Suprema (Infima analog) nach:

- **Supremum:** Seien  $m, m' \in M$ . Wir behaupten, dass  $m \sqcup m'$  das Supremum von  $\{m, m'\}$  ist.
  - **obere Schranke:** Es gilt  $m = m \sqcap (m \sqcup m')$  (Absorption) und damit  $m \preceq m \sqcup m'$ . Ebenso gilt  $m' = m' \sqcap (m' \sqcup m)$  und damit  $m' \preceq m \sqcup m'$ , da  $m' \sqcup m = m \sqcup m'$  (Kommutativität).
  - **kleinste obere Schranke:** Sei  $m'' \in M$ , so dass  $m \preceq m''$  und  $m' \preceq m''$ . D.h.  $m = m \sqcap m''$  und  $m' = m' \sqcap m''$ . Wir folgern zunächst mit Absorption und Kommutativität  
 $m \sqcup m'' = (m \sqcap m'') \sqcup m'' = m''$  und  
 $m' \sqcup m'' = (m' \sqcap m'') \sqcup m'' = m''$ . Damit ergibt sich nun

$$\begin{aligned}(m \sqcup m') \sqcap m'' &= (m \sqcup m') \sqcap (m \sqcup m'') \\&= (m \sqcup m') \sqcap (m \sqcup (m' \sqcup m'')) \\&= (m \sqcup m') \sqcap ((m \sqcup m') \sqcup m'') = (m \sqcup m')\end{aligned}$$

und damit  $(m \sqcup m') \preceq m''$ .

□

## Notizen

- §9.7 liefert algebraische Struktur ala §9.12 für jeden Verband
- §9.12 liefert Verband für jede derartige algebraische Struktur  
→ starke Korrespondenz

## §9.13 Korollar

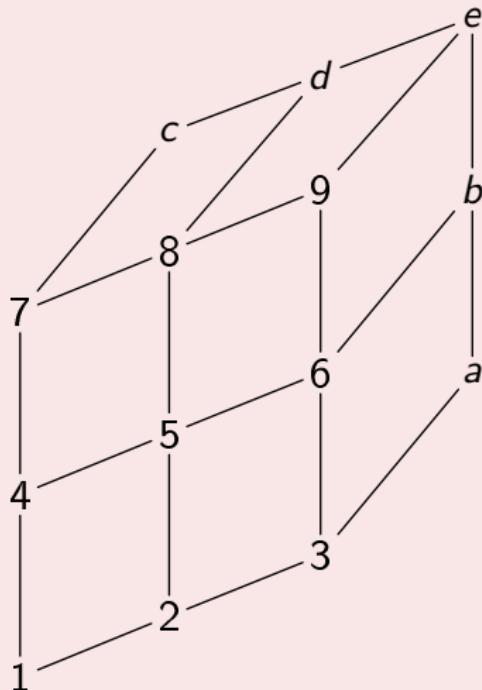
Die Funktion  $f$  mit  $f((M, \preceq)) = (M, \vee, \wedge)$  für alle Verbände  $(M, \preceq)$  ist bijektiv zwischen Verbänden und algebraischen Strukturen ala §9.12.

## Beweis.

Hier ohne Beweis. Es wäre noch zu zeigen, dass die Unwandlungen aus §9.7 und §9.12 unter Komposition die Identitäten liefern. □

## Abschlussfrage

Ist dies ein Verband? Vollständig? Distributiv?



Frohe Weihnachten und einen guten Start in 2015!

- Supremum und Infimum
- Grundlagen Verbände
- Eigenschaften von Verbänden
- Korrespondenzen

Zehnte Übungsserie ist bereits im OLAT.

# Diskrete Strukturen

## Vorlesung 10: BOOLESCHE ALGEBREN

Andreas Maletti

6. Januar 2015

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## heutige Vorlesung

- ① Algebraische Strukturen
- ② Einführung BOOLEsche Algebren
- ③ Eigenschaften von BOOLEschen Algebren
- ④ Isomorphiesatz

Bitte Fragen direkt stellen!

Organisation

## Prüfung

am **20.02.2015** um 09:00 Uhr im HS 3 und im AudiMax

- 1 DIN-A4-Blatt mit Notizen als Hilfsmittel zugelassen  
(beliebig beschrieben oder bedruckt)
- Abmeldung noch bis 25. Januar möglich

## Tutorium

- CHRISTOPH GAMM: 9. Januar (Fr.), 15 Uhr **im Hs. 5**
- DOREEN HEUSEL: 16. Januar (Fr.), 15 Uhr **im Hs. 5**
- THOMAS WEIDNER: 23. Januar (Fr.), 15 Uhr **im Hs. 5**
- CLAUDIO RÖHL: 29. Januar (Do.), 17 Uhr **im Hs. 17**
- ANDREAS MALETTI: 6. Februar (Fr.), 15 Uhr **im Hs. 5**

Wiederholung: Verbände

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ **Algebraische Strukturen**
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## Definition (§9.2)

Sei  $(M, \preceq)$  eine teilweise geordnete Menge und  $M' \subseteq M$ .

- Das **Supremum von  $M'$**  ist das kleinste Element von  $\uparrow M'$   
(kleinste obere Schranke für  $M'$ )
- Das **Infimum von  $M'$**  ist das größte Element von  $\downarrow M'$   
(größte untere Schranke für  $M'$ )
- Sollten solche Elemente nicht existieren,  
dann existiert auch das Supremum/Infimum nicht
- Falls sie existieren, dann schreiben wir auch
  - $\sup M'$  für das Supremum von  $M'$
  - $\inf M'$  für das Infimum von  $M'$

## Definition (§9.4)

Eine teilweise geordnete Menge  $(M, \preceq)$  heißt **Verband** gdw.  
für alle  $m_1, m_2 \in M$

- das Supremum von  $\{m_1, m_2\}$  und  $(m_1 \vee m_2)$
- das Infimum von  $\{m_1, m_2\}$   $(m_1 \wedge m_2)$

existieren. Weiterhin heißt  $(M, \preceq)$  **vollständiger Verband** gdw.  
sogar die Suprema und Infima beliebiger Teilmengen  $M' \subseteq M$   
existieren.

## Definition (§9.5)

Ein Verband  $(M, \preceq)$  ist **distributiv** gdw. für alle  $m_1, m_2, m_3 \in M$

$$m_1 \wedge (m_2 \vee m_3) = (m_1 \wedge m_2) \vee (m_1 \wedge m_3)$$

$$m_1 \vee (m_2 \wedge m_3) = (m_1 \vee m_2) \wedge (m_1 \vee m_3)$$

Algebraische Strukturen

## Motivation

- bisher nur Korrespondenz via Bijektion  
(für jede Äquivalenzrelation gibt es eine Zerlegung, ...)
- häufig möchte man jedoch strukturerhaltende “Gleichheit”,  
die Umbenennungen der Elemente ignoriert
- **Ziel:** “gleich” rechnen in strukturäquivalenten Mengen
- daher zunächst Formalisierung ‘algebraische Struktur’



## §10.1 Definition

Sei  $U$  eine Grundmenge und seien

- $R_1, \dots, R_k \subseteq U \times U$  Relationen auf  $U$
- $f_1, \dots, f_\ell: U \times U \rightarrow U$  binäre (zweistellige) Funktionen auf  $U$
- $g_1, \dots, g_m: U \rightarrow U$  unäre (einstellige) Funktionen auf  $U$  und
- $c_1, \dots, c_n \in U$  Elemente (auch: Konstanten) von  $U$ .

Dann ist  $(U, (R_1, \dots, R_k), (f_1, \dots, f_\ell), (g_1, \dots, g_m), (c_1, \dots, c_n))$  eine **algebraische Struktur** des Typs  $(k, \ell, m, n)$ .

## Beispiele

- jede Äquivalenzrelation  $\equiv \subseteq M \times M$  liefert eine algebraische Struktur  $(M, (\equiv), (), (), ())$  des Typs  $(1, 0, 0, 0)$
- jeder Maßraum  $(\Sigma, \mathcal{M})$  liefert eine algebraische Struktur  $(\mathcal{M}, (), (\cup), (\cdot^c), (\Sigma))$  des Typs  $(0, 1, 1, 1)$

## Notizen

- **algebraische Struktur**  
= Grundmenge mit Relationen, Funktionen und Konstanten
- wir betrachten nur binäre und unäre Funktionen  
und (2-stellige) Relationen
- Reihenfolge im Typ:
  - 1 Anzahl Relationen
  - 2 Anzahl binärer Funktionen
  - 3 Anzahl unärer Funktionen
  - 4 Anzahl Konstanten
- wir lassen leere Blöcke am Ende weg  
und lassen die Gruppierung weg, falls offensichtlich  
z.B.  $(M, (\preceq))$  oder  $(M, \preceq)$  statt  $(M, (\preceq), (), (), ())$

## weitere Beispiele

- jede teilweise geordnete Menge  $(M, \preceq)$  ist eine algebraische Struktur des Typs  $(1, 0, 0, 0)$
- die PEANO-Axiome spezifizieren eine algebraische Struktur  $(N, s, z)$  des Typs  $(0, 0, 1, 1)$   
(Beschreibung der natürlichen Zahlen)
- jede Potenzmenge  $\mathcal{P}(M)$  liefert eine algebraische Struktur  $(\mathcal{P}(M), \subseteq, \cup, \cap, \cdot^c, \emptyset, M)$  des Typs  $(1, 2, 1, 2)$

## §10.2 Definition

Seien  $\mathcal{U} = (U, (R_1, \dots, R_k), (f_1, \dots, f_\ell), (g_1, \dots, g_m), (c_1, \dots, c_n))$  und  $\mathcal{U}' = (U', (R'_1, \dots, R'_k), (f'_1, \dots, f'_\ell), (g'_1, \dots, g'_m), (c'_1, \dots, c'_n))$  zwei algebraische Strukturen gleichen Typs. Eine Funktion  $\varphi: U \rightarrow U'$  heißt **Isomorphismus von  $\mathcal{U}$  nach  $\mathcal{U}'$** , gdw.

- $\varphi$  bijektiv ist,
- für alle  $1 \leq i \leq k$  und  $u_1, u_2 \in U$  gilt

$$(u_1, u_2) \in R_i \quad \text{gdw.} \quad (\varphi(u_1), \varphi(u_2)) \in R'_i$$

- für alle  $1 \leq i \leq \ell$  und  $u_1, u_2 \in U$  gilt

$$\varphi(f_i(u_1, u_2)) = f'_i(\varphi(u_1), \varphi(u_2))$$

- $\varphi(g_i(u)) = g'_i(\varphi(u))$  für alle  $1 \leq i \leq m$  und  $u \in U$ , und
- $\varphi(c_i) = c'_i$  für alle  $1 \leq i \leq n$ .

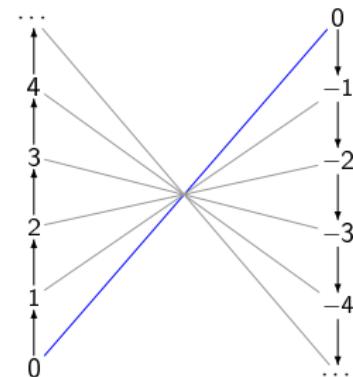
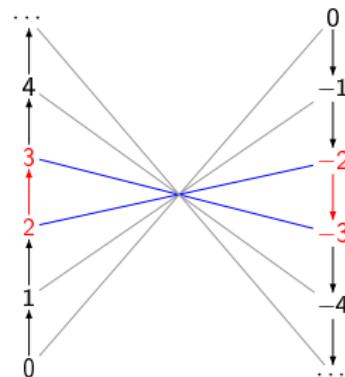
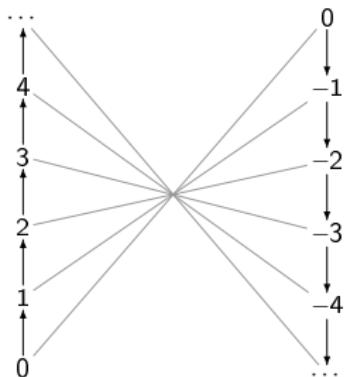
$\mathcal{U}$  und  $\mathcal{U}'$  heißen **isomorph**, gdw.  
ein Isomorphismus von  $\mathcal{U}$  nach  $\mathcal{U}'$  existiert.

## Beispiel

$(\mathbb{N}, \text{nachfolger}, 0)$  und  $(\{z \in \mathbb{Z} \mid z \leq 0\}, g, 0)$  mit  $g(z) = z - 1$  für alle  $z \leq 0$  sind isomorph

**Isomorphismus:**  $\varphi(n) = -n$  für alle  $n \in \mathbb{N}$

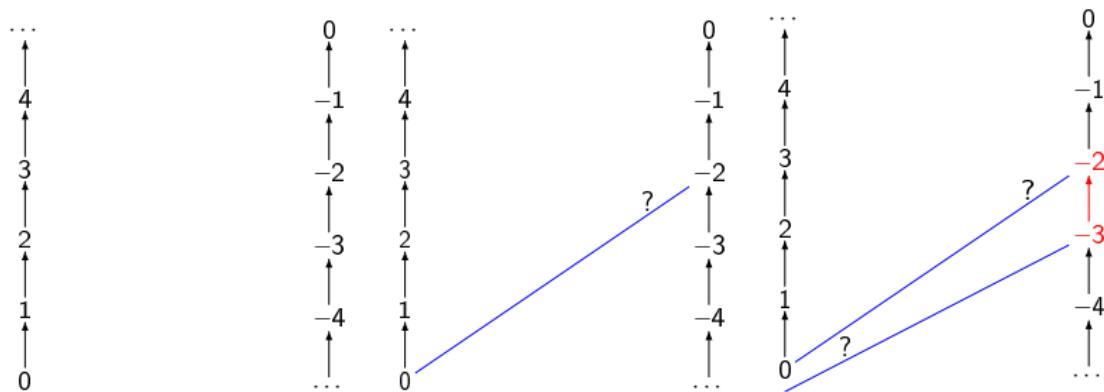
- $\varphi$  bijektiv (leicht nachweisbar)
- $\varphi(\text{nachfolger}(n)) = \varphi(n + 1) = -n - 1 = g(-n) = g(\varphi(n))$
- $\varphi(0) = 0$



## weiteres Beispiel

$(\mathbb{N}, \leq)$  und  $(\{z \in \mathbb{Z} \mid z \leq 0\}, \leq)$  sind **nicht** isomorph

**Beweis:** Sei  $\varphi$  Isomorphismus und  $z = \varphi(0)$ . Da  $z - 1 \leq 0$  und  $\varphi$  bijektiv, existiert  $n \in \mathbb{N} \setminus \{0\}$ , so dass  $\varphi(n) = z - 1$ . Es gilt  $0 \leq n$ , aber  $\varphi(0) = z \not\leq z - 1 = \varphi(n)$  im Widerspruch zur Isomorphismus-Eigenschaft. Also existiert kein Isomorphismus und die Strukturen sind daher nicht isomorph.



## §10.3 Theorem

Isomorphie ist eine Äquivalenzrelation auf algebraischen Strukturen eines bestimmten Typs.

Beweis.

in der Übung



## §10.4 Theorem

$\text{id}_{\mathbb{Q}}$  ist der einzige Isomorphismus von und auf  $(\mathbb{Q}, +, \cdot)$

Beweis (1/2).

Sei  $\varphi: \mathbb{Q} \rightarrow \mathbb{Q}$  ein Isomorphismus von und auf  $(\mathbb{Q}, +, \cdot)$ .

Wir zeigen zunächst  $\varphi(0) = 0$ ,  $\varphi(1) = 1$  und  $\varphi(-1) = -1$ .

- $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$ . Es gibt nur eine Zahl  $n \in \mathbb{Q}$ , so dass  $n = n + n$ . Also  $\varphi(0) = 0$ .
- $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$ . Es gibt nur zwei Zahlen  $n \in \mathbb{Q}$ , so dass  $n = n \cdot n$ . Da  $\varphi(0) = 0$  und  $\varphi$  injektiv ist, gilt also  $\varphi(1) = 1$ .
- $\varphi(1) = \varphi((-1) \cdot (-1)) = \varphi(-1) \cdot \varphi(-1)$ . Es gibt nur zwei Zahlen  $n \in \mathbb{Q}$ , so dass  $n = n \cdot n$ . Da  $\varphi(1) = 1$  und  $\varphi$  injektiv ist, gilt also  $\varphi(-1) = -1$ .

## Beweis (2/2).

Sei  $\varphi: \mathbb{Q} \rightarrow \mathbb{Q}$  ein Isomorphismus von und auf  $(\mathbb{Q}, +, \cdot)$ .

- Für jedes  $n \in \mathbb{N}$  gilt

$$\varphi(n) = \varphi(\underbrace{1 + \cdots + 1}_{n \text{ mal}}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{n \text{ mal}} = \underbrace{1 + \cdots + 1}_{n \text{ mal}} = n$$

- Analog für  $z \in \mathbb{Z}$  mit  $z \leq 0$  unter Nutzung von  $-1$
- Seien  $m, n \in \mathbb{Z}$  mit  $n > 0$ . Z.zg.  $\varphi(\frac{m}{n}) = \frac{m}{n}$ . Es gilt

$$m = \varphi(m) = \varphi\left(\frac{m}{n} \cdot n\right) = \varphi\left(\frac{m}{n}\right) \cdot \varphi(n) = \varphi\left(\frac{m}{n}\right) \cdot n$$

Diese Gleichung lässt sich eindeutig lösen und wir erhalten  
 $\varphi\left(\frac{m}{n}\right) = \frac{m}{n}$ .

Also gilt  $\varphi = \text{id}_{\mathbb{Q}}$ .

□

## BOOLEsche Algebren

## §10.5 Definition

Sei  $(M, \preceq)$  ein Verband mit kleinstem Element  $\perp$  (von  $M$ ) und größtem Element  $\top$  (von  $M$ ).

- Sei  $m \in M$ . Ein Element  $m' \in M$  heißt **Komplement von  $m$**  gdw.  $m \wedge m' = \perp$  und  $m \vee m' = \top$ .
- Der Verband  $(M, \preceq)$  heißt **komplementiert** gdw. für jedes  $m \in M$  ein Komplement  $m' \in M$  von  $m$  existiert.
- Der Verband  $(M, \preceq)$  heißt **BOOLEsche Algebra** gdw. er komplementiert und distributiv ist und  $\perp \neq \top$  gilt.

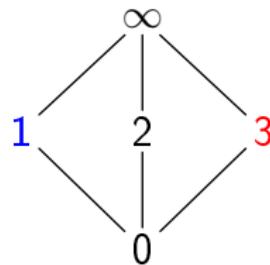
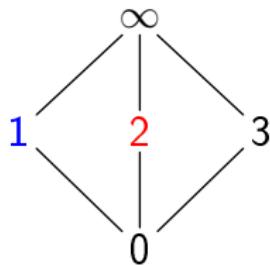
## GEORGE BOOLE (\* 1815; † 1864)

- engl. Philosoph und Mathematiker
- symbolische Aussagenlogik
- nur Grundschulausbildung



## Notizen

- Komplemente sind in allgemeinen Verbänden nicht eindeutig
- 2 ist Komplement von 1
- 3 ist auch Komplement von 1



## §10.6 Theorem

Sei  $(M, \preceq)$  ein distributiver Verband mit kleinstem Element  $\perp$  und größtem Element  $\top$ . Für jedes  $m \in M$  existiert höchstens ein Komplement von  $m$ .

### Beweis.

Sei  $m \in M$  und seien  $m', m'' \in M$  Komplemente von  $m$ .

- Wir zeigen  $m' = m' \wedge m''$

$$\begin{aligned}m' &= \top \wedge m' = (m \vee m'') \wedge m' = (m \wedge m') \vee (m'' \wedge m') \\&= \perp \vee (m'' \wedge m') = m' \wedge m''\end{aligned}$$

- Wir zeigen  $m'' = m' \wedge m''$

$$\begin{aligned}m'' &= \top \wedge m'' = (m \vee m') \wedge m'' = (m \wedge m'') \vee (m' \wedge m'') \\&= \perp \vee (m' \wedge m'') = m' \wedge m''\end{aligned}$$

Also  $m' = m' \wedge m'' = m''$





## Beispiel

$(\{0, 1\}, \{(0, 0), (0, 1), (1, 1)\})$  Verband der Wahrheitswerte mit

- kleinstem Element 0 und größtem Element 1
- Supremum  $\vee$  und Infimum  $\wedge$

Ist distributiv, da linear geordnet.

Für jedes  $b \in \{0, 1\}$  gilt  $b \wedge \underbrace{(1 - b)}_{\neg b} = 0$  und  $b \vee \underbrace{(1 - b)}_{\neg b} = 1$ .

Also komplementiert und damit BOOLEsche Algebra

## weiteres Beispiel

- für jede Menge  $M$  ist  $(\mathcal{P}(M), \subseteq)$  ein distributiver Verband
    - mit kleinstem Element  $\emptyset$  und größtem Element  $M$
    - Supremum  $\cup$  und Infimum  $\cap$
  - $M' \cap (M')^c = \emptyset$  und  $M' \cup (M')^c = M$  für jedes  $M' \in \mathcal{P}(M)$
- komplementiert und sogar BOOLEsche Algebra falls  $M \neq \emptyset$

## §10.7 Theorem

Sei  $(\Sigma, \mathcal{M})$  ein Maßraum mit  $\Sigma \neq \emptyset$ .

Dann ist  $(\mathcal{M}, \subseteq)$  eine BOOLEsche Algebra.

## Beweis.

$(\mathcal{M}, \subseteq)$  ist ein distributiver Verband (§9.10) mit kleinstem Element  $\emptyset$  und größtem Element  $\Sigma$ . Der Abschluss unter Komplementen liefert Komplementierung. □

## noch ein Beispiel

- sei  $M \neq \emptyset$  eine Menge und

$$\begin{aligned}\mathcal{M} = & \{M' \in \mathcal{P}(M) \mid M' \text{ endlich}\} \\ & \cup \{M' \in \mathcal{P}(M) \mid M \setminus M' \text{ endlich}\}\end{aligned}$$

- distributiver, aber nicht vollständiger, Verband
    - mit kleinstem Element  $\emptyset$  und größtem Element  $M$
    - Supremum  $\cup$  und Infimum  $\cap$
  - $M' \cap (M')^c = \emptyset$  und  $M' \cup (M')^c = M$  für jedes  $M' \in \mathcal{P}(M)$
- komplementiert und damit BOOLEsche Algebra

## §10.8 Theorem

Sei  $(M, \preceq)$  eine BOOLEsche Algebra mit kleinstem Element  $\perp$  und größtem Element  $\top$  und sei  $\cdot^c: M \rightarrow M$ , so dass  $m^c = m'$  für alle  $m \in M$ , wobei  $m'$  das Komplement von  $m$  ist. Dann gelten

- ①  $(m^c)^c = m$  für alle  $m \in M$  und
- ②  $(m_1 \wedge m_2)^c = m_1^c \vee m_2^c$  und  $(m_1 \vee m_2)^c = m_1^c \wedge m_2^c$   
für alle  $m_1, m_2 \in M$

## Beweis (1/2).

- ① Per Definition ist  $(m^c)^c$  das Komplement von  $m^c$ . Aufgrund der Kommutativität von  $\wedge$  und  $\vee$  (§9.7) ist  $m$  auch Komplement von  $m^c$ . Da das Komplement eindeutig ist (§10.6), gilt  $m = (m^c)^c$ .

## Beweis (2/2).

- ② Wir zeigen, dass  $(m_1 \vee m_2) \wedge (m_1^c \wedge m_2^c) = \perp$  und  $(m_1 \vee m_2) \vee (m_1^c \wedge m_2^c) = \top$ . Aufgrund der Eindeutigkeit des Komplements ist dann  $(m_1 \vee m_2)^c = m_1^c \wedge m_2^c$ .

$$\begin{aligned} & (m_1 \vee m_2) \wedge (m_1^c \wedge m_2^c) \\ &= (m_1 \wedge m_1^c \wedge m_2^c) \vee (m_2 \wedge m_1^c \wedge m_2^c) \\ &= (\perp \wedge m_2^c) \vee (\perp \wedge m_1^c) = \perp \vee \perp = \perp \end{aligned}$$

Analog rechnen wir die zweite Gleichheit

$$\begin{aligned} & (m_1 \vee m_2) \vee (m_1^c \wedge m_2^c) \\ &= (m_1 \vee m_2 \vee m_1^c) \wedge (m_1 \vee m_2 \vee m_2^c) \\ &= (\top \vee m_2) \vee (\top \vee m_1) = \top \vee \top = \top \end{aligned}$$

Ebenso für das zweite DEMORGAN-Gesetz.



## Notizen

- wir nutzen  $m^c$  für das Komplement von  $m$  in BOOLEschen Algebren

### §10.9 Theorem (vgl. §9.12)

Sei  $(M, \sqcap, \sqcup, \cdot^*, \perp, \top)$  eine algebraische Struktur des Typs  $(0, 2, 1, 2)$ , so dass für alle  $m_1, m_2 \in M$

- $\sqcap$  und  $\sqcup$  kommutativ, distributiv und assoziativ sind,
- $m_1 \sqcup (m_1 \sqcap m_2) = m_1$  und  $m_1 \sqcap (m_1 \sqcup m_2) = m_1$ , Absorption
- und  $m_1 \sqcap m_1^* = \perp$  und  $m_1 \sqcup m_1^* = \top$ . Komplemente

Dann ist  $(M, \preceq)$  mit  $m_1 \preceq m_2$  gdw.  $m_1 = m_1 \sqcap m_2$  eine BOOLEsche Algebra.

## Beweis.

Unter Nutzung von §9.12 leicht nachzurechnen. □

Eigenschaften

## §10.10 Definition

Sei  $(M, \preceq)$  eine BOOLEsche Algebra mit kleinstem Element  $\perp$ .

Ein Element  $m \in M$  ist ein **Atom** gdw.

- $m \neq \perp$  und
- für alle  $m' \in M$  mit  $m' \leq m$  gilt  $m' \in \{\perp, m\}$ .

## Notizen

- Atome sind die (direkten) Nachbarn des kleinsten Elements  $\perp$  im HASSE-Diagramm
- Atome sind genau die minimalen Elemente in  $M \setminus \{\perp\}$

## Beispiele

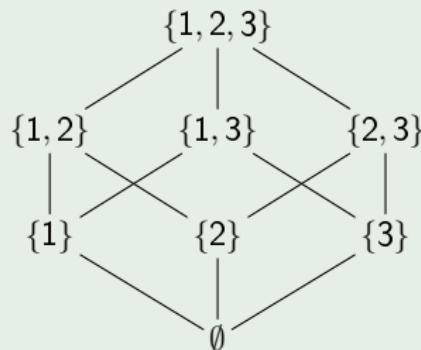
- BOOLEsche Algebra der Wahrheitswerte



Atome:  $\{1\}$

1 Atom

- Potenzmenge von  $M = \{1, 2, 3\}$



Atome:  $\{\{1\}, \{2\}, \{3\}\}$

3 Atome

## §10.11 Theorem

Sei  $(M, \preceq)$  eine BOOLEsche Algebra mit endlichem  $M$  und kleinstem Element  $\perp$ . Es gelten:

- ①  $a \wedge m \in \{\perp, a\}$  für jedes  $m \in M$  und jedes Atom  $a \in M$
- ②  $a \wedge b = \perp$  für alle Atome  $a, b \in M$  mit  $a \neq b$
- ③ für jedes  $m \in M \setminus \{\perp\}$  existiert ein Atom  $a \in M$  mit  $a \preceq m$

## Beweis (1/2).

- ① Offenkundig gilt  $a \wedge m \preceq a$ . Da  $a$  Atom ist, gilt  $a \wedge m \in \{\perp, a\}$ .
- ② Wenn  $a$  und  $b$  Atome sind, dann folgen aus  $a \wedge b \preceq a$  und  $a \wedge b \preceq b$  sowohl  $a \wedge b \in \{\perp, a\}$  als auch  $a \wedge b \in \{\perp, b\}$ . Da  $a \neq b$ , muss  $a \wedge b = \perp$  gelten.

## Beweis (2/2).

③ Sei  $m_0 \in M \setminus \{\perp\}$  beliebig.

- Falls  $m_0$  ein Atom ist, dann gilt  $m_0 \preceq m_0$ .
- Falls  $m_0$  kein Atom ist, dann existiert  $m_1 \in M$  mit  $m_1 \preceq m_0$  und  $m_1 \notin \{\perp, m_0\}$ . Wir schreiben  $m \succ m'$  gdw.  $m' \preceq m$  und  $m \neq m'$ . Also  $m_0 \succ m_1$ . Mit  $m_1$  können wir das Argument wiederholen und damit eine Kette

$$m_0 \succ m_1 \succ m_2 \succ m_3 \succ \dots$$

konstruieren. Dies Kette muss mit einem Atom  $m_i$  mit  $m_i \preceq m_0$  terminieren, da  $M$  endlich ist. □

## Notizen

- Infimum mit einem Atom  $a$  kann nur kleinstes Element  $\perp$  oder  $a$  liefern
- Infimum mit zwei verschiedenen Atomen ist immer das kleinste Element  $\perp$  (denn Atome sind unvergleichbar)
- Jedes Element (außer  $\perp$ ) liegt über einem Atom

## §10.12 Theorem

Sei  $(M, \preceq)$  eine BOOLEsche Algebra mit endlichem  $M$ , kleinstem Element  $\perp$  und größtem Element  $\top$ . Seien  $m \in M$  und  $A_m = \{m' \in M \mid m' \text{ Atom}, m' \preceq m\}$  die Menge der kleineren Atome. Dann gilt  $m = \sup A_m$ .

Beweis (1/2).

Wir beweisen die Aussage zunächst für  $m = \top$ . Da  $\top$  das größte Element ist, enthält  $A_\top$  alle Atome  $A_\top = \{a_1, \dots, a_k\}$ . Nehmen wir nun an, dass  $\top \neq \sup A_\top$ . Dann gilt auch  $\top^c = \perp \neq (\sup A_\top)^c = a_1^c \wedge \dots \wedge a_k^c$  aufgrund der Eindeutigkeit der Komplemente. Da  $a_1^c \wedge \dots \wedge a_k^c \neq \perp$  existiert gemäß §10.11 3 ein Atom  $a_i \in A_\top$ , so dass  $a_i \preceq a_1^c \wedge \dots \wedge a_k^c$ .

$$a_i = a_i \wedge a_1^c \wedge \dots \wedge a_k^c = a_i \wedge a_i^c \wedge \dots = \perp$$

da  $a_i \in A_\top$ . Also ist  $a_i = \perp$  kein Atom. Widerspruch.

## Beweis (2/2).

Also gilt  $\top = \sup A_\top$ . Sei nun  $m$  beliebig. Es gilt gemäß §10.11 ①

$$\begin{aligned} m &= \top \wedge m = (\sup A_\top) \wedge m = (a_1 \vee \cdots \vee a_k) \wedge m \\ &= (a_1 \wedge m) \vee \cdots \vee (a_k \wedge m) = \underbrace{(a_1 \wedge m)}_{\in \{a_1, \perp\}} \vee \cdots \vee \underbrace{(a_k \wedge m)}_{\in \{a_k, \perp\}} \end{aligned}$$

Für jedes  $1 \leq i \leq k$  gilt  $a_i \wedge m = a_i$  gdw.  $a_i \preceq m$ . Sei  $A_m = \{a_{j_1}, \dots, a_{j_n}\}$ . Also gilt

$$m = (a_{j_1} \wedge m) \vee \cdots \vee (a_{j_n} \wedge m) = a_{j_1} \vee \cdots \vee a_{j_n} = \sup A_m \quad \square$$

## Notizen

- jedes Element einer endlichen BOOLEschen Algebra lässt sich also als Supremum von Atomen darstellen
- wie wir gleich zeigen, ist diese Darstellung sogar eindeutig

## §10.13 Theorem

Sei  $(M, \preceq)$  eine BOOLEsche Algebra mit endlichem  $M$  und kleinstem Element  $\perp$ . Weiterhin sei  $A$  die Menge aller Atome von  $(M, \preceq)$ . Für alle  $A_1 \subseteq A$  und  $A_2 \subseteq A$  mit  $A_1 \neq A_2$  gilt  $\sup A_1 \neq \sup A_2$ .

### Beweis.

Indirekt. Seien  $A_1 \subseteq A$  und  $A_2 \subseteq A$  Teilmengen der Atome mit  $A_1 \neq A_2$ , so dass  $\sup A_1 = \sup A_2$ . O.B.d.A. existiert  $a \in A_1$ , so dass  $a \notin A_2$ . Also gilt unter Nutzung von §10.11②

$$\begin{aligned} a &= a \vee \perp = (a \wedge a) \vee \sup \{\perp\} \\ &= (a \wedge a) \vee \sup \{a \wedge a_1 \mid a_1 \in A_1 \setminus \{a\}\} \\ &= a \wedge \sup A_1 = a \wedge \sup A_2 \\ &= \sup \{a \wedge a_2 \mid a_2 \in A_2\} = \sup \{\perp\} = \perp \end{aligned}$$

Also gilt  $a = \perp$ , womit  $a$  kein Atom ist. Widerspruch. □

## Notizen

- jedes Element hat Darstellung als Supremum von Atomen
- verschiedene Mengen von Atomen liefern verschiedene Suprema

## §10.14 Theorem

Eine endliche BOOLEsche Algebra  $(M, \preceq)$  mit  $n$  Atomen besitzt genau  $2^n$  Elemente (d.h.  $|M| = 2^n$ )

## Beweis.

Sei  $A$  die Menge der Atome. Dann ist  $\text{sup}: \mathcal{P}(A) \rightarrow M$  injektiv gemäß §10.13. Also  $2^n = 2^{|A|} = |\mathcal{P}(A)| \leq |M|$ . Sei  $f: M \rightarrow \mathcal{P}(A)$ , so dass  $f(m) = A_m$  wie in §10.12. Diese Funktion ist auch injektiv und damit  $|M| \leq |\mathcal{P}(A)| = 2^n$ , womit  $|M| = 2^n$  folgt. □

Isomorphiesatz von STONE

## Motivation

- wir zeigen noch, dass alle endlichen BOOLESchen Algebren isomorph zu Potenzmengenalgebren sind
- Isomorphismusatz von STONE

MARSHALL HARVEY STONE (\* 1903; † 1989)

- amer. Mathematiker
- Funktionsanalysis und BOOLESche Algebren
- begeisterter Reisender und starb auf Reise



## §10.15 Theorem (Isomorphiesatz von STONE)

Sei  $\mathcal{M} = (M, \preceq)$  eine endliche BOOLESche Algebra mit Atomen  $A$ . Dann sind  $\mathcal{M}$  und  $(\mathcal{P}(A), \subseteq)$  isomorph.

### Beweis (1/2).

Für jedes  $m \in M$ , sei  $A_m = \{a \in A \mid a \preceq m\}$ . Wir definieren die Funktion  $\varphi: M \rightarrow \mathcal{P}(A)$  durch  $\varphi(m) = A_m$  für alle  $m \in M$ .

- **injektiv:** (*Kontraposition*) Seien  $m_1, m_2 \in M$ , so dass  $A_{m_1} = \varphi(m_1) = \varphi(m_2) = A_{m_2}$ . Gemäß §10.12 gilt dann  $m_1 = \sup A_{m_1} = \sup A_{m_2} = m_2$ .
- **surjektiv:** Sei  $A' \subseteq A$  eine Teilmenge der Atome. Da  $A$  endlich ist, existiert  $m = \sup A'$ . Also gilt  $\varphi(m) = A'$  aufgrund von §10.13.
- Also ist  $\varphi$  bijektiv.

## Beweis (2/2).

Es bleibt zu zeigen, dass die Struktur erhalten wird. Sei  $m_1, m_2 \in M$  beliebig. Z.zg.

$$m_1 \preceq m_2 \quad \text{gdw.} \quad \varphi(m_1) \subseteq \varphi(m_2)$$

- ( $\rightarrow$ ) Sei  $m_1 \preceq m_2$ . Es gilt  $\varphi(m_1) = A_{m_1}$  und  $a \preceq m_1$  für alle  $a \in A_{m_1}$ . Also auch  $a \preceq m_2$  und damit  $a \in A_{m_2} = \varphi(m_2)$ . Also  $\varphi(m_1) \subseteq \varphi(m_2)$ .
- ( $\leftarrow$ ) Sei  $\varphi(m_1) \subseteq \varphi(m_2)$ . Dann gilt  $A_{m_1} \subseteq A_{m_2}$  und damit gemäß §10.12

$$\begin{aligned} m_1 &= \sup A_{m_1} \preceq \sup A_{m_1} \vee \sup(A_{m_2} \setminus A_{m_1}) \\ &= \sup(A_{m_1} \cup (A_{m_2} \setminus A_{m_1})) = \sup A_{m_2} = m_2 \end{aligned}$$

Also sind  $\mathcal{M}$  und  $(\mathcal{P}(A), \subseteq)$  isomorph. □

## Notizen

- jede endliche BOOLESCHE Algebra ist isomorph zu einer Potenzmengenalgebra
  - die Gesetze der endlichen Potenzmengenalgebra  $(\mathcal{P}(M), \subseteq)$  gelten auch in allen BOOLESCHEN Algebren dieser Größe
- Rechnen in endlichen BOOLESCHEN Algebren  
= Rechnen mit endlichen Teilmengen

## Korollar

Jeder endliche Maßraum  $(\Sigma, \mathcal{E})$  ist als BOOLESCHE Algebra  $(\mathcal{E}, \subseteq)$  isomorph zu einer Potenzmengenalgebra.

## Frage

Gilt diese Isomorphie auch für unendliche BOOLEsche Algebren?

## Beobachtungen

- jede unendliche Potenzmengenalgebra ist überabzählbar (d.h. nicht abzählbar)
    - ist die Menge  $M$  endlich, dann ist  $\mathcal{P}(M)$  auch endlich
    - ist die Menge  $M$  abzählbar unendlich, dann ist  $|\mathcal{P}(M)| > |M|$  (§6.19) und damit überabzählbar
  - es gibt aber abzählbar unendliche BOOLEsche Algebren (und sogar solche ohne Atome)
- **nicht** jede BOOLEsche Algebra ist isomorph zu einer Potenzmengenalgebra

- Algebraische Strukturen
- Isomorphismen
- BOOLEsche Algebren
- Atome und Isomorphiesatz von STONE

Elfte Übungsserie ist bereits im OLAT.

# Diskrete Strukturen

## Vorlesung 11: Körper

Andreas Maletti

13. Januar 2015

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## heutige Vorlesung

- ① Definition Gruppe
- ② Grundlegende Eigenschaften von Gruppen
- ③ Definition Körper
- ④ Grundlegende Eigenschaften von Körpern
- ⑤ Ausblick Isomorphiesatz

Bitte Fragen direkt stellen!

Organisation

## Prüfung

am **20.02.2015** um 09:00 Uhr im HS 3 und im AudiMax

- 1 DIN-A4-Blatt mit Notizen als Hilfsmittel zugelassen  
(beliebig beschrieben oder bedruckt)
- Abmeldung noch bis 25. Januar möglich

## Tutorium

- DOREEN HEUSEL: 16. Januar (Fr.), 15 Uhr **im Hs. 5**
- THOMAS WEIDNER: 23. Januar (Fr.), 15 Uhr **im Hs. 5**
- CLAUDIO RÖHL: 29. Januar (Do.), 17 Uhr **im Hs. 17**
- ANDREAS MALETTI: 6. Februar (Fr.), 15 Uhr **im Hs. 5**

Wiederholung: Algebraische Strukturen

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ **Algebraische Strukturen**
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## Definition (§10.1)

Sei  $U$  eine Grundmenge und seien

- $R_1, \dots, R_k \subseteq U \times U$  Relationen auf  $U$
- $f_1, \dots, f_\ell: U \times U \rightarrow U$  binäre (zweistellige) Funktionen auf  $U$
- $g_1, \dots, g_m: U \rightarrow U$  unäre (einstellige) Funktionen auf  $U$  und
- $c_1, \dots, c_n \in U$  Elemente (auch: Konstanten) von  $U$ .

Dann ist  $(U, (R_1, \dots, R_k), (f_1, \dots, f_\ell), (g_1, \dots, g_m), (c_1, \dots, c_n))$  eine **algebraische Struktur** des Typs  $(k, \ell, m, n)$ .

## Notizen

- die Funktionen heißen auch **Operationen**
- heute hauptsächlich Strukturen mit Operationen

## Definition (§10.2)

Seien  $\mathcal{U} = (U, (R_1, \dots, R_k), (f_1, \dots, f_\ell), (g_1, \dots, g_m), (c_1, \dots, c_n))$  und  $\mathcal{U}' = (U', (R'_1, \dots, R'_k), (f'_1, \dots, f'_\ell), (g'_1, \dots, g'_m), (c'_1, \dots, c'_n))$  zwei algebraische Strukturen gleichen Typs. Eine Funktion  $\varphi: U \rightarrow U'$  heißt **Isomorphismus von  $\mathcal{U}$  nach  $\mathcal{U}'$** , gdw.

- $\varphi$  bijektiv ist,
- $(u_1, u_2) \in R_i$  gdw.  $(\varphi(u_1), \varphi(u_2)) \in R'_i$   
für alle  $1 \leq i \leq k$  und  $u_1, u_2 \in U$  gilt
- $\varphi(f_i(u_1, u_2)) = f'_i(\varphi(u_1), \varphi(u_2))$   
für alle  $1 \leq i \leq \ell$  und  $u_1, u_2 \in U$  gilt
- $\varphi(g_i(u)) = g'_i(\varphi(u))$  für alle  $1 \leq i \leq m$  und  $u \in U$ , und
- $\varphi(c_i) = c'_i$  für alle  $1 \leq i \leq n$ .

$\mathcal{U}$  und  $\mathcal{U}'$  heißen **isomorph**, gdw.  
ein Isomorphismus von  $\mathcal{U}$  nach  $\mathcal{U}'$  existiert.

## Notizen

- Isomorphismus ist Bijektion die alle Relationen und Operationen “erhält”
- gleiches “Rechnen” in isomorphen Strukturen
- isomorphe Strukturen unterscheiden sich nur in der Benennung der Elemente der Grundmenge

Gruppen

## Wiederholung (§10.9 und §9.12)

Eine algebraische Struktur  $(M, \sqcap, \sqcup, \cdot^*, \perp, \top)$  des Typs  $(0, 2, 1, 2)$ , so dass für alle  $m_1, m_2 \in M$

- $\sqcap$  und  $\sqcup$  kommutativ, distributiv und assoziativ sind,
- $m_1 \sqcup (m_1 \sqcap m_2) = m_1$  und  $m_1 \sqcap (m_1 \sqcup m_2) = m_1$ , Absorption
- und  $m_1 \sqcap m_1^* = \perp$  und  $m_1 \sqcup m_1^* = \top$ . Komplemente

liefert eine BOOLEsche Algebra.

## Motivation

- hat zwei binäre Funktionen  
(und eine unäre Funktion und 2 Konstanten)
- wir schauen uns zunächst nur die Eigenschaften  
der binären Funktion  $\sqcup$  an

## Beispiele

- ganze Zahlen  $(\mathbb{Z}, +, (-\cdot), 0)$  mit Addition
  - $n_1 + n_2 = n_2 + n_1$  für alle  $n_1, n_2 \in \mathbb{Z}$  (Kommutativität)
  - $n_1 + (n_2 + n_3) = (n_1 + n_2) + n_3$  für alle  $n_1, n_2, n_3 \in \mathbb{Z}$  (Assoziativität)
  - $n + (-n) = 0$  für alle  $n \in \mathbb{Z}$  (Komplement)
  - außerdem gilt:  $0 + n = n$  für alle  $n \in \mathbb{Z}$
- rationale Zahlen  $(\mathbb{Q} \setminus \{0\}, \cdot, \cdot^{-1}, 1)$  mit Multiplikation
  - $n_1 \cdot n_2 = n_2 \cdot n_1$  für alle  $n_1, n_2 \in \mathbb{Q} \setminus \{0\}$  (Kommutativität)
  - $n_1 \cdot (n_2 \cdot n_3) = (n_1 \cdot n_2) \cdot n_3$  für alle  $n_1, n_2, n_3 \in \mathbb{Q} \setminus \{0\}$  (Assoziativität)
  - $n \cdot n^{-1} = 1$  für alle  $n \in \mathbb{Q} \setminus \{0\}$  (Komplement)
  - außerdem gilt:  $1 \cdot n = n$  für alle  $n \in \mathbb{Q} \setminus \{0\}$

## §11.1 Definition

Eine algebraische Struktur  $(M, \oplus, \cdot^*, e)$  des Typs  $(0, 1, 1, 1)$  ist eine **(ABELSche) Gruppe**, gdw.

- $\oplus$  kommutativ und assoziativ ist,  
 $m_1 \oplus m_2 = m_2 \oplus m_1$  für alle  $m_1, m_2 \in M$  und  
 $m_1 \oplus (m_2 \oplus m_3) = (m_1 \oplus m_2) \oplus m_3$  für alle  $m_1, m_2, m_3 \in M$
  - $e \oplus m = m$  für alle  $m \in M$  und (neutrales Element)
  - $m \oplus m^* = e$  für alle  $m \in M$ . (Inverse)

## NIELS HENRIK ABEL (\* 1802; † 1829)

- norw. Mathematiker
  - Begründer der Gruppentheorie
  - verstarb mit 26 Jahren an Lungentuberkulose



## Notizen

- die Bedingung für das neutrale Element ist neu  
(und gilt nicht in BOOLEschen Algebren, denn  $\top \vee m = \top$ )
- Komplemente heißen auch **Inverse**
- manchmal auch “multiplikativ” geschrieben

$$(M, \odot, \cdot^{-1}, 1)$$

## §11.2 Theorem

Seien  $(M, \oplus, \cdot^*, e)$  und  $(M, \oplus, \cdot^\dagger, e)$  zwei Gruppen mit gleicher binärer Operation und gleichem neutralen Element. Dann gilt  $m^* = m^\dagger$  für alle  $m \in M$ .

(d.h., die Inversen sind eindeutig bestimmt)

### Beweis.

*Direkt.* Unter Anwendung der Gesetze gilt für alle  $m \in M$

$$\begin{aligned}m^* &= e \oplus m^* = \underbrace{(m \oplus m^\dagger)}_e \oplus m^* = (m^\dagger \oplus m) \oplus m^* \\&= m^\dagger \oplus \underbrace{(m \oplus m^*)}_e = m^\dagger \oplus e = m^\dagger\end{aligned}$$

□

### Notizen

- aufgrund der Eindeutigkeit wird die unäre Funktion  $\cdot^*$  oft nicht angegeben

## §11.3 Theorem

Seien  $(M, \oplus, e)$  und  $(M, \oplus, u)$  zwei Gruppen mit gleicher binärer Operation. Dann gilt  $e = u$ .

(d.h., das neutrale Element ist eindeutig bestimmt)

### Beweis.

*Direkt.* Unter Anwendung der Gesetze gilt

$$e = e \oplus u = u \oplus e = u$$



### Notizen

- aufgrund der Eindeutigkeit werden die unäre Funktion  $\cdot^*$  und das **neutrale Element**  $e$  oft nicht angegeben

## §11.4 Definition (Gruppe)

Eine algebraische Struktur  $(M, \oplus)$  des Typs  $(0, 1, 0, 0)$  ist eine **(ABELSche) Gruppe**, gdw.

- $\oplus$  kommutativ und assoziativ ist und
  - $m_1 \oplus m_2 = m_2 \oplus m_1$  für alle  $m_1, m_2 \in M$  und
  - $m_1 \oplus (m_2 \oplus m_3) = (m_1 \oplus m_2) \oplus m_3$  für alle  $m_1, m_2, m_3 \in M$
- ein Element  $e \in M$  existiert, so dass
  - $e \oplus m = m$  für alle  $m \in M$  und (neutrales Element)
  - für alle  $m \in M$  ein  $m' \in M$  existiert, so dass  $m \oplus m' = e$ . (Inverse)

## Beispiele

- $(\mathbb{N}, +)$  ist **keine** Gruppe
  - das neutrale Element ist 0  $0 + n = n$
  - aber es gibt kein  $n \in \mathbb{N}$ , so dass  $1 + n = 0$
- $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{Q} \setminus \{0\}, \cdot)$  und  $(\mathbb{R} \setminus \{0\}, \cdot)$  sind Gruppen
- $(\mathbb{Q}, \cdot)$  ist **keine** Gruppe
  - das neutrale Element ist 1  $1 \cdot n = n$
  - aber es gibt kein  $n \in \mathbb{Q}$ , so dass  $0 \cdot n = 1$

## Beispiel (1/3)

Sei  $m \in \mathbb{N}$  mit  $m \geq 1$ .

- Wir definieren  $\sim_m \subseteq \mathbb{Z} \times \mathbb{Z}$  durch

$$\sim_m = \{(n_1, n_2) \in \mathbb{Z} \times \mathbb{Z} \mid m|(n_1 - n_2)\}$$

- $\sim_m$  ist Äquivalenzrelation (reflexiv, symmetrisch, transitiv)
  - reflexiv:**  $n \sim_m n$  für alle  $n \in \mathbb{Z}$ , denn  $m|0$
  - symmetrisch:** Sei  $n_1 \sim_m n_2$ . Dann  $m|(n_1 - n_2)$  also existiert  $k \in \mathbb{Z}$ , so dass  $m \cdot k = n_1 - n_2$ . Dann ist  $m \cdot (-k) = -(m \cdot k) = -(n_1 - n_2) = n_2 - n_1$ . Also  $n_2 \sim_m n_1$
  - transitiv:** Seien  $n_1 \sim_m n_2$  und  $n_2 \sim_m n_3$ . Dann gelten  $m|(n_1 - n_2)$  und  $m|(n_2 - n_3)$  und es existieren  $k_1, k_2 \in \mathbb{Z}$ , so dass  $m \cdot k_1 = n_1 - n_2$  und  $m \cdot k_2 = n_2 - n_3$ . Also

$$\begin{aligned}m \cdot (k_1 + k_2) &= (m \cdot k_1) + (m \cdot k_2) = (n_1 - n_2) + (n_2 - n_3) \\&= n_1 - n_3\end{aligned}$$

und damit  $n_1 \sim_m n_3$

## Beispiel (2/3)

Sei  $m \in \mathbb{N}$  mit  $m \geq 1$ .

- Sei  $\mathbb{Z}_m = (\mathbb{Z}/\sim_m) = \{[n]_{\sim_m} \mid n \in \mathbb{Z}\}$  (Restklassen)
- Wir definieren  $+_m: \mathbb{Z}_m \times \mathbb{Z}_m \rightarrow \mathbb{Z}_m$  durch  $[n_1] +_m [n_2] = [n_1 + n_2]$  für alle  $n_1, n_2 \in \mathbb{Z}$
- Repräsentantenunabhängigkeit: Seien  $n_1 \sim_m n'_1$  und  $n_2 \sim_m n'_2$ . Z.zg.  $n_1 + n_2 \sim_m n'_1 + n'_2$ . Es gelten  $m|(n_1 - n'_1)$  und  $m|(n_2 - n'_2)$  also existieren  $k_1, k_2 \in \mathbb{Z}$ , so dass  $m \cdot k_1 = n_1 - n'_1$  und  $m \cdot k_2 = n_2 - n'_2$ . Also

$$\begin{aligned} m \cdot (k_1 + k_2) &= (m \cdot k_1) + (m \cdot k_2) = (n_1 - n'_1) + (n_2 - n'_2) \\ &= (n_1 + n_2) - (n'_1 + n'_2) \end{aligned}$$

und damit  $n_1 + n_2 \sim_m n'_1 + n'_2$

## Beispiel (3/3)

Sei  $m \in \mathbb{N}$  mit  $m \geq 1$ .

- $(\mathbb{Z}_m, +_m)$  ist eine Gruppe

- kommutativ:

$$[n_1] +_m [n_2] = [n_1 + n_2] = [n_2 + n_1] = [n_2] +_m [n_1] \text{ für alle } n_1, n_2 \in \mathbb{Z}$$

- assoziativ: für alle  $n_1, n_2, n_3 \in \mathbb{Z}$

$$\begin{aligned}[n_1] +_m ([n_2] +_m [n_3]) &= [n_1] +_m [n_2 + n_3] = [n_1 + n_2 + n_3] \\ &= [n_1 + n_2] +_m [n_3] \\ &= ([n_1] +_m [n_2]) +_m [n_3]\end{aligned}$$

- neutrales Element ist  $[0]$ , denn  $[0] +_m [n] = [0 + n] = [n]$  für alle  $n \in \mathbb{Z}$
- Inverse: für alle  $n \in \mathbb{Z}$  gilt  $[n] +_m [-n] = [n - n] = [0]$

## Eigenschaften von Gruppen

## §11.5 Theorem

Sei  $(M, \oplus, \cdot^*, e)$  eine Gruppe und  $m_1, m_2 \in M$ . Dann existiert genau ein  $m \in M$ , so dass  $m_1 \oplus m = m_2$ .

Beweis.

Sei  $m \in M$ , so dass  $m_1 \oplus m = m_2$ . Wir bestimmen  $m$  durch

$$\begin{aligned}m &= e \oplus m = \underbrace{(m_1 \oplus m_1^*) \oplus m}_e = (m_1^* \oplus m_1) \oplus m \\&= m_1^* \oplus \underbrace{(m_1 \oplus m)}_{m_2} = m_1^* \oplus m_2\end{aligned}$$

□

## §11.6 Konsequenzen

- Gleichungen  $m \oplus x = n$  lassen sich in der Gruppe  $(M, \oplus)$  lösen
- wir dürfen kürzen:  $m \oplus x = m \oplus y$  impliziert  $x = y$

## §11.7 Definition

Sei  $(M, \odot, \cdot^{-1}, e)$  eine Gruppe und  $U \subseteq M$ . Dann liefert  $U$  eine Untergruppe, gdw.

- $e \in U$ ,
- $u_1 \odot u_2 \in U$  für alle  $u_1, u_2 \in U$  und
- $u^{-1} \in U$  für alle  $u \in U$ .

Die Untergruppe von  $U$  ist  $(U, \otimes)$  mit  $\otimes: U \times U \rightarrow U$ , so dass  $u_1 \otimes u_2 = u_1 \odot u_2$  für alle  $u_1, u_2 \in U$ .

## Beispiele

- $M$  liefert stets eine Untergruppe der Gruppe  $(M, \odot)$
- $\mathbb{N}$  liefert keine Untergruppe von  $(\mathbb{Z}, +)$   
(denn  $-2 \notin \mathbb{N}$  obwohl  $2 \in \mathbb{N}$ )

## Notizen

- Menge  $U$  liefert Untergruppe gdw.  
man Menge  $U$  nicht mit den Operationen verlassen kann

## §11.8 Theorem

Sei  $(M, \odot, \cdot^{-1}, e)$  eine Gruppe. Dann liefert  $\{e\}$  eine Untergruppe.

## Beweis.

- neutrales Element (Konstante):  $e \in \{e\}$
- binäre Operation:  $e \odot e = e \in \{e\}$
- Inverse (unäre Operation): Es gilt  $e \odot e^* = e \odot e$ . Nach Kürzen bleibt  $e^* = e \in \{e\}$ .

□

## Beispiele

- $\mathbb{Z}$  liefert eine Untergruppe von  $(\mathbb{Q}, +)$
- $\mathbb{Q}$  liefert eine Untergruppe von  $(\mathbb{R}, +)$
- $\mathbb{Q} \setminus \{0\}$  liefert eine Untergruppe von  $(\mathbb{R} \setminus \{0\}, \cdot)$

## §11.9 Beobachtung

In der linear geordneten Menge  $(\mathbb{N}, \leq)$  existiert für jede nichtleere Teilmenge  $N \subseteq \mathbb{N}$  das kleinste Element von  $N$ .

Beweis.

- ①  $i \leftarrow 0$  (setze  $i$  auf 0)
- ② falls  $i \in N$ , liefere  $i$  (Element gefunden)
- ③ sonst  $i \leftarrow i + 1$  und zu ② (probiere nächste Zahl)

Terminiert mit  $i \in N$  und für alle  $n \in \mathbb{N}$  mit  $n < i$  gilt  $n \notin N$ . Also  $i \leq n$  für alle  $n \in N$ , womit  $i$  das kleinste Element von  $N$  ist. □

## §11.10 Theorem

Sei  $k \in \mathbb{Z}$ . Dann liefert  $k\mathbb{Z} = \{k \cdot n \mid n \in \mathbb{Z}\}$  eine Untergruppe von  $(\mathbb{Z}, +)$ .

### Beweis.

- $0 \in k\mathbb{Z}$ , da  $k \cdot 0 = 0$
- $(k \cdot n_1) + (k \cdot n_2) = k \cdot (n_1 + n_2) \in k\mathbb{Z}$  für alle  $n_1, n_2 \in \mathbb{Z}$
- $-(k \cdot n) = k \cdot (-n) \in k\mathbb{Z}$  für alle  $n \in \mathbb{Z}$

Also liefert  $k\mathbb{Z}$  eine Untergruppe von  $(\mathbb{Z}, +)$ . □

## §11.11 Theorem

Sei  $U \subseteq \mathbb{Z}$ , so dass  $U$  eine Untergruppe von  $(\mathbb{Z}, +)$  liefert. Dann existiert  $k \in \mathbb{Z}$ , so dass  $U = k\mathbb{Z}$ .

Beweis (1/2).

Per Fallunterscheidung:

- Sei  $U = \{0\}$ . Dann ist  $U = 0\mathbb{Z}$ .
- Sei  $U \neq \{0\}$ . Da  $0 \in U$ , folgt  $U' = U \setminus \{0\} \neq \emptyset$ . Weiterhin gilt auch  $U' \cap \mathbb{N} \neq \emptyset$ , denn für jedes  $u \in U'$  mit  $u < 0$  gilt auch  $-u \in U'$ . Also existiert gemäß §11.8 ein kleinstes Element  $k$  von  $U' \cap \mathbb{N}$ . Z.zg.  $U = k\mathbb{Z}$ .  
 $(\supseteq)$  Sei  $k \cdot n \in k\mathbb{Z}$ . Falls  $n = 0$ , dann ist  $k \cdot n = 0 \in U$ . Zunächst

$$|k \cdot n| = k \cdot |n| = \underbrace{k + \cdots + k}_{|n| \text{ mal}} \in U$$

denn  $k \in U$  und  $U$  liefert Untergruppe. Damit sind  $k \cdot n$  und  $-(k \cdot n)$  Elemente von  $U$ .

## Beweis (2/2).

Per Fallunterscheidung:

- Sei  $U \neq \{0\}$ . Z.zg.  $U = k\mathbb{Z}$ .

( $\subseteq$ ) Sei  $u \in U$ . Falls  $u = 0$ , dann gilt  $u \in k\mathbb{Z}$ . Sei nun  $u \neq 0$ . Wir teilen nun  $u$  durch  $k$  mit Rest. Sei also

$$u = k \cdot n + r \quad \text{mit} \quad n \in \mathbb{Z}, 0 \leq r < k$$

Offensichtlich ist  $k \cdot n \in k\mathbb{Z} \subseteq U$ . Zusammen mit  $u \in U$  haben wir  $r = u - (k \cdot n) \in U$ . Da aber  $r \in U \cap \mathbb{N}$  mit  $r < k$  und  $k$  das kleinste Element von  $U' \cap \mathbb{N}$  ist, muss  $r = 0$  gelten. Also ist  $u = k \cdot n$  und ist damit in  $k\mathbb{Z}$ . □

Körper

## Wiederholung (§10.9 und §9.12)

Eine algebraische Struktur  $(M, \sqcap, \sqcup, \cdot^*, \perp, \top)$  des Typs  $(0, 2, 1, 2)$ , so dass für alle  $m_1, m_2 \in M$

- $\sqcap$  und  $\sqcup$  kommutativ, distributiv und assoziativ sind,
- $m_1 \sqcup (m_1 \sqcap m_2) = m_1$  und  $m_1 \sqcap (m_1 \sqcup m_2) = m_1$ , Absorption
- und  $m_1 \sqcap m_1^* = \perp$  und  $m_1 \sqcup m_1^* = \top$ . Komplemente

liefert eine BOOLEsche Algebra.

## Motivation

- hat zwei binäre Funktionen  
(und eine unäre Funktion und 2 Konstanten)
- nun kombinieren wir zwei Operationen (Gruppen)  
auf diese Weise

## §11.12 Definition (Körper)

Eine algebraische Struktur  $(M, \oplus, \odot)$  des Typs  $(0, 2, 0, 0)$  ist ein **Körper**, gdw.

- $(M, \oplus)$  eine Gruppe mit neutralem Element  $e$  ist,
- $(M \setminus \{e\}, \odot)$  eine Gruppe ist, und
- $m \odot (m_1 \oplus m_2) = (m \odot m_1) \oplus (m \odot m_2)$   
für alle  $m, m_1, m_2 \in M$ . (Distributivität)

## Notizen

- Körper  
= 2 distributiv verbundene Gruppen auf der gleichen Menge
- $(M, \oplus)$  = **additive Gruppe**
- $(M \setminus \{e\}, \odot)$  = **multiplikative Gruppe**
- **nur**  $\odot$  distributiv über  $\oplus$  (wie in der Arithmetik)

## Beispiele

- $(\mathbb{Q}, +, \cdot)$  ist ein Körper
- $(\mathbb{R}, +, \cdot)$  ist ein Körper
- $(\mathbb{Z}, +, \cdot)$  ist **kein** Körper  
denn  $(\mathbb{Z} \setminus \{0\}, \cdot)$  ist keine Gruppe

## §11.13 Theorem

Sei  $(M, \oplus, \odot)$  ein Körper und sei  $e$  das neutrale Element von  $(M, \oplus)$ . Dann gilt  $e \odot m = e$  für alle  $m \in M$ .

## Beweis.

$$\begin{aligned}(e \odot m) \oplus e &= e \odot m = m \odot e = m \odot (e \oplus e) \\&= (m \odot e) \oplus (m \odot e) = (e \odot m) \oplus (e \odot m)\end{aligned}$$

Da  $(M, \oplus)$  eine Gruppe ist, können wir “kürzen” (§11.6) und erhalten  $e = e \odot m$ .



## Beispiel

Sei  $m \in \mathbb{N}$  mit  $m \geq 1$ .

- Wir definieren  $\cdot_m: \mathbb{Z}_m \times \mathbb{Z}_m \rightarrow \mathbb{Z}_m$  durch  
 $[n_1] \cdot_m [n_2] = [n_1 \cdot n_2]$  für alle  $n_1, n_2 \in \mathbb{Z}$
- Repräsentantenunabhängigkeit:** Seien  $n_1 \sim_m n'_1$  und  $n_2 \sim_m n'_2$ . Z.zg.  $n_1 \cdot n_2 \sim_m n'_1 \cdot n'_2$ . Es gelten  $m|(n_1 - n'_1)$  und  $m|(n_2 - n'_2)$  also existieren  $k_1, k_2 \in \mathbb{Z}$ , so dass  
 $m \cdot k_1 = n_1 - n'_1$  und  $m \cdot k_2 = n_2 - n'_2$ . Also

$$\begin{aligned}& (n_1 \cdot n_2) - (n'_1 \cdot n'_2) \\&= (n_1 \cdot n_2) - \underbrace{(n_1 \cdot n'_2) + (n_1 \cdot n'_2)}_{=0} - (n'_1 \cdot n'_2) \\&= n_1 \cdot (n_2 - n'_2) + (n_1 - n'_1) \cdot n'_2 \\&= n_1 \cdot m \cdot k_2 + m \cdot k_1 \cdot n'_2 = m \cdot ((n_1 \cdot k_2) + (k_1 \cdot n'_2))\end{aligned}$$

und damit  $n_1 \cdot n_2 \sim_m n'_1 \cdot n'_2$

## §11.14 Theorem

Sei  $m \in \mathbb{N}$  eine Primzahl. Dann ist  $(\mathbb{Z}_m, +_m, \cdot_m)$  ein Körper.

Beweis (1/2).

- Wir wissen bereits, dass  $(\mathbb{Z}_m, +_m)$  eine Gruppe ist.
- Offensichtlich gilt für alle  $n, n_1, n_2 \in \mathbb{Z}$

$$\begin{aligned}[n] \cdot_m ([n_1] +_m [n_2]) &= [n] \cdot_m [n_1 + n_2] = [n \cdot (n_1 + n_2)] \\ &= [(n \cdot n_1) + (n \cdot n_2)] = [n \cdot n_1] +_m [n \cdot n_2] \\ &= ([n] \cdot_m [n_1]) +_m ([n] \cdot_m [n_2])\end{aligned}$$

- Z.zg.  $(\mathbb{Z}_m \setminus \{[0]\}, \cdot_m)$  ist eine Gruppe
  - **kommutativ:**  $[n_1] \cdot_m [n_2] = [n_1 \cdot n_2] = [n_2 \cdot n_1] = [n_2] \cdot_m [n_1]$  für alle  $n_1, n_2 \in \mathbb{Z}$
  - **assoziativ:** für alle  $n_1, n_2, n_3 \in \mathbb{Z}$

$$\begin{aligned}[n_1] \cdot_m ([n_2] \cdot_m [n_3]) &= [n_1] \cdot_m [n_2 \cdot n_3] = [n_1 \cdot n_2 \cdot n_3] \\ &= [n_1 \cdot n_2] \cdot_m [n_3] = ([n_1] \cdot_m [n_2]) \cdot_m [n_3]\end{aligned}$$

## Beweis (2/2).

- Z.zg.  $(\mathbb{Z}_m \setminus \{[0]\}, \cdot_m)$  ist eine Gruppe
  - **neutrales Element** ist  $[1]$ , denn  $[1] \cdot_m [n] = [1 \cdot n] = [n]$  für alle  $n \in \mathbb{Z}$
  - **Inverse:** Sei  $n < m$  mit  $n \neq 0$ . Wir werden noch beweisen (EUKLIDISCHER Algorithmus), dass  $x, y \in \mathbb{Z}$  existieren, so dass  $\text{ggT}(n, m) = nx + my$ . Da  $m$  prim ist und  $n < m$ , gilt  $\text{ggT}(n, m) = 1 = nx + my$ . Des Weiteren gilt für jedes  $k \in \mathbb{Z}$

$$nx + my = nx + \underbrace{nkm - nkm}_{0} + my = n(x + km) + m(y - kn)$$

Wähle  $k$ , so dass  $x' = x + km \in \{0, \dots, m-1\}$ . Dann gilt

$$1 = nx + my = nx' + m(y - kn)$$

womit  $1 - nx' = m(y - kn)$  und damit  $1 \sim_m nx'$  also  $[1] = [nx']$ . Es folgt  $[n] \cdot_m [x'] = [nx'] = [1]$ . □

## Eigenschaften von Körpern

## §11.14 Theorem

Sei  $(M, \oplus, \odot)$  ein Körper und  $e$  das neutrale Element von  $(M, \oplus)$ .  
Für beliebige  $m_1, m_2 \in M$  mit  $m_1 \odot m_2 = e$  gilt  $e \in \{m_1, m_2\}$ .

### Beweis.

O.B.d.A. sei  $m_1 \neq e$ . Sei  $m_1^{-1}$  das multiplikativ Inverse zu  $m_1$  und  $u$  das neutrale Element der multiplikativen Gruppe (d.h.  $m_1 \odot m_1^{-1} = u$ ). Dann gilt

$$\begin{aligned}m_2 &= u \odot m_2 = \underbrace{(m_1 \odot m_1^{-1}) \odot m_2}_u = (m_1^{-1} \odot m_1) \odot m_2 \\&= m_1^{-1} \odot \underbrace{(m_1 \odot m_2)}_e = m_1^{-1} \odot e = e\end{aligned}$$

□

## §11.15 Definition (Polynom)

Sei  $(M, \oplus, \odot)$  ein Körper mit neutralem Element  $e$  von  $(M, \oplus)$ , und sei  $n \in \mathbb{N}$ . Jede Wahl  $a_0, \dots, a_n \in M$  mit  $a_n \neq e$  definiert ein **Polynom**  $p = (a_0, \dots, a_n)$  vom **Grad**  $n$ . Dieses Polynom  $p$  definiert eine Funktion  $f_p: M \rightarrow M$  für alle  $x \in M$  durch

$$f_p(x) = a_0 \oplus (a_1 \odot x) \oplus (a_2 \odot x \odot x) \oplus \cdots \oplus (a_n \odot \underbrace{x \odot \cdots \odot x}_{n \text{ mal}})$$

Wir schreiben auch  $\text{grad}(p) = n$ .

Das **Nullpolynom**  $p$  mit  $p = ()$  hat Grad  $-\infty$ .

## Beispiel

Im Körper  $(\mathbb{Z}_5, +_5, \cdot_5)$  ist  $p = ([2], [4], [1])$  ein Polynom vom Grad 2. Es gilt

$$f_p([2]) = [2] +_5 ([4] \cdot_5 [2]) +_5 ([2] \cdot_5 [2]) = [2] +_5 [3] +_5 [4] = [4]$$

## §11.16 Definition (Nullstelle)

Seien  $(M, \oplus, \odot)$  ein Körper und  $e$  das neutrale Element von  $(M, \oplus)$ . Weiterhin sei  $p$  ein Polynom. Ein Element  $m \in M$  ist **Nullstelle** von  $p$  gdw.  $f_p(m) = e$ .

### Beispiel

Hat das Polynom  $p = ([2], [4], [1])$  Nullstellen in  $(\mathbb{Z}, +_5, \cdot_5)$ ?

- $f_p([0]) = [2]$
- $f_p([1]) = [2] +_5 [4] +_5 [1] = [2]$
- $f_p([2]) = [4]$
- $f_p([3]) = [2] +_5 [2] +_5 [4] = [3]$
- $f_p([4]) = [2] +_5 [1] +_5 [1] = [4]$

## §11.17 Theorem (HORNER-Schema)

Seien  $(M, \oplus, \odot)$  ein Körper und  $n \in \mathbb{N}$ . Weiterhin sei  $p = (a_0, \dots, a_n)$  ein Polynom vom Grad  $n \geq 0$ . Dann gilt für alle  $x \in M$

$$f_p(x) = a_0 \oplus \left( x \odot \left( a_1 \oplus \left( x \odot \left( a_2 \oplus \left( x \odot \cdots \left( x \odot a_n \right) \cdots \right) \right) \right) \right) \right)$$

Beweis.

Einfaches Ausklammern



WILLIAM GEORGE HORNER (\* 1786; † 1837)

- engl. Mathematiker
- Lösung algebraischer Gleichungen
- eigentlich bereits 500 Jahre vorher von ZHU SHIJIE entdeckt



## §11.18 Theorem

Sei  $(M, \oplus, \odot)$  ein Körper. Weiterhin seien  $p_1, p_2$  Polynome mit  $\text{grad}(p_2) \geq 0$ . Dann existieren Polynome  $t$  und  $r$ , so dass für alle  $x \in M$

$$f_{p_1}(x) = f_t(x) \odot f_{p_2}(x) \oplus f_r(x)$$

und  $\text{grad}(r) < \text{grad}(p_2)$ .

Beweis.

normale Polynomdivision; Training in der Übung



Isomorphiesatz von Körpern

## §11.19 Definition

Ein Körper  $(M, \oplus, \odot)$  ist **endlich** (oder ein **GALOIS-Körper**) gdw.  $M$  endlich ist

### ÉVARISTE GALOIS (\* 1811; † 1832)

- franz. Mathematiker
- löste als Jugendlicher ein 350 Jahre altes Problem
- verstarb leider bereits mit 20 in einem Duell



## §11.20 Theorem (MOORE 1893)

- Sei  $(M, \oplus, \odot)$  ein GALOIS-Körper (endlicher Körper).  
Dann existieren  $n, p \in \mathbb{N}$  mit  $p$  prim, so dass  $|M| = p^n$ .
- Seien  $\mathcal{K}_1$  und  $\mathcal{K}_2$  GALOIS-Körper mit gleich vielen Elementen.  
Dann sind  $\mathcal{K}_1$  und  $\mathcal{K}_2$  isomorph.

ELIAKIM HASTINGS MOORE (\* 1862; † 1932)

- amer. Mathematiker
- Vorreiter der abstrakten Algebra
- studierte Mathematik in Berlin



## Notizen

Sei  $\mathcal{M} = (M, \oplus, \odot)$  ein GALOIS-Körper.

- für  $p = |M|$  prim, ist  $\mathcal{M}$  isomorph zu  $(\mathbb{Z}_p, +_p, \cdot_p)$
- die weiteren GALOIS-Körper ergeben sich mit Hilfe von Polynomen
- $|M| \neq 6$  (kein Körper hat 6 Elemente)
- wichtig in der Kodierungstheorie und Kryptographie

## Frage

Zeigen Sie, dass  $(\{a, b, c, d, e\}, \oplus, \odot)$  mit folgenden Operationen ein Körper ist.

$\oplus$	a	b	c	d	e
a	c	d	e	a	b
b	d	e	a	b	c
c	e	a	b	c	d
d	a	b	c	d	e
e	b	c	d	e	a

$\odot$	a	b	c	d	e
a	b	a	e	d	c
b	a	b	c	d	e
c	e	c	a	d	b
d	d	d	d	d	d
e	c	e	b	d	a

## Lösung

- 5 ist prim, also existiert ein Körper mit 5 Elementen
- jeder solche Körper ist isomorph zu  $\mathcal{Z}_5 = (\mathbb{Z}_5, +_5, \cdot_5)$
- wir versuchen  $\mathcal{Z}_5$  zu "identifizieren"
- dies sind Tafeln von  $\mathcal{Z}_5 \rightarrow$  isomorph zu  $\mathcal{Z}_5$  und damit Körper

## Frage

Zeigen Sie, dass  $(\{a, b, c, d, e\}, \oplus, \odot)$  mit folgenden Operationen ein Körper ist.

$\oplus$	4	1	3	0	2
4	3	0	2	4	1
1	0	2	4	1	3
3	2	4	1	3	0
0	4	1	3	0	2
2	1	3	0	2	4

$\odot$	4	1	3	0	2
4	1	4	2	0	3
1	4	1	3	0	2
3	2	3	4	0	1
0	0	0	0	0	0
2	3	2	1	0	4

## Lösung

- 5 ist prim, also existiert ein Körper mit 5 Elementen
- jeder solche Körper ist isomorph zu  $\mathbb{Z}_5 = (\mathbb{Z}_5, +_5, \cdot_5)$
- wir versuchen  $\mathbb{Z}_5$  zu "identifizieren"
- dies sind Tafeln von  $\mathbb{Z}_5 \rightarrow$  isomorph zu  $\mathbb{Z}_5$  und damit Körper

- Definition und Eigenschaften von Gruppen
- Definition und Eigenschaften von Körpern
- Ausblick Isomorphiesatz

Zwölfte Übungsserie ist bereits im OLAT.

# Diskrete Strukturen

## Vorlesung 12: Graphen

Andreas Maletti

20. Januar 2015

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## heutige Vorlesung

- ① Definition Graph und einfache Eigenschaften
- ② Untergraphen und Bäume
- ③ Planarität

Bitte Fragen direkt stellen!

Organisation

## Prüfung

am **20.02.2015** um 09:00 Uhr im HS 3 und im AudiMax

- 1 DIN-A4-Blatt mit Notizen als Hilfsmittel zugelassen  
(beliebig beschrieben oder bedruckt)
- Abmeldung noch bis **25. Januar** möglich

## Tutorium

- THOMAS WEIDNER: 23. Januar (Fr.), 15 Uhr **im Hs. 5**
- CLAUDIO RÖHL: 29. Januar (Do.), 17 Uhr **im Hs. 17**
- ANDREAS MALETTI: 6. Februar (Fr.), 15 Uhr **im Hs. 5**

Wiederholung: Relationen

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## Definition (§3.13 und §3.14)

Jede Teilmenge  $R \subseteq M \times M$  ist eine **Relation auf  $M$** . Sie ist

- **symmetrisch** gdw.

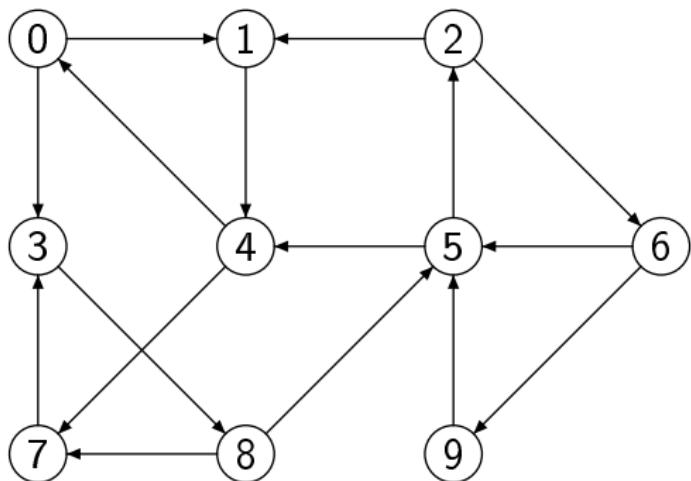
$$(\forall m \in M).(\forall m' \in M).\left((m, m') \in R \rightarrow (m', m) \in R\right)$$

- **irreflexiv** gdw.

$$(\forall m \in M).\left((m, m) \notin R\right)$$

## Notizen

- **algebraische Struktur** = Grundmenge mit darauf definierten Relationen, Funktionen und Konstanten
- Typ der algebraischen Struktur =  $(r, b, u, k)$ 
  - $r$  = Anzahl der Relationen
  - $b$  = Anzahl der binären Funktionen (Operationen)
  - $u$  = Anzahl der unären Funktionen
  - $k$  = Anzahl der Konstanten



Darstellung der Relation

$$\{(0, 1), (0, 3), (1, 4), (2, 1), (2, 6), (3, 8), (4, 0), (4, 7), (5, 2), (5, 4), (6, 5), (6, 9), (7, 3), (8, 5), (8, 7), (9, 5)\}$$

Graphen

## §12.1 Definition

(Gerichtete) Graphen sind genau die algebraischen Strukturen des Typs  $(1, 0, 0, 0)$ . Jeder Graph ist also eine Struktur  $(E, K)$

- für eine Menge  $E$  der **Ecken** und
- eine Relation  $K \subseteq E \times E$  der **Kanten**.

Ein  $(e, e') \in K$  heißt **Kante von  $e$  zu  $e'$** , wobei

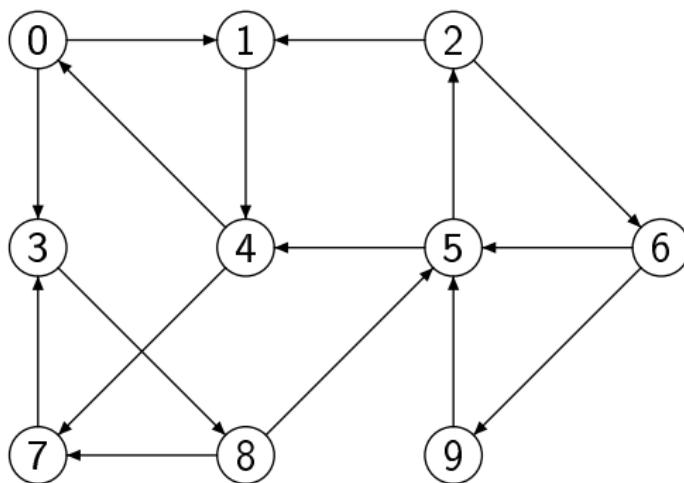
- $e$  die **Startecke** von  $(e, e')$  und
- $e'$  die **Zielecke** von  $(e, e')$  ist

## Notizen

- jeder Verband ist ein Graph
- jede Äquivalenzrelation  $\equiv \subseteq M \times M$  liefert Graph  $(M, \equiv)$
- jede teilweise Ordnung  $\preceq \subseteq M \times M$  liefert Graph  $(M, \preceq)$

## Intuition

- ein Graph besteht aus einer Menge von (benannten) Punkten die beliebig miteinander verbunden sind
- **Ecke** = benannter Punkt
- **Kante** = gerichtete Verbindung zwischen zwei Punkten



## §12.2 Definition

Ein Graph  $\mathcal{G} = (E, K)$  ist

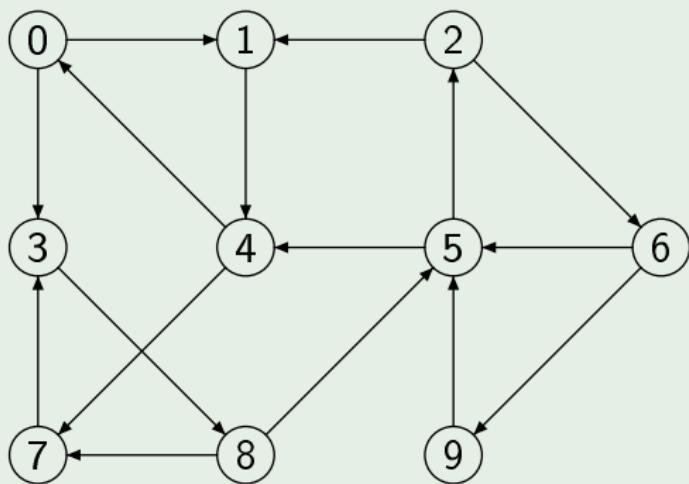
- **endlich** gdw.  $E$  endlich ist (endlich viele Ecken)
- **vollständig** gdw.  $K = E \times E$  ist (hat alle Kanten)
- **ungerichtet** gdw.  $K$  symmetrisch ist
- **schlingenfrei** gdw.  $K$  irreflexiv ist
- **schlingenfrei vollständig** gdw.  $K = (E \times E) \setminus \text{id}_E$  (hat alle Kanten außer Schlingen)

Jede Kante  $(e, e) \in K$  heißt **Schlinge von  $\mathcal{G}$** .

## Notizen

- wir werden nur endliche Graphen betrachten
- $\mathcal{G}$  ist schlingenfrei gdw.  $\mathcal{G}$  keine Schlinge hat

## Beispiel

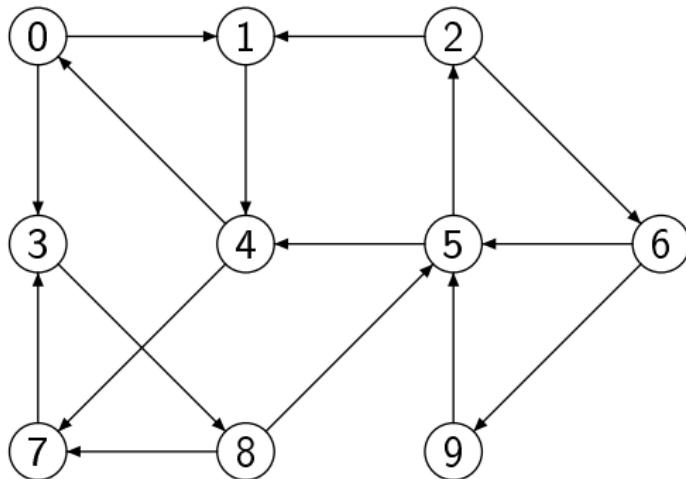


nicht: vollständig, ungerichtet und schlingenfrei vollständig,  
aber endlich und schlingenfrei

## §12.3 Definition

Seien  $(E, K)$  ein Graph und  $e \in E$  eine Ecke.

- Die **Vorgänger von  $e$**  sind  $V(e) = \{e' \in E \mid (e', e) \in K\}$ .  
(Ecken, die Kante zu  $e$  haben)
- Die **Nachfolger von  $e$**  sind  $N(e) = \{e' \in E \mid (e, e') \in K\}$ .  
(Ecken, zu denen Kante von  $e$  aus existiert)
- Der **Eingangsgrad von  $e$**  ist  $\text{in-grad}(e) = |V(e)|$ .  
(Anzahl der Vorgänger)
- Der **Ausgangsgrad von  $e$**  ist  $\text{aus-grad}(e) = |N(e)|$ .  
(Anzahl der Nachfolger)



## Beispiele

- $V(0) = \{4\}$  und  $N(0) = \{1, 3\}$   
in-grad(0) = 1 und aus-grad(0) = 2
- $V(4) = \{1, 5\}$  und  $N(4) = \{0, 7\}$   
in-grad(4) = 2 und aus-grad(4) = 2

## §12.4 Theorem

Für jeden Graphen  $(E, K)$  gilt  $|K| = \sum_{e \in E} \text{aus-grad}(e)$

Beweis.

(direkt.)

$$\begin{aligned}|K| &= |\{(e, e') \mid (e, e') \in K\}| \\&= \sum_{e \in E} |\{(e, e') \mid (e, e') \in K\}| \\&= \sum_{e \in E} |\{e' \mid (e, e') \in K\}| \\&= \sum_{e \in E} |N(e)| = \sum_{e \in E} \text{aus-grad}(e)\end{aligned}$$

□

Notiz

- analog gilt  $|K| = \sum_{e \in E} \text{in-grad}(e)$

## §12.5 Definition

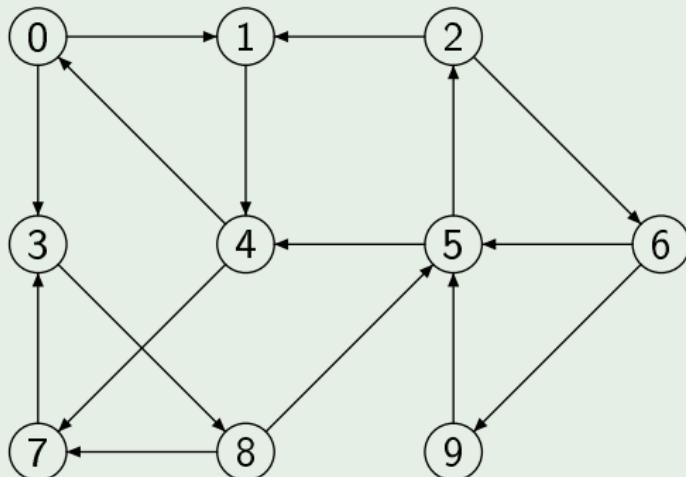
Sei  $(E, K)$  ein Graph und  $n \geq 1$ .

- Eine Folge  $(e_0 \rightarrow \dots \rightarrow e_n)$  mit  $e_0, \dots, e_n \in E$  heißt **Weg von  $e_0$  nach  $e_n$**  gdw.  $(e_i, e_{i+1}) \in K$  für alle  $0 \leq i < n$ . Ein solcher Weg hat die **Länge  $n$** .
- Gilt zusätzlich  $e_i \neq e_j$  für alle  $0 \leq i < j < n$ , dann ist  $(e_0 \rightarrow \dots \rightarrow e_n)$  sogar ein **Pfad von  $e_0$  nach  $e_n$** . (die Ecken  $(e_0, \dots, e_{n-1})$  sind paarweise verschieden)
- **Kreise** sind genau die Pfade  $(e_0 \rightarrow \dots \rightarrow e_n)$  mit  $e_0 = e_n$  und  $n \geq 3$ .

## Notizen

- Weg ist Sequenz von Ecken, so dass jede Ecke Nachfolger der vorherigen Ecke ist
- Pfad ist Weg aus verschiedenen Ecken; nur die letzte Ecke kann mit einer anderen Ecke übereinstimmen

## Beispiel



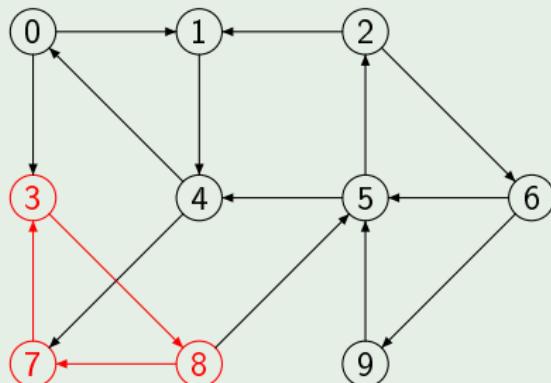
- $(3 \rightarrow 8 \rightarrow 7 \rightarrow 3 \rightarrow 8 \rightarrow 5 \rightarrow 4 \rightarrow 0)$  ist ein Weg von 3 nach 0, aber kein Pfad (wiederholt 8)
  - $(3 \rightarrow 8 \rightarrow 9 \rightarrow 5 \rightarrow 2 \rightarrow 1 \rightarrow 0)$  ist kein Weg von 3 nach 0
  - $(3 \rightarrow 8 \rightarrow 7 \rightarrow 3)$  ist ein Pfad von 3 nach 3 und ein Kreis

## §12.6 Definition

Ein Graph  $(E, K)$  ist **kreisfrei** (oder: azyklisch) gdw.  
er keinen Kreis enthält.

### Notizen

- Schlingen sind nie Kreise
- Pfade ( $e \rightarrow e' \rightarrow e$ ) sind keine Kreise
- dieser Graph ist **nicht** kreisfrei:



## §12.7 Definition

Sei  $\mathcal{G} = (E, K)$  ein Graph. Für alle  $e, e' \in E$  gelte  $e \sim_{\mathcal{G}} e'$  gdw.

- ein Weg von  $e$  nach  $e'$  existiert und
- ein Weg von  $e'$  nach  $e$  existiert.

## Notizen

- beidseitige Erreichbarkeit
- $(e)$  ist ein Weg der Länge 0 von  $e$  nach  $e$  für alle  $e \in E$

## §12.8 Theorem

Sei  $\mathcal{G} = (E, K)$  ein Graph.

Dann ist  $\sim_{\mathcal{G}}$  eine Äquivalenzrelation auf  $E$ .

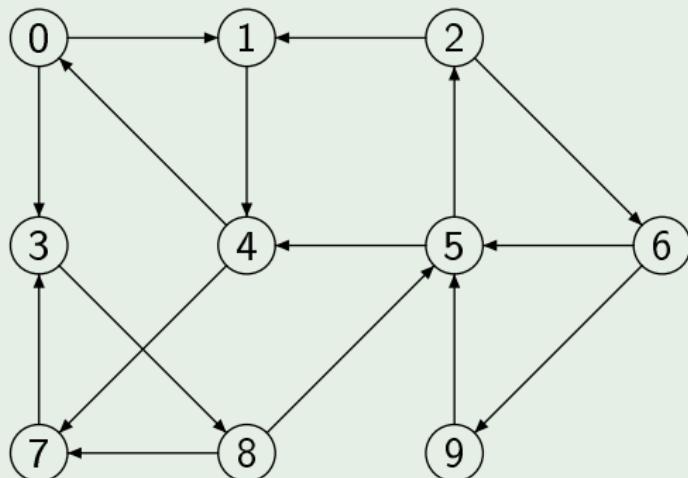
Beweis.

- **reflexiv:** Sei  $e \in E$ . Dann ist  $(e)$  ein Weg von  $e$  nach  $e$  und damit  $e \sim_{\mathcal{G}} e$ .
- **symmetrisch:** Sei  $e \sim_{\mathcal{G}} e'$ . Dann existiert ein Weg von  $e$  nach  $e'$  und ein Weg von  $e'$  nach  $e$ . Also auch  $e' \sim_{\mathcal{G}} e$ .
- **transitiv:** Seien  $e \sim_{\mathcal{G}} e'$  und  $e' \sim_{\mathcal{G}} e''$ . Dann existieren Wege
  - $(e \rightarrow \dots \rightarrow e')$  und  $(e' \rightarrow \dots \rightarrow e'')$  und
  - $(e'' \rightarrow \dots \rightarrow e')$  und  $(e' \rightarrow \dots \rightarrow e)$ .Folglich existieren auch Wege  $(e \rightarrow \dots \rightarrow e' \rightarrow \dots \rightarrow e'')$  und  $(e'' \rightarrow \dots \rightarrow e' \rightarrow \dots \rightarrow e)$  und damit  $e \sim_{\mathcal{G}} e''$ . □

## §12.9 Definition

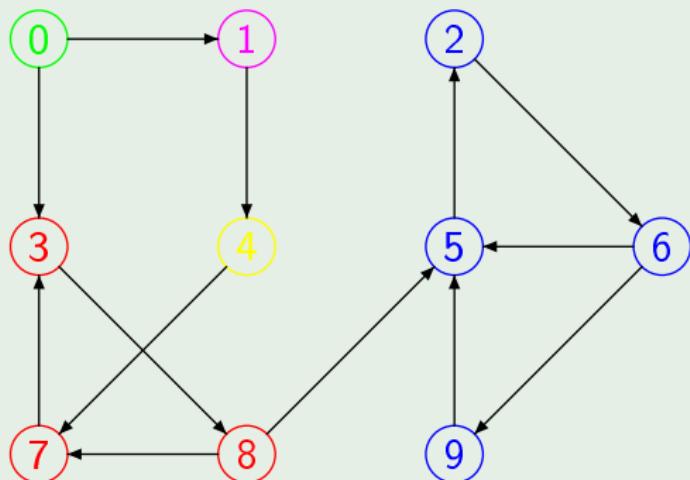
Sei  $\mathcal{G}$  ein Graph. Die Äquivalenzklassen von  $\sim_{\mathcal{G}}$  heißen **Zusammenhangskomponenten von  $\mathcal{G}$ .**

### Beispiel



hat 1 Zusammenhangskomponente  $\{0, \dots, 9\}$

## Beispiel



hat 5 Zusammenhangskomponenten

$$\{\{0\}, \{1\}, \{2, 5, 6, 9\}, \{3, 7, 8\}, \{4\}\}$$

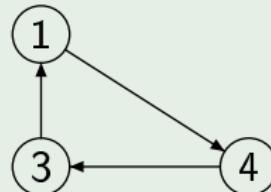
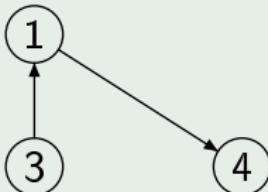
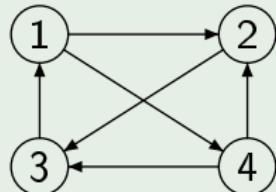
## §12.10 Definition

Seien  $\mathcal{G} = (E, K)$  und  $\mathcal{G}' = (E', K')$  zwei Graphen. Dann ist  $\mathcal{G}'$  ein Teilgraph von  $\mathcal{G}$  gdw.

$$E' \subseteq E \quad \text{und} \quad K' \subseteq K$$

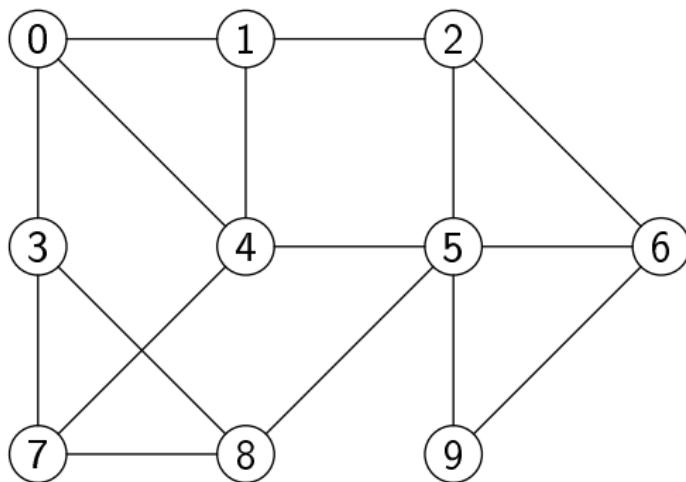
Gelten  $E' \subseteq E$  und  $K' = K \cap (E' \times E')$ , dann heißt  $\mathcal{G}'$  auch  $E'$ -Teilgraph von  $\mathcal{G}$ .

## Beispiele



- 2. Graph ist Teilgraph des 1. Graph
- 3. Graph ist  $\{1, 3, 4\}$ -Teilgraph des 1. Graph

## Ungerichtete Graphen

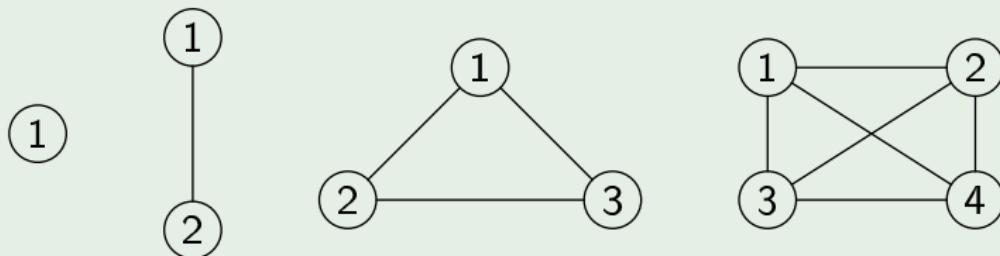


## Notizen

- Kanten in beide Richtungen ohne Pfeil
- **keine** BOOLEsche Algebra ist ein ungerichteter Graph  
(da mind. 2 Elemente und antisymmetrisch)

## Beispiele

Schlingenfrei vollständige Graphen:



## §12.11 Theorem

Für jeden ungerichteten Graphen  $(E, K)$  und  $e \in E$  gilt

- $V(e) = N(e)$
- $\text{in-grad}(e) = \text{aus-grad}(e)$

Beweis.

Einfaches Überprüfen ...



Notizen

- $N(e)$  heißt auch **Nachbarschaft von  $e$**
- wir schreiben auch  $\text{grad}(e)$  statt  $\text{aus-grad}(e)$  [oder  $\text{in-grad}(e)$ ] und nennen es **Grad von  $e$**

## §12.12 Theorem

In jedem endlichen, schlingenfreien und ungerichteten Graphen  $(E, K)$  ist die Anzahl der Ecken mit ungeradem Grad gerade.

Beweis.

(direkt.) Ein endlicher, schlingenfreier und ungerichteter Graph hat eine gerade Zahl  $|K|$  an Kanten. Also ist nach §12.4 auch  $|K| = \sum_{e \in E} \text{grad}(e)$  gerade. Seien

$$E_g = \{e \in E \mid \text{grad}(e) \text{ gerade}\} \quad \text{und} \quad E_u = E \setminus E_g$$

Dann gilt  $\sum_{e \in E} \text{grad}(e) = \sum_{e \in E_g} \text{grad}(e) + \sum_{e \in E_u} \text{grad}(e)$ , womit  $\sum_{e \in E_u} \text{grad}(e)$  gerade ist. Da  $\text{grad}(e)$  für jedes  $e \in E_u$  ungerade ist, muss  $|E_u|$  gerade sein. □

Notiz

Auf jedem Empfang schütteln gerade viele Gäste ungerade vielen Gästen die Hand

## §12.13 Theorem

Jeder endliche ungerichtete Graph  $\mathcal{G} = (E, K)$  hat mindestens  $|E| - \lfloor \frac{|K|}{2} \rfloor$  Zusammenhangskomponenten.

Beweis.

(vollständige Induktion über  $|K|$ )

- **IA:** Sei  $|K| = 0$ . Dann gibt es keine Kanten und nur Wege der Länge 0. Damit bildet jede Ecke ihre eigene Zusammenhangskomponente, wovon es  $|E| = |E| - \lfloor \frac{|K|}{2} \rfloor$  gibt.
- **IS:** Sei  $|K| = k + 1$  und wähle  $(e, e') \in K$  beliebig. Gemäß IH hat  $\mathcal{G}' = (E, K \setminus \{(e, e'), (e', e)\})$  mind.  $|E| - \lfloor \frac{k-1}{2} \rfloor$  Zusammenhangskomponenten. Aufgrund von  $(e, e')$  hat  $\mathcal{G}$  höchstens eine Komponente weniger als  $\mathcal{G}'$ , also hat  $(E, K)$  mind.  $|E| - \lfloor \frac{k-1}{2} \rfloor - 1 = |E| - \lfloor \frac{k+1}{2} \rfloor$  Zusammenhangskomponenten. □

## §12.14 Korollar

Jeder endliche ungerichtete Graph  $\mathcal{G} = (E, K)$  mit  
1 Zusammenhangskomponente hat mind.  $2 \cdot (|E| - 1)$  Kanten.

Beweis.

Gemäß §12.13 gilt  $|E| - \lfloor \frac{|K|}{2} \rfloor \leq 1$ . Durch Umformen erhalten wir  
 $|E| \leq \lfloor \frac{|K|}{2} \rfloor + 1 \leq \frac{|K|}{2} + 1$ . Durch weiteres Umformen erhalten wir

$$|K| \geq 2 \cdot (|E| - 1)$$

□

Notiz

- es gibt Graphen mit mind.  $2 \cdot (|E| - 1)$  Kanten, die mehr als 1 Zusammenhangskomponente haben

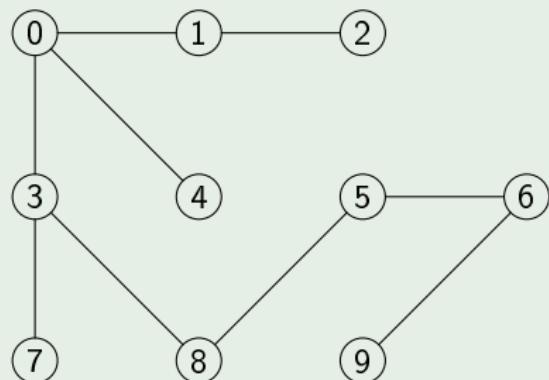
Bäume

## §12.15 Definition

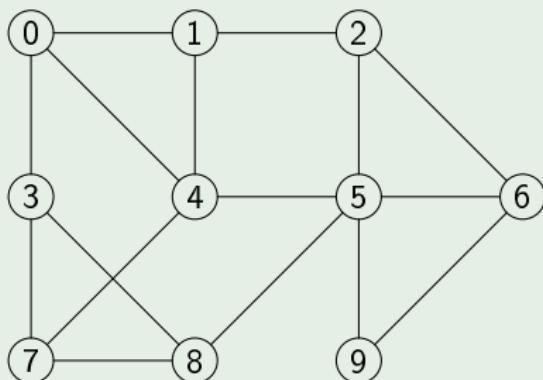
Ein ungerichteter Graph  $\mathcal{G} = (E, K)$  heißt auch **Baum** gdw.  $\mathcal{G}$  genau eine Zusammenhangskomponente hat und sowohl schlingen- als auch kreisfrei ist.

## Beispiele

Baum



kein Baum



## §12.16 Theorem

Sei  $\mathcal{G} = (E, K)$  ein endlicher ungerichteter Graph mit genau einer Zusammenhangskomponente. Dann existiert ein Baum  $\mathcal{T} = (E, K')$ , der ein Untergraph von  $\mathcal{G}$  ist.

Beweis (1/2).

Wir betrachten die Menge

$$\mathcal{M} = \{(E'', K'') \mid E'' \subseteq E, K'' \subseteq K, (E'', K'') \text{ Baum}\}$$

die nichtleer ist, denn für jedes  $e \in E$  ist  $(\{e\}, \emptyset) \in \mathcal{M}$ .

Wir wählen  $(E', K') \in \mathcal{M}$  mit maximaler Anzahl von Ecken; d.h.  $|E'| \geq |E''|$  für alle  $(E'', K'') \in \mathcal{M}$ . Z.zg.  $E' = E$ . (indirekt)  
Per Definition gilt  $\emptyset \neq E' \subseteq E$  und sei  $e' \in E'$  und  $e \in E \setminus E'$ . Da  $\mathcal{G}$  nur eine Zusammenhangskomponente hat, gilt  $e' \sim_{\mathcal{G}} e$  und damit existiert ein Weg  $(e_0 \rightarrow e_1 \rightarrow \dots \rightarrow e_n)$  mit  $e_0 = e'$  und  $e_n = e$ .

Beweis (2/2).

Da  $e' \in E'$  und  $e \notin E'$  existiert  $i \leq n$ , so dass  $e_{i-1} \in E'$  und  $e_i \notin E'$ . Wir konstruieren

$$\mathcal{T}' = (E' \cup \{e_i\}, K' \cup \{(e_{i-1}, e_i), (e_i, e_{i-1})\})$$

Dies ist offensichtlich ein Baum und  $\mathcal{T}' \in \mathcal{M}$ . Es gilt aber  $|E' \cup \{e_i\}| > |E'|$ , womit der Widerspruch erreicht wird. Also gilt  $E' = E$  und damit die Behauptung. □

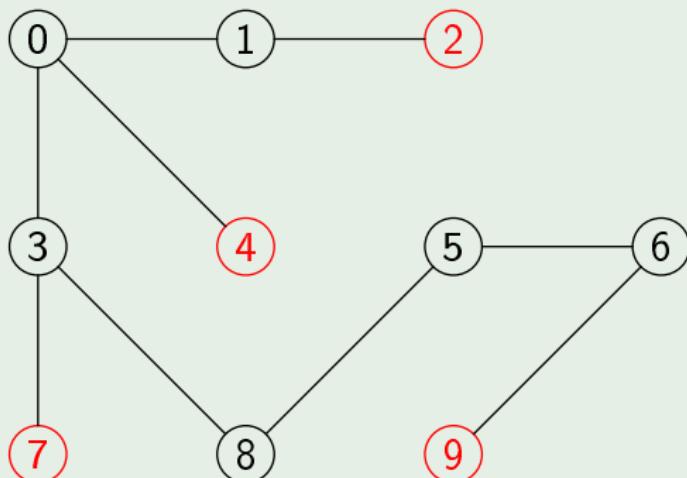
## §12.17 Definition

Sei  $(E, K)$  ein Baum.

Eine Ecke  $e \in E$  mit  $\text{grad}(e) = 1$  heißt auch **Blatt**.

### Beispiel

Blätter rot markiert



## §12.18 Theorem

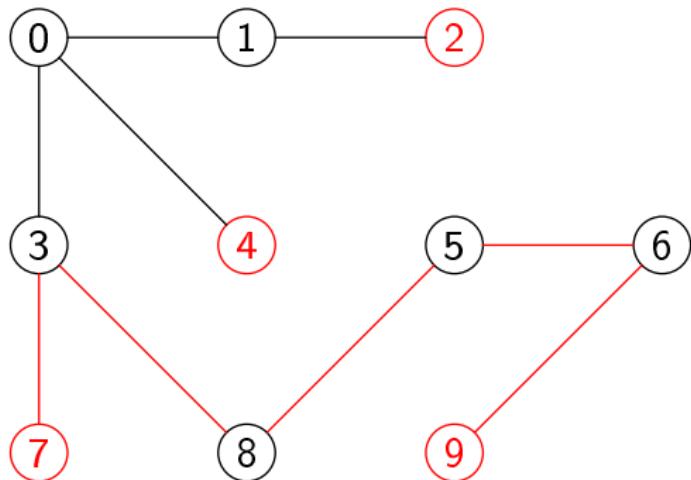
Sei  $\mathcal{T} = (E, K)$  ein endlicher Baum mit  $|E| \geq 2$ .

Dann hat  $\mathcal{T}$  mind. 2 Blätter.

### Beweis.

Da  $\mathcal{T}$  nur eine Zusammenhangskomponente hat, muss es mind. eine Kante geben. Sei  $(e, e') \in K$ . Da  $\mathcal{T}$  schlingenfrei ist, gilt  $e \neq e'$ . Da es nur endlich viele Pfade gibt (da sich die Ecken auf dem Pfad nicht wiederholen können), existiert ein Pfad  $(e_0 \rightarrow \dots \rightarrow e_n)$  maximaler Länge, so dass  $e_0 \neq e_n$ ; d.h. alle Ecken des Pfads sind verschieden. Z.zg.  $e_0$  und  $e_n$  sind Blätter. (*indirekt*) Sei  $e_0$  kein Blatt; d.h. es existiert  $e'' \in E$ , so dass  $(e_0, e'') \in K$  und  $e'' \neq e_1$ . Dann folgt auch  $e'' \neq e_i$  für alle  $i \leq n$ , denn sonst gäbe es einen Kreis. Dann ist jedoch  $(e'' \rightarrow e_0 \rightarrow \dots \rightarrow e_n)$  ein längerer Pfad mit  $e'' \neq e_n$ . Widerspruch! Analog für  $e_n$ . □

Konstruktion eines maximalen Pfads:



## §12.19 Theorem

Sei  $\mathcal{T} = (E, K)$  ein endlicher Baum. Dann gilt  $|E| = \frac{|K|}{2} + 1$ .

Beweis.

(indirekt) Sei  $(E, K)$  ein Baum mit der geringsten Anzahl an Ecken, so dass  $|E| \neq \frac{|K|}{2} + 1$ . D.h. für alle Bäume  $(E', K')$  mit  $|E'| < |E|$  gilt  $|E'| = \frac{|K'|}{2} + 1$ .

Offensichtlich gilt  $|E| \geq 2$ , denn alle Bäume  $(E', K')$  mit einer Ecke haben keine Kanten, also  $1 = |E'| = \frac{|K'|}{2} + 1 = 1$ . Also hat  $(E, K)$  zwei Blätter  $b, b'$  nach §12.18. Wir betrachten den Graph

$$(E \setminus \{b\}, K \setminus \{(b, e'), (e', b)\})$$

wobei  $N(b) = \{e'\}$ . Dies ist wieder ein Baum und da er kleiner ist, gilt die Behauptung für ihn; also  $|E| - 1 = \frac{|K|-2}{2} + 1$ . Daraus folgt jedoch  $|E| = \frac{|K|}{2} + 1$ . Widerspruch. □

Planare Graphen

## §12.20 Definition

Ein ungerichteter Graph  $(E, K)$  ist **planar** gdw.  
er in der  $(\mathbb{R} \times \mathbb{R})$ -Ebene so darstellbar ist,  
dass die Kantenbögen sich nicht überschneiden

## Notizen

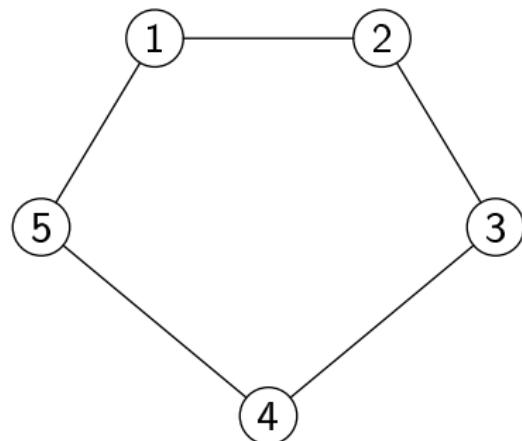
- eine überschneidungsfreie Darstellung genügt
- gleiche Graph kann völlig verschiedenen dargestellt werden

## Beispiel

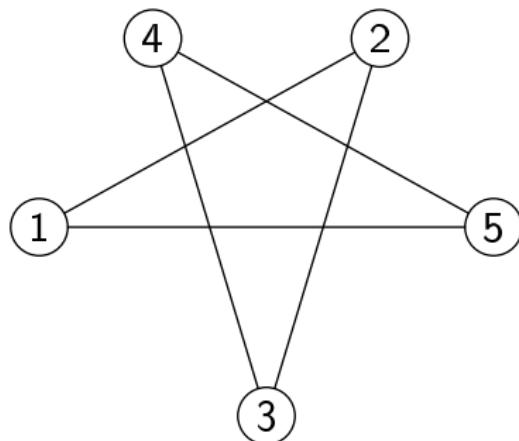
Ungerichteter Graph  $(\{1, 2, 3, 4, 5\}, K)$  ist planar, wobei

$$K = \{(1, 2), (2, 3), (3, 4), (4, 5), (5, 1), (2, 1), (3, 2), (4, 3), (5, 4), (1, 5)\}$$

planare Darstellung:

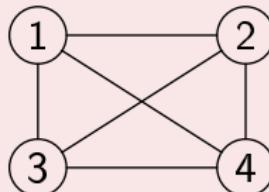


nicht-planare Darstellung:



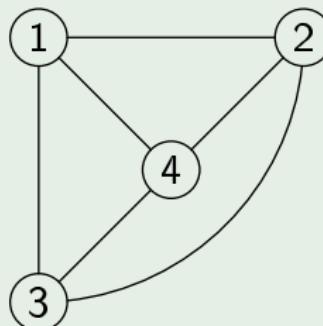
## Frage

Ist dieser ungerichtete Graph planar?



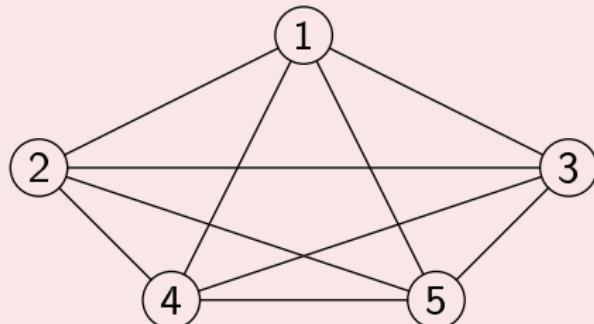
## Lösung

Ja



## Frage

Ist dieser ungerichtete Graph planar?



## Lösung

Dies scheint schwierig ...

## §12.21 Theorem (EULERSche Polyederformel)

Sei  $\mathcal{G} = (E, K)$  ein endlicher, schlingenfreier, ungerichteter Graph mit genau 1 Zusammenhangskomponente. Dann gilt

$$\text{Anzahl der Flächen} = \frac{|K|}{2} - |E| + 2$$

### Beweis (1/2).

(*Induktion über  $|K|$* ) Da  $\mathcal{G}$  nur eine Zusammenhangskomponente hat, muss  $|E| \leq \frac{|K|}{2} + 1$  gelten. Im IA sei daher  $|E| = \frac{|K|}{2} + 1$ . Gemäß §12.16 hat  $\mathcal{G}$  einen Baum  $(E, K')$  als Untergraph.

Gemäß §12.19 gilt jedoch  $|E| = \frac{|K'|}{2} + 1$  und damit  $|K'| = |K|$ . Also ist  $\mathcal{G}$  selbst ein Baum und hat damit weder Kreise noch Schlingen. Also hat  $\mathcal{G}$  keine innere Fläche und die Anzahl seiner Flächen ist 1.

$$\frac{|K|}{2} - |E| + 2 = \frac{|K|}{2} - \left(\frac{|K|}{2} + 1\right) + 2 = 1$$

## Beweis (2/2).

(Induktion über  $|K|$ ) Sei nun  $|E| < \frac{|K|}{2} + 1$ . Dann ist  $\mathcal{G}$  kein Baum (§12.19), also existiert ein Kreis  $(e_0 \rightarrow e_1 \rightarrow \dots \rightarrow e_n)$ . Wir entfernen die Kanten  $K'' = \{(e_0, e_1), (e_1, e_0)\}$ , womit zwei vorher abgetrennte Flächen zu einer Fläche verschmelzen. Für den Graphen  $\mathcal{G}' = (E, K')$  mit  $K' = K \setminus K''$  gilt die EULERSche Polyederformel gemäß IH. Also gilt

$$\text{Anzahl der Flächen von } \mathcal{G}$$

$$= \text{Anzahl der Flächen von } \mathcal{G}' + 1$$

$$= \frac{|K'|}{2} - |E| + 2 + 1$$

$$= \frac{|K|-2}{2} - |E| + 3$$

$$= \frac{|K|}{2} - |E| + 2$$

□

## LEONHARD EULER (\* 1707; † 1783)

- schweiz. Mathematiker und Physiker
- ist für einen Großteil der mathematischen Notation verantwortlich
- Universalgelehrter



## §12.22 Theorem

Sei  $\mathcal{G} = (E, K)$  ein endlicher, schlingenfreier, ungerichteter und planarer Graph mit genau 1 Zusammenhangskomponente.

Dann gilt

$$|K| \leq 6 \cdot |E| - 12$$

## Beweis.

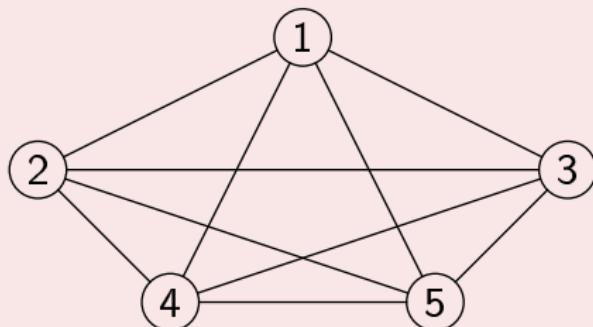
Sei  $|R|$  die Anzahl der Flächen. Jede Fläche wird von mind. 3 Kanten begrenzt und jedes Kantenpaar  $\{(e, e'), (e', e)\}$  kann nur 2 Flächen begrenzen. Es folgt  $3 \cdot |R| \leq 2 \cdot \frac{|K|}{2} = |K|$ . Unter Nutzung der EULERSchen Polyederformel erhalten wir

$$3 \cdot \left( \frac{|K|}{2} - |E| + 2 \right) = \frac{3}{2}|K| - 3|E| + 6 \leq |K|$$

Durch Umstellen erhalten wir die Behauptung. □

## Frage

Ist dieser ungerichtete Graph  $(E, K)$  planar?



## Lösung

**Nein**, denn er ist endlich, schlingenfrei und ungerichtet, aber

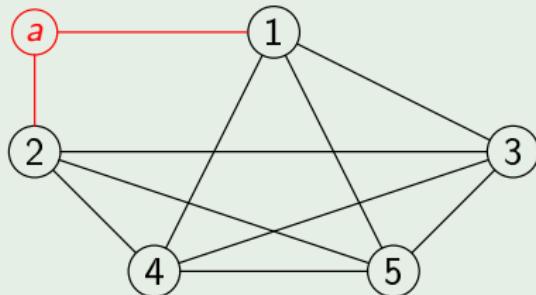
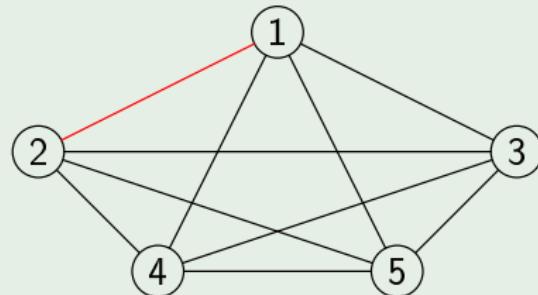
- $|K| = 20$  und  $|E| = 5$
- damit kann er gemäß §12.22 nicht planar sein,  
denn  $20 > 6 \cdot 5 - 12 = 18$

## §12.23 Definition

Sei  $\mathcal{G} = (E, K)$  ein ungerichteter schlingenfreier Graph. Ein Graph  $(E \cup \{e\}, K')$  mit  $e \notin E$  ist eine **primitive Unterteilung von  $\mathcal{G}$**  gdw. eine Kante  $(e', e'') \in K$  existiert, so dass

$$K' = (K \setminus \{(e', e''), (e'', e')\}) \cup \{(e', e), (e, e'), (e'', e), (e, e'')\}$$

## Beispiel



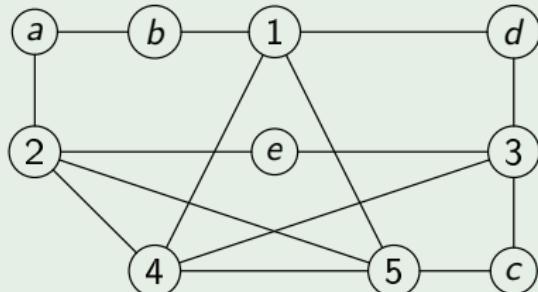
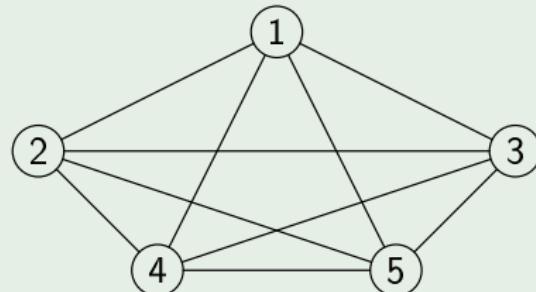
rechts eine primitive Unterteilung von links

## §12.24 Definition

Sei  $\mathcal{G} = (E, K)$  ein ungerichteter schlingenfreier Graph. Ein Graph  $\mathcal{G}' = (E', K')$  ist eine **Unterteilung von  $\mathcal{G}$**  gdw. Graphen  $\mathcal{G}_1, \dots, \mathcal{G}_n$  existieren, so dass

- $\mathcal{G}_1 = \mathcal{G}$  und  $\mathcal{G}_n = \mathcal{G}'$  und
- $\mathcal{G}_{i+1}$  eine primitive Unterteilung von  $\mathcal{G}_i$ ; für alle  $i < n$  ist

## Beispiel



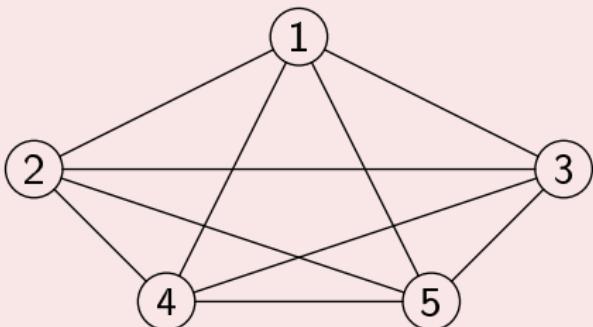
rechts eine Unterteilung von links

## §12.25 Theorem (KURATOWSKI)

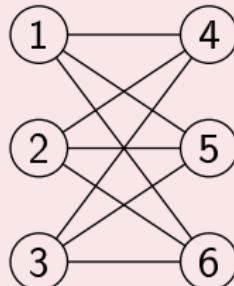
Ein Graph  $\mathcal{G}$  ist genau dann planar, wenn er keinen Teilgraphen hat, der isomorph zu

- einer Unterteilung von  $K_5$  oder
- einer Unterteilung von  $K_{3,3}$  ist.

$K_5$



$K_{3,3}$



KAZIMIERZ KURATOWSKI (\* 1896; † 1980)

- poln. Mathematiker und Logiker
- abstrakte Topologie und metr. Strukturen
- bewies ZORNs Lemma



- Definition und einfache Eigenschaften von Graphen
- Ungerichtete Graphen und Bäume
- Planare Graphen

# Diskrete Strukturen

## Vorlesung 13: Graphen II

Andreas Maletti

27. Januar 2015

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## heutige Vorlesung

- ① Adjazenzmatrix
- ② Erreichbarkeit
- ③ Gewichtete Graphen
- ④ Leichteste Wege

Bitte Fragen direkt stellen!

Organisation

## Prüfung

am **20.02.2015** um 09:00 Uhr im Hs. 3 und im AudiMax

- 1 DIN-A4-Blatt mit Notizen als Hilfsmittel zugelassen  
(beliebig beschrieben oder bedruckt)

## Tutorium

- CLAUDIO RÖHL: 29. Januar (Do.), 17 Uhr **im Hs. 17**
- ANDREAS MALETTI: 6. Februar (Fr.), 15 Uhr **im Hs. 5**

Wiederholung: Graphen

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## Definition (§12.1)

Ein (gerichteter) Graph ist eine algebraische Struktur  $\mathcal{G} = (E, K)$  des Typs  $(1, 0, 0, 0)$  mit

- einer Menge  $E$  der Ecken und
- einer Relation  $K \subseteq E \times E$  der Kanten.

Der Graph  $\mathcal{G}$  ist

- endlich gdw.  $E$  endlich ist (endlich viele Ecken)
- ungerichtet gdw.  $K$  symmetrisch ist
- schlingenfrei gdw.  $K$  irreflexiv ist

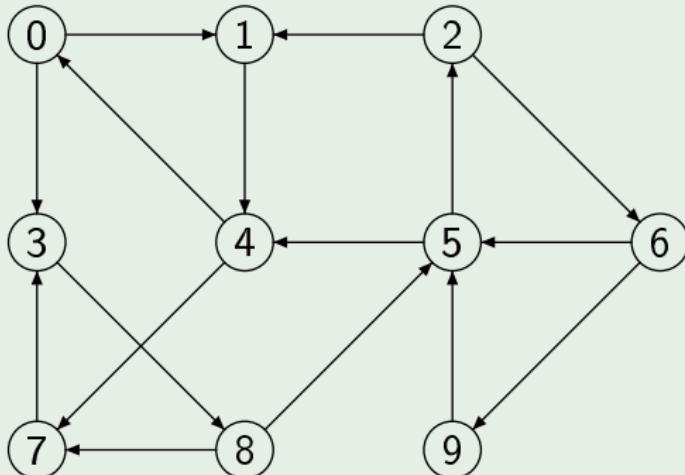
Jede Kante  $(e, e) \in K$  heißt Schlinge von  $\mathcal{G}$ .

## Definition (§12.5 und §12.6)

Sei  $(E, K)$  ein Graph und  $n \geq 1$ .

- Eine Folge  $(e_0 \rightarrow \dots \rightarrow e_n)$  mit  $e_0, \dots, e_n \in E$  heißt **Weg von  $e_0$  nach  $e_n$**  gdw.  $(e_i, e_{i+1}) \in K$  für alle  $0 \leq i < n$ . Ein solcher Weg hat die **Länge  $n$** .
- Gilt zusätzlich  $e_i \neq e_j$  für alle  $0 \leq i < j < n$ , dann ist  $(e_0 \rightarrow \dots \rightarrow e_n)$  sogar ein **Pfad von  $e_0$  nach  $e_n$** .  
(die Ecken  $(e_0, \dots, e_{n-1})$  sind paarweise verschieden)
- **Kreise** sind genau die Pfade  $(e_0 \rightarrow \dots \rightarrow e_n)$  mit  $e_0 = e_n$  und  $n \geq 3$ .
- Der Graph  $(E, K)$  ist **kreisfrei** (oder: azyklisch) gdw. er keinen Kreis enthält.

## Beispiel



- $(3 \rightarrow 8 \rightarrow 7 \rightarrow 3 \rightarrow 8 \rightarrow 5 \rightarrow 4 \rightarrow 0)$   
ist ein Weg von 3 nach 0, aber **kein** Pfad (wiederholt 8)
  - $(3 \rightarrow 8 \rightarrow 9 \rightarrow 5 \rightarrow 2 \rightarrow 1 \rightarrow 0)$  ist **kein** Weg von 3 nach 0
  - $(3 \rightarrow 8 \rightarrow 7 \rightarrow 3)$  ist ein Pfad von 3 nach 3 und ein Kreis

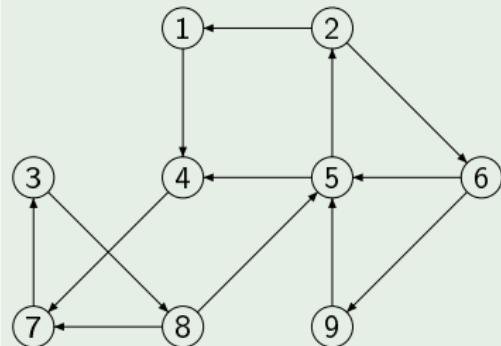
Adjazenzmatrix

## §13.1 Definition

Sei  $\mathcal{G} = (E, K)$  ein Graph mit  $E = \{1, \dots, n\}$ . Die **Adjazenzmatrix von  $\mathcal{G}$**  ist die  $(n \times n)$ -Matrix  $M_{\mathcal{G}} = (m_{ij})_{1 \leq i, j \leq n}$ , so dass für alle  $1 \leq i, j \leq n$

$$m_{ij} = \begin{cases} 1 & \text{falls } (i, j) \in K \\ 0 & \text{sonst} \end{cases}$$

## Beispiel

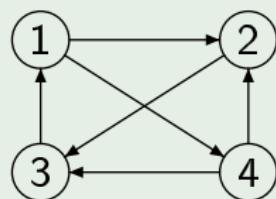


$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

## Notizen

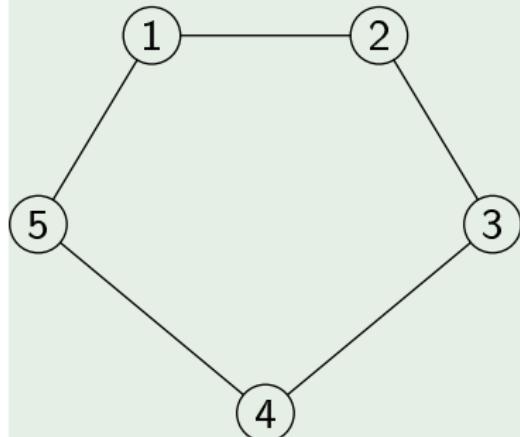
- Adjazenzmatrix  $M_{\mathcal{G}}$  leicht aus  $\mathcal{G}$  konstruierbar
- umgekehrt kann aus jeder quadratischen  $\{0, 1\}$ -Matrix  $M$  ein Graph  $\mathcal{G}$  konstruiert werden, so dass  $M = M_{\mathcal{G}}$

## Beispiel



$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

## Beispiel



$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

## §13.2 Theorem

Sei  $\mathcal{G} = (E, K)$  ein Graph mit  $E = \{1, \dots, n\}$ .

- $\mathcal{G}$  ist schlingenfrei gdw.  
die Hauptdiagonale von  $M_{\mathcal{G}}$  nur aus 0 besteht  
 $[(M_{\mathcal{G}})_{ii} = 0 \text{ für alle } 1 \leq i \leq n]$
- $\mathcal{G}$  ist ungerichtet gdw.  $M_{\mathcal{G}}$  symmetrisch ist

Beweis.

Einfaches Nachrechnen



## §13.3 Definition

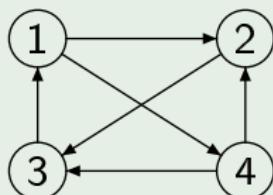
Sei  $(E, K)$  ein Graph. Die Relation  $K^* \subseteq E \times E$  definiert durch

$$K^* = \{(i, j) \mid 1 \leq i, j \leq n, \text{ ein Weg von } i \text{ nach } j \text{ existiert}\}$$

$((i, j) \in K^* \text{ gdw. } j \text{ von } i \text{ aus erreichbar ist})$

heißt **Erreichbarkeitsrelation von  $(E, K)$** .

## Beispiel



$$K^* = E \times E$$

## §13.4 Theorem

Sei  $(E, K)$  ein Graph mit  $E = \{1, \dots, n\}$ . Weiterhin seien  $1 \leq i, j \leq n$ . Falls ein Weg von  $i$  nach  $j$  existiert, dann existiert auch ein Pfad von  $i$  nach  $j$ .

### Beweis (1/2).

Wir beweisen diese Eigenschaft per Induktion über die Länge.

- **Induktionsanfang:** Sei  $(i_0)$  ein Weg der Länge 0. Dann ist  $(i_0)$  automatisch auch ein Pfad.
- **Induktionsschritt:** Sei  $(i_0 \rightarrow \dots \rightarrow i_{m-1} \rightarrow i_m)$  ein Weg der Länge  $m > 0$ . Dann ist  $(i_0 \rightarrow \dots \rightarrow i_{m-1})$  ein Weg der Länge  $m - 1$  von  $i_0$  nach  $i_{m-1}$ . Gemäß Induktionshypothese existiert ein Pfad  $(j_0 \rightarrow \dots \rightarrow j_{m-1})$  von  $i_0$  nach  $i_{m-1}$ . Also gelten  $j_0 = i_0$  und  $j_{m-1} = i_{m-1}$ .

Beweis (2/2).

Wir haben einen Pfad  $(j_0 \rightarrow \dots \rightarrow j_{m-1})$  von  $i_0$  nach  $i_{m-1}$ . Also gelten  $j_0 = i_0$  und  $j_{m-1} = i_{m-1}$ . Wir unterscheiden nun zwei Fälle:

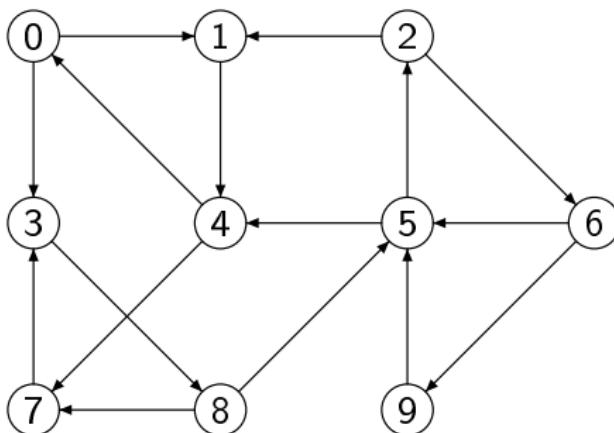
- Falls  $(j_0 \rightarrow \dots \rightarrow j_{m-1} \rightarrow i_m)$  bereits ein Pfad ist, dann sind wir offensichtlich fertig.
- Sei  $(j_0 \rightarrow \dots \rightarrow j_{m-1} \rightarrow i_m)$  **kein** Pfad. Da  $(j_0 \rightarrow \dots \rightarrow j_{m-1})$  ein Pfad ist, existiert genau ein  $0 \leq \ell < m - 1$ , so dass  $j_\ell = j_{m-1}$ . Dann ist  $(j_0 \rightarrow \dots \rightarrow j_\ell \rightarrow i_m)$  ein Weg von  $j_0 = i_0$  nach  $i_m$ , denn

$$(j_\ell, i_m) = (j_{m-1}, i_m) = (i_{m-1}, i_m) \in K$$

Des Weiteren ist dies offensichtlich ein Pfad, denn  $(j_0 \rightarrow \dots \rightarrow j_\ell \rightarrow \dots \rightarrow j_{m-1})$  ist ein Pfad.

In beiden Fällen erhalten wir einen Pfad von  $i_0$  nach  $i_m$ .

□



## Illustration

- um aus einem Weg einen Pfad zu machen, schneiden wir die enthaltenen Schlingen und Kreise heraus
- $(3 \rightarrow 8 \rightarrow 7 \rightarrow 3 \rightarrow 8 \rightarrow 5 \rightarrow 4 \rightarrow 0)$  ist ein Weg von 3 nach 0, aber **kein** Pfad
- $(3 \rightarrow 8 \rightarrow 5 \rightarrow 4 \rightarrow 0)$  ist Pfad von 3 nach 0

## §13.5 Korollar

Sei  $(E, K)$  ein Graph mit  $E = \{1, \dots, n\}$ . Weiterhin seien  $1 \leq i, j \leq n$ . Falls ein Weg von  $i$  nach  $j$  existiert, dann existiert auch ein Weg von  $i$  nach  $j$  mit Länge  $\ell < n$ .

### Beweis.

Falls ein Weg von  $i$  nach  $j$  existiert, dann existiert gemäß §13.4 auch ein Pfad  $(i_0 \rightarrow \dots \rightarrow i_\ell)$  von  $i$  nach  $j$ . Dieser Pfad, der natürlich auch ein Weg ist, hat höchstens die Länge  $\ell \leq n$ , denn sonst müssen sich Ecken wiederholen. Wir unterscheiden wieder zwei Fälle:

- Sei  $\ell < n$ . Dann gilt die Aussage.
- Sei  $\ell = n$ . Aufgrund der Pfadeigenschaft sind  $\{i_0, \dots, i_{\ell-1}\}$  paarweise verschieden, also existiert ein  $0 \leq k \leq \ell - 1$ , so dass  $i_k = i_\ell$ . Dann ist  $(i_0 \rightarrow \dots \rightarrow i_k)$  auch ein Weg von  $i_0 = i$  nach  $i_k = i_\ell = j$  der Länge  $k < \ell \leq n$ . □

Erreichbarkeit

## §13.6 Definition

Sei  $\mathcal{G} = (E, K)$  ein Graph mit  $E = \{1, \dots, n\}$ . Dann ist  $M_{\mathcal{G}}^0 = \mathbf{1}$  die  $(n \times n)$ -Einheitsmatrix und  $M_{\mathcal{G}}^{k+1} = M_{\mathcal{G}}^k \cdot M_{\mathcal{G}}$  für alle  $k \in \mathbb{N}$ .  
(Multiplikation von Matrizen)

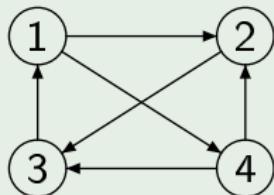
## Zur Erinnerung: Multiplikation von Matrizen

Seien  $K = (k_{ij})_{1 \leq i,j \leq n}$  und  $M = (m_{ij})_{1 \leq i,j \leq n}$   $(n \times n)$ -Matrizen.  
Dann ist  $K \cdot M = (p_{ij})_{1 \leq i,j \leq n}$  die  $(n \times n)$ -Matrix mit

$$p_{ij} = \sum_{\ell=1}^n k_{i\ell} \cdot m_{\ell j}$$

(Zeile mal Spalte)

## Beispiel



$$M_{\mathcal{G}} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

$$M_{\mathcal{G}}^2 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

## §13.7 Theorem

Sei  $\mathcal{G} = (E, K)$  ein Graph mit  $E = \{1, \dots, n\}$ . Weiterhin seien  $k \in \mathbb{N}$  und  $M_{\mathcal{G}}^k = (p_{ij})_{1 \leq i, j \leq n}$ . Für alle  $1 \leq i, j \leq n$  ist  $p_{ij}$  die Anzahl der Wege der Länge  $k$  von  $i$  nach  $j$ .

### Beweis (1/2).

Wir beweisen diese Aussage per Induktion über  $k$ .

- **Induktionsanfang:** Sei  $k = 0$ . Dann ist  $M_{\mathcal{G}}^0 = \mathbf{1}$  die Einheitsmatrix. In der Tat existiert für jedes  $1 \leq i \leq n$  der Weg  $(i)$  der Länge 0 von  $i$  nach  $i$ . Weitere Wege der Länge 0 existieren nicht. Daher sind  $p_{ii} = 1$  und  $p_{ij} = 0$  korrekt für alle  $1 \leq i, j \leq n$  mit  $i \neq j$ .

## Beweis (2/2).

Wir beweisen diese Aussage per Induktion über  $k$ .

- **Induktionsschritt:** Sei  $k > 0$ . Dann ist  $M_G^k = M_G^{k-1} \cdot M_G$ .

Seien  $M_G^{k-1} = (q_{ij})_{1 \leq i,j \leq n}$  und  $M_G = (m_{ij})_{1 \leq i,j \leq n}$  und  $1 \leq i_0, i_k \leq n$  beliebig.

Jeder Weg  $(i_0 \rightarrow \dots \rightarrow i_{k-1} \rightarrow i_k)$  der Länge  $k$  von  $i_0$  nach  $i_k$  lässt sich aufspalten in einen Weg  $(i_0 \rightarrow \dots \rightarrow i_{k-1})$  der Länge  $k - 1$  und eine Kante  $(i_{k-1}, i_k) \in K$ . Umgekehrt liefert auch jeder Weg der Länge  $k - 1$  von  $i_0$  nach  $\ell$  zusammen mit einer Kante  $(\ell, i_k) \in K$  einen Weg der Länge  $k$  von  $i_0$  nach  $i_k$ .

Also existieren  $\sum_{\ell \in V(i_k)} q_{i_0 \ell}$  Wege von  $i_0$  nach  $i_k$ , denn  $q_{i_0 \ell}$  ist gemäß IH die Anzahl der Wege der Länge  $k - 1$  von  $i_0$  nach  $\ell$ . Weiterhin gilt  $\sum_{\ell \in V(i_k)} q_{i_0 \ell} = \sum_{\ell=1}^n q_{i_0 \ell} \cdot m_{\ell i_k} = p_{i_0 i_k}$ .  
(siehe Formel für Multiplikation von Matrizen) □

## §13.8 Theorem

Sei  $\mathcal{G} = (E, K)$  ein Graph mit  $E = \{1, \dots, n\}$ .

Für alle  $1 \leq i, j \leq n$  gilt

$$(i, j) \in K^* \quad \text{gdw.} \quad \sum_{k=0}^{n-1} (M_{\mathcal{G}}^k)_{ij} > 0$$

### Beweis.

Wie üblich beweisen wir beide Richtungen:

- ( $\leftarrow$ ) Sei  $\sum_{k=0}^{n-1} (M_{\mathcal{G}}^k)_{ij} > 0$ . Dann existiert  $0 \leq k \leq n - 1$  mit  $(M_{\mathcal{G}}^k)_{ij} > 0$ . Gemäß §13.7 existiert also ein Weg der Länge  $k$  von  $i$  nach  $j$ . Also  $(i, j) \in K^*$ .
- ( $\rightarrow$ ) Sei  $(i, j) \in K^*$ . Dann existiert ein Weg von  $i$  nach  $j$ . Gemäß §13.5 existiert dann auch ein Weg der Länge  $\ell < n$  von  $i$  nach  $j$ . Nach §13.7 gilt also  $(M_{\mathcal{G}}^\ell)_{ij} > 0$  und damit  $\sum_{k=0}^{n-1} (M_{\mathcal{G}}^k)_{ij} > 0$ .

□

## Notizen

- wir können die Erreichbarkeitsrelation  $K^*$  durch Iteration der Adjazenzmatrix  $M_G$  berechnen
- die Erreichbarkeitsrelation  $K^*$  ist immer reflexiv und transitiv (nette kleine Beweise; siehe Übung)
  - heißt auch reflexiv, transitiver Abschluss von  $K$
- Matrixiteration löst Erreichbarkeit sofort für alle Paare  $(i, j)$

Exkurs für Informatiker

## Erreichbarkeitsalgorithmus

Eingabe: Graph  $(E, K)$  und Ecken  $i, j \in E$

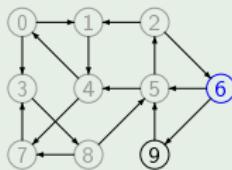
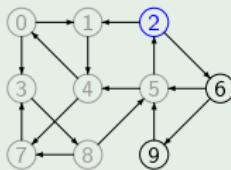
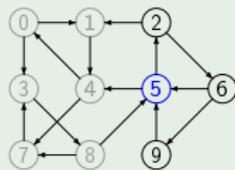
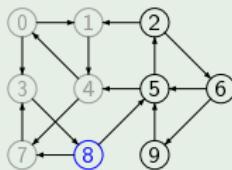
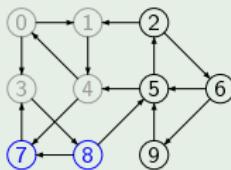
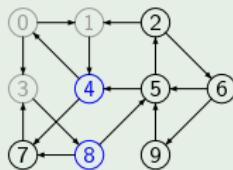
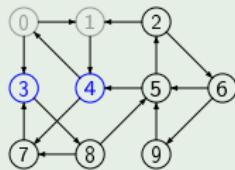
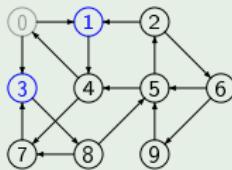
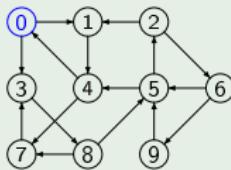
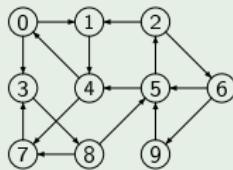
- ① setze  $B \leftarrow \emptyset$   $B = \text{besuchte Ecken}$
- ② setze  $R \leftarrow \{i\}$   $R = \text{Randecken}$
- ③ wähle eine unbesuchte Randecke  $e \in R \setminus B$  (Wahl irrelevant)
- ④ setze  $B \leftarrow B \cup \{e\}$  füge  $e$  zu  $B$  hinzu;  $e$  besucht
- ⑤ setze  $R \leftarrow R \cup N(e)$   
füge Nachfolger  $N(e)$  von  $e$  zu Randecken  $R$  hinzu
- ⑥ liefere **ja** falls  $j \in B \cup R$
- ⑦ liefere **nein** falls  $R = B$
- ⑧ gehe zu ③

# Bäume und Graphen — Erreichbarkeit

## Illustration

Erreichbarkeit  $0 \rightarrow 6$ :

$B = \text{grau}$ ;  $R = \text{blau}$



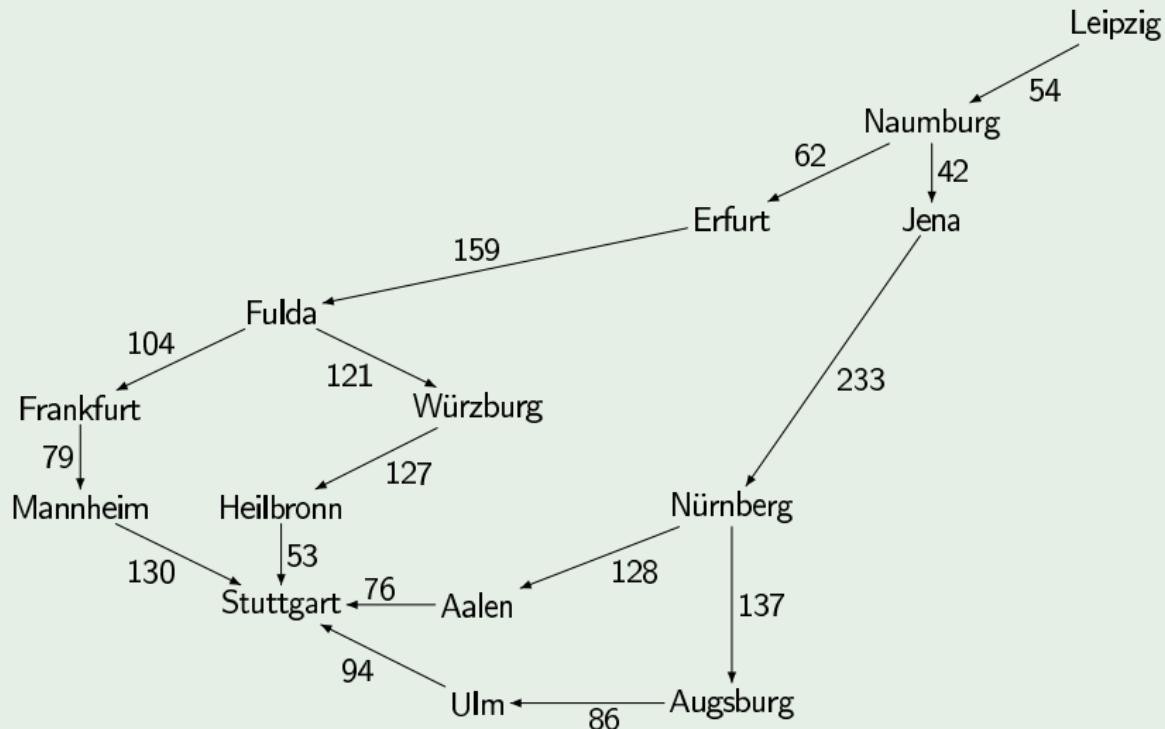
wähle 0; wähle 1; wähle 3; wähle 4; wähle 7; wähle 8; wähle 5;  
wähle 2; liefere **ja**

Gewichtete Graphen

## Motivation

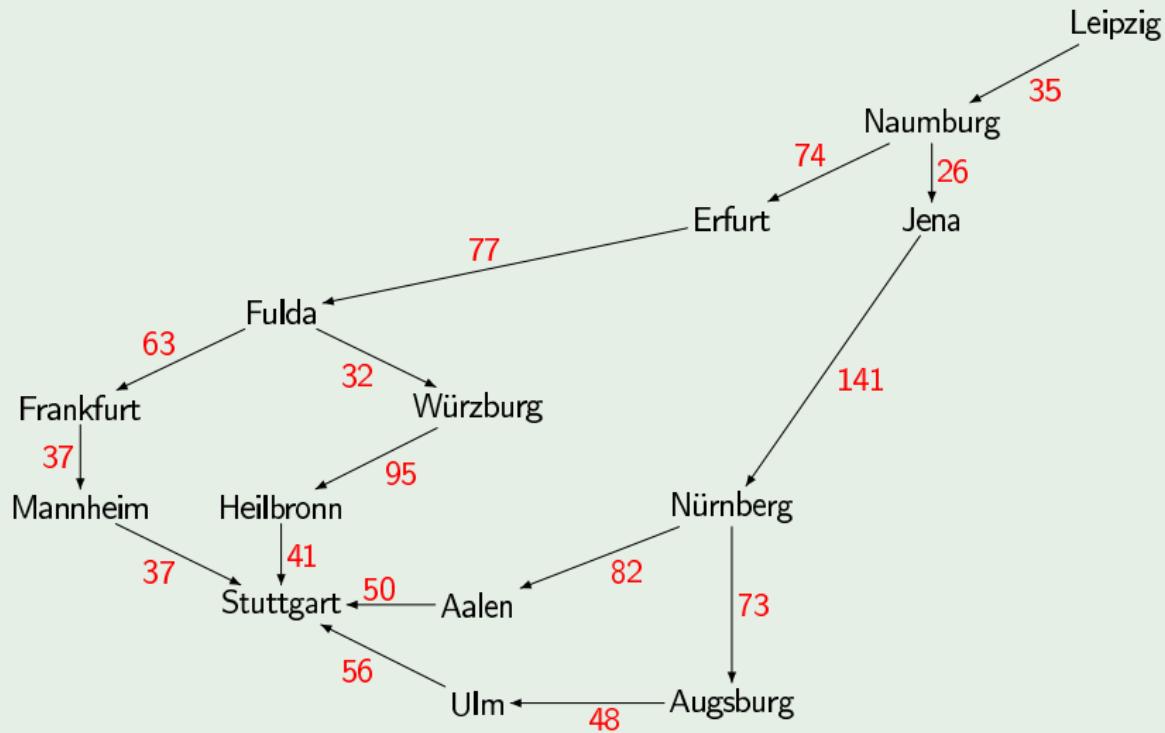
- oft werden die Kanten eines Graphen noch bewertet
  - Länge (Real-Entfernung) der Kante
  - Dauer des Übergangs entlang der Kante
  - Kapazität des Kanals
  - etc.
- wir möchten optimale Wege finden
  - kürzeste Wege
  - schnellste Verbindungen
  - maximale Flüsse

## Entfernungen (in km)



# Bäume und Graphen — Gewichtete Graphen

Dauer (in min)



## §13.9 Definition

Sei  $(E, K)$  ein Graph und  $g: K \rightarrow \mathbb{N}$  eine Funktion.

Dann ist  $(E, K, g)$  ein **gewichteter Graph** mit **Gewichtsfunktion**  $g$ .

## Notizen

- wir suchen leichteste Wege zwischen Ecken  
(die Wege geringsten Gewichts)
- dies motiviert die nächste Definition

## §13.10 Definition

Sei  $(E, K, g)$  ein gewichteter Graph und  $w = (e_0 \rightarrow \dots \rightarrow e_m)$  ein Weg von  $e_0$  nach  $e_m$ . Das **Gewicht** von  $w$  ist

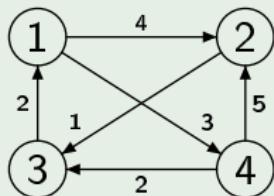
$$g(w) = \sum_{i=1}^m g(e_{i-1}, e_i)$$

## §13.11 Definition

Sei  $\mathcal{G} = (E, K, g)$  ein gewichteter Graph mit  $E = \{1, \dots, n\}$ . Die **Gewichtsmatrix von  $\mathcal{G}$**  ist die  $(n \times n)$ -Matrix  $A_{\mathcal{G}} = (a_{ij})_{1 \leq i, j \leq n}$ , so dass für alle  $1 \leq i, j \leq n$

$$a_{ij} = \begin{cases} g(i, j) & \text{falls } (i, j) \in K \\ \infty & \text{sonst} \end{cases}$$

## Beispiel



$$\begin{pmatrix} \infty & 4 & \infty & 3 \\ \infty & \infty & 1 & \infty \\ 2 & \infty & \infty & \infty \\ \infty & 5 & 2 & \infty \end{pmatrix}$$

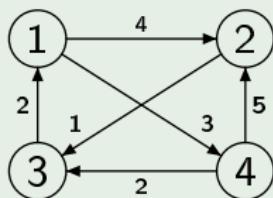
## §13.12 Definition

Sei  $\mathcal{G} = (E, K, g)$  ein gewichteter Graph mit  $E = \{1, \dots, n\}$ . Die Distanzmatrix  $D_{\mathcal{G}} = (d_{ij})_{1 \leq i, j \leq n}$  ist die  $(n \times n)$ -Matrix, so dass für alle  $1 \leq i, j \leq n$

$$d_{ij} = \begin{cases} \min\{g(w) \mid w \text{ Weg von } i \text{ nach } j\} & \text{falls } (i, j) \in K^* \\ \infty & \text{sonst} \end{cases}$$

$(d_{ij} = \text{Länge des kürzesten Weges von } i \text{ nach } j)$

## Beispiel



$$D_{\mathcal{G}} = \begin{pmatrix} 0 & 4 & 5 & 3 \\ 3 & 0 & 1 & 6 \\ 2 & 6 & 0 & 5 \\ 4 & 5 & 2 & 0 \end{pmatrix}$$

## Konventionen

- wir werden jetzt auch mit  $\infty$  rechnen
- es gelten:
  - $\infty + n = \infty$  für alle  $n \in \mathbb{N} \cup \{\infty\}$
  - $\min(\infty, n) = n$  für alle  $n \in \mathbb{N} \cup \{\infty\}$
- die “üblichen” Rechenregeln gelten weiterhin  
(Assoziativität, Kommutativität, etc.)

## §13.13 Theorem

Sei  $(E, K, g)$  ein gewichteter Graph mit  $E = \{1, \dots, n\}$ . Weiterhin seien  $1 \leq i, j \leq n$ . Falls ein Weg  $w$  von  $i$  nach  $j$  existiert, dann existiert auch ein Pfad  $w'$  von  $i$  nach  $j$  mit  $g(w') \leq g(w)$ .

Beweis (1/2 — siehe Beweis von Theorem §13.4).

Wir beweisen diese Eigenschaft per Induktion über die Länge.

- **Induktionsanfang:** Sei  $w = (i_0)$  ein Weg der Länge 0. Dann ist  $w' = w$  automatisch auch ein Pfad und es gilt  $g(w') \leq g(w)$ .
- **Induktionsschritt:** Sei  $w = (i_0 \rightarrow \dots \rightarrow i_{m-1} \rightarrow i_m)$  ein Weg der Länge  $m > 0$ . Dann ist  $v = (i_0 \rightarrow \dots \rightarrow i_{m-1})$  ein Weg der Länge  $m - 1$  von  $i_0$  nach  $i_{m-1}$ . Es gilt

$$g(v) = \sum_{k=1}^{m-1} g(i_{k-1}, i_k) \leq \sum_{k=1}^m g(i_{k-1}, i_k) = g(w)$$

□

## Beweis (2/2).

Gemäß Induktionshypothese existiert ein Pfad

$v' = (j_0 \rightarrow \dots \rightarrow j_{m-1})$  von  $i_0$  nach  $i_{m-1}$  mit  $g(v') \leq g(v)$ . Also gelten  $j_0 = i_0$  und  $j_{m-1} = i_{m-1}$ . Wir unterscheiden nun zwei Fälle:

- Falls  $w' = (j_0 \rightarrow \dots \rightarrow j_{m-1} \rightarrow i_m)$  bereits ein Pfad ist, dann gilt offensichtlich

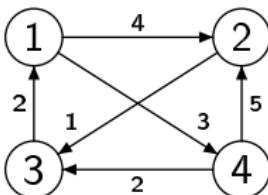
$$g(w') = g(v') + g(j_{m-1}, i_m) \leq g(v) + g(i_{m-1}, i_m) = g(w)$$

- Sei  $(j_0 \rightarrow \dots \rightarrow j_{m-1} \rightarrow i_m)$  **kein** Pfad. Da  $(j_0 \rightarrow \dots \rightarrow j_{m-1})$  ein Pfad ist, existiert genau ein  $0 \leq \ell < m - 1$ , so dass  $j_\ell = j_{m-1}$ . Dann ist  $w' = (j_0 \rightarrow \dots \rightarrow j_\ell \rightarrow i_m)$  ein Pfad von  $j_0 = i_0$  nach  $i_m$  (wie bisher). Zusätzlich gilt

$$g(w') = \left( \sum_{k=1}^{\ell} g(j_{k-1}, j_k) \right) + g(j_\ell, i_m)$$

$$\leq g(v') + g(j_{m-1}, i_m) \leq g(v) + g(i_{m-1}, i_m) = g(w)$$

□



## Illustration

- um aus einem Weg einen Pfad zu machen, schneiden wir die enthaltenen Schlingen und Kreise heraus
- das Gewicht wird dadurch höchstens kleiner
- $w = (1 \rightarrow 2 \rightarrow 3 \rightarrow 1 \rightarrow 4 \rightarrow 2 \rightarrow 3)$   
ist ein Weg von 1 nach 3, aber **kein** Pfad
- das Gewicht des Weges ist  $g(w) = 4 + 1 + 2 + 3 + 5 + 1 = 16$
- $w' = (1 \rightarrow 4 \rightarrow 2 \rightarrow 3)$  ist Pfad von 1 nach 3 mit Gewicht  $g(w') = 3 + 5 + 1 = 9$

## §13.14 Korollar

Sei  $(E, K, g)$  ein gewichteter Graph mit  $E = \{1, \dots, n\}$ . Weiterhin seien  $1 \leq i, j \leq n$ . Falls ein Weg  $w$  von  $i$  nach  $j$  existiert, dann existiert auch ein Weg  $w'$  von  $i$  nach  $j$  mit Länge  $\ell < n$  und  $g(w') \leq g(w)$ .

Beweis.

einfache Übung



Leichteste Wege

## §13.15 Definition

Seien  $K = (k_{ij})_{1 \leq i,j \leq n}$  und  $M = (m_{ij})_{1 \leq i,j \leq n}$  ( $n \times n$ )-Matrizen.  
Dann ist  $K \odot M = (p_{ij})_{1 \leq i,j \leq n}$  die ( $n \times n$ )-Matrix mit

$$p_{ij} = \min\{k_{i\ell} + m_{\ell j} \mid 1 \leq \ell \leq n\}$$

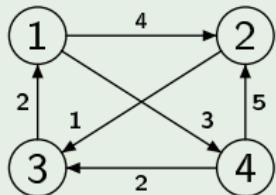
## §13.16 Definition

Sei  $\mathcal{G} = (E, K, g)$  ein gewichteter Graph mit  $E = \{1, \dots, n\}$ .

Dann seien

- $A_{\mathcal{G}}^0 = \tilde{\mathbf{0}}$  die ( $n \times n$ )-Matrix, die entlang der Hauptdiagonalen 0 und sonst  $\infty$  enthält und
- $A_{\mathcal{G}}^{k+1} = A_{\mathcal{G}}^k \odot A_{\mathcal{G}}$  für alle  $k \in \mathbb{N}$

## Beispiel



$$A_G = \begin{pmatrix} \infty & 4 & \infty & 3 \\ \infty & \infty & 1 & \infty \\ 2 & \infty & \infty & \infty \\ \infty & 5 & 2 & \infty \end{pmatrix}$$

$$A_G^2 = \begin{pmatrix} \infty & 4 & \infty & 3 \\ \infty & \infty & 1 & \infty \\ 2 & \infty & \infty & \infty \\ \infty & 5 & 2 & \infty \end{pmatrix} \odot \begin{pmatrix} \infty & 4 & \infty & 3 \\ \infty & \infty & 1 & \infty \\ 2 & \infty & \infty & \infty \\ \infty & 5 & 2 & \infty \end{pmatrix} = \begin{pmatrix} \infty & 8 & 5 & \infty \\ 3 & \infty & \infty & \infty \\ \infty & 6 & \infty & 5 \\ 4 & \infty & 6 & \infty \end{pmatrix}$$

## §13.17 Theorem

Sei  $\mathcal{G} = (E, K, g)$  ein gewichteter Graph mit  $E = \{1, \dots, n\}$ . Weiterhin seien  $k \in \mathbb{N}$  und  $A_{\mathcal{G}}^k = (a_{ij})_{1 \leq i, j \leq n}$ . Für alle  $1 \leq i, j \leq n$  ist  $a_{ij}$  das Gewicht eines leichtesten Weges der Länge  $k$  von  $i$  nach  $j$  (oder  $\infty$  falls kein solcher Weg existiert).

### Beweis (1/2).

Wir beweisen diese Aussage per Induktion über  $k$ .

- **Induktionsanfang:** Sei  $k = 0$ . Dann ist  $A_{\mathcal{G}}^k = \tilde{0}$ . In der Tat existiert für jedes  $1 \leq i \leq n$  der Weg  $(i)$  der Länge 0 von  $i$  nach  $i$  mit Gewicht 0. Weitere Wege der Länge 0 existieren nicht. Daher sind  $p_{ii} = 0$  und  $p_{ij} = \infty$  korrekt für alle  $1 \leq i, j \leq n$  mit  $i \neq j$ .

## Beweis (2/2).

Wir beweisen diese Aussage per Induktion über  $k$ .

- **Induktionsschritt:** Sei  $k > 0$ . Dann ist  $A_G^k = A_G^{k-1} \odot A_G$ . Seien  $A_G^{k-1} = (q_{ij})_{1 \leq i,j \leq n}$  und  $A_G = (m_{ij})_{1 \leq i,j \leq n}$  und  $1 \leq i_0, i_k \leq n$  beliebig. Jeder Weg  $(i_0 \rightarrow \dots \rightarrow i_{k-1} \rightarrow i_k)$  der Länge  $k$  von  $i_0$  nach  $i_k$  liefert einen Weg  $(i_0 \rightarrow \dots \rightarrow i_{k-1})$  der Länge  $k - 1$  und eine Kante  $(i_{k-1}, i_k) \in K$  (und umgekehrt).

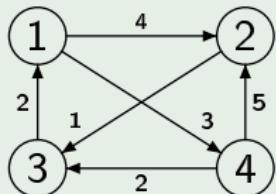
Der leichteste Weg der Länge  $k$  von  $i_0$  nach  $i_k$  hat daher Gewicht  $\min\{q_{i_0\ell} + g(\ell, i_k) \mid \ell \in V(i_k)\}$ , denn  $q_{i_0\ell}$  ist gemäß IH das Gewicht des leichtesten Weges der Länge  $k - 1$  von  $i_0$  nach  $\ell$ . Weiterhin gilt

$$\begin{aligned}& \min\{q_{i_0\ell} + g(\ell, i_k) \mid \ell \in V(i_k)\} \\&= \min\{q_{i_0\ell} + m_{\ell i_k} \mid 1 \leq \ell \leq n\} = a_{i_0 i_k}\end{aligned}$$

(siehe Formel für  $\odot$  von Matrizen)



## Beispiel



$$A_G = \begin{pmatrix} \infty & 4 & \infty & 3 \\ \infty & \infty & 1 & \infty \\ 2 & \infty & \infty & \infty \\ \infty & 5 & 2 & \infty \end{pmatrix}$$

$$A_G^0 = \begin{pmatrix} 0 & \infty & \infty & \infty \\ \infty & 0 & \infty & \infty \\ \infty & \infty & 0 & \infty \\ \infty & \infty & \infty & 0 \end{pmatrix}$$

$$A_G^1 = \begin{pmatrix} \infty & 4 & \infty & 3 \\ \infty & \infty & 1 & \infty \\ 2 & \infty & \infty & \infty \\ \infty & 5 & 2 & \infty \end{pmatrix}$$

$$A_G^2 = \begin{pmatrix} \infty & 8 & 5 & \infty \\ 3 & \infty & \infty & \infty \\ \infty & 6 & \infty & 5 \\ 4 & \infty & 6 & \infty \end{pmatrix}$$

$$A_G^3 = \begin{pmatrix} 7 & \infty & 9 & \infty \\ \infty & 7 & \infty & 6 \\ \infty & 10 & 7 & \infty \\ 8 & 8 & \infty & 7 \end{pmatrix}$$

## §13.18 Theorem

Sei  $\mathcal{G} = (E, K, g)$  ein gewichteter Graph mit  $E = \{1, \dots, n\}$ .

Für alle  $1 \leq i, j \leq n$  gilt

$$(D_{\mathcal{G}})_{ij} = \min\{(A_{\mathcal{G}}^k)_{ij} \mid 0 \leq k \leq n-1\}$$

### Beweis.

Falls kein Weg von  $i$  nach  $j$  existiert, dann gilt  $(A_{\mathcal{G}}^k)_{ij} = \infty$  für alle  $0 \leq k \leq n-1$  gemäß §13.17. Also ist auch  $(D_{\mathcal{G}})_{ij} = \infty$ .

Sei  $w$  ein leichtester Weg von  $i$  nach  $j$ . Dann gilt  $(D_{\mathcal{G}})_{ij} = g(w)$ . Dann existiert gemäß §13.14 auch ein Weg  $w'$  der Länge  $\ell < n$  von  $i$  nach  $j$  mit Gewicht  $g(w') \leq g(w)$ . Weiterhin gilt  $(A_{\mathcal{G}}^{\ell})_{ij} \leq g(w')$  gemäß §13.17. Also gilt auch

$$\begin{aligned} \min\{(A_{\mathcal{G}}^k)_{ij} \mid 0 \leq k \leq n-1\} &\leq g(w') \\ &\leq g(w) \leq \min\{(A_{\mathcal{G}}^k)_{ij} \mid 0 \leq k \leq n-1\}, \end{aligned}$$

da  $w$  ein leichtester Weg von  $i$  nach  $j$  ist. □

## Notizen

- wir können die Distanzmatrix  $D_{\mathcal{G}}$  durch  
     $\odot$ -Iteration der Gewichtsmatrix  $A_{\mathcal{G}}$  berechnen
- die Distanzmatrix  $K^*$  hat immer 0 auf der Hauptdiagonale  
(nette kleine Beweise; siehe Übung)
- Matrixiteration löst Distanzproblem für alle Paare  $(i, j)$

Exkurs für Informatiker

## Algorithmus von DIJKSTRA

**Eingabe:** gewichteter Graph  $(E, K, g)$  und Ecken  $i, j \in E$

- ① setze  $d(i) \leftarrow 0$  und  $d(j) \leftarrow \infty$  für alle  $j \neq i$
- ② setze  $U \leftarrow E$   $(U = \text{unbesuchte Ecken})$
- ③ wähle  $e \leftarrow \arg \min_{e' \in U} d(e')$  (leichteste unbesuchte Ecke)
- ④ setze  $d(e') \leftarrow \min(d(e'), d(e) + g(e, e'))$  für alle  $e' \in N(e)$
- ⑤ setze  $U \leftarrow U \setminus \{e\}$  (entferne  $e$  aus  $U$ ;  $e$  besucht)
- ⑥ liefere  $d(j)$  falls  $j \notin U$ ; sonst zu ③

EDSGER WYBE DIJKSTRA (\* 1930; † 2002)

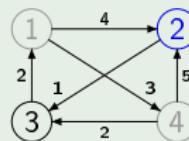
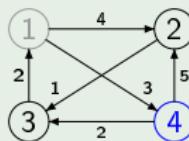
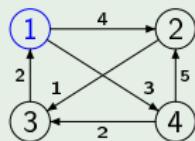
- niederl. Informatiker
- bekannt für leichteste Wege, Semaphore
- erhielt TURING-Preis



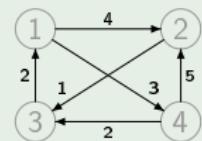
© Hamilton Richards

## Illustration

leichtester Weg  $1 \rightarrow 3$ :



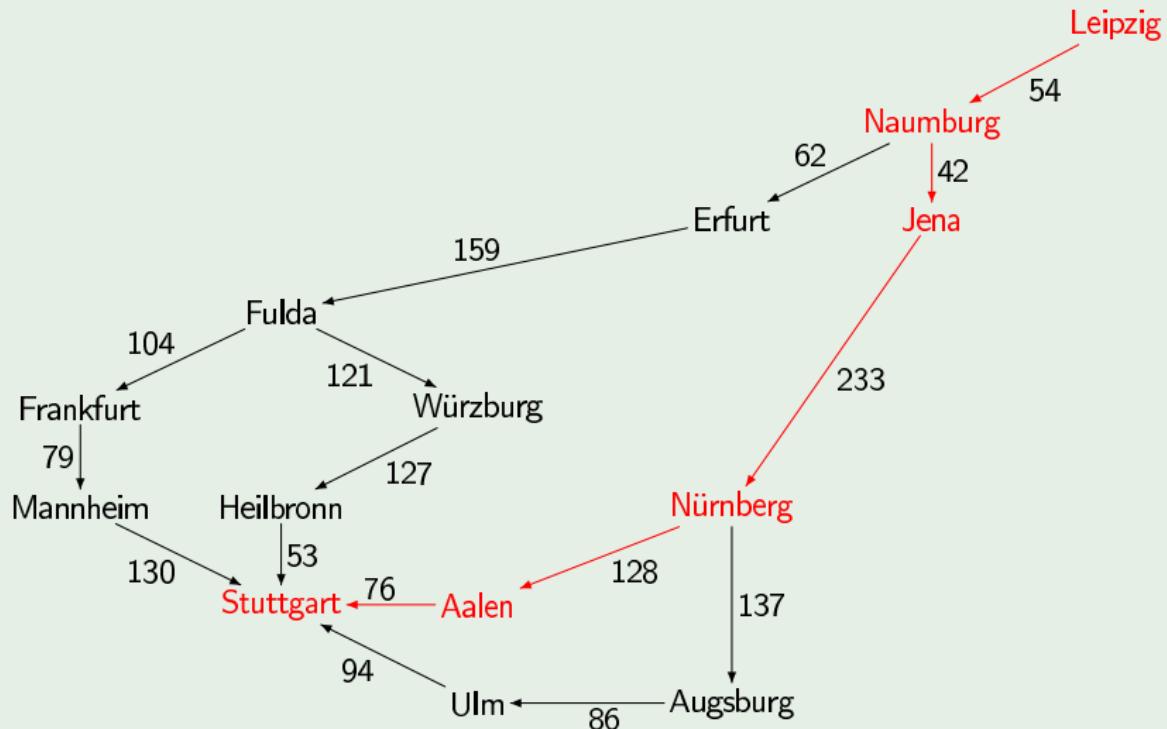
$E \setminus U = \text{grau}; e = \text{blau}$



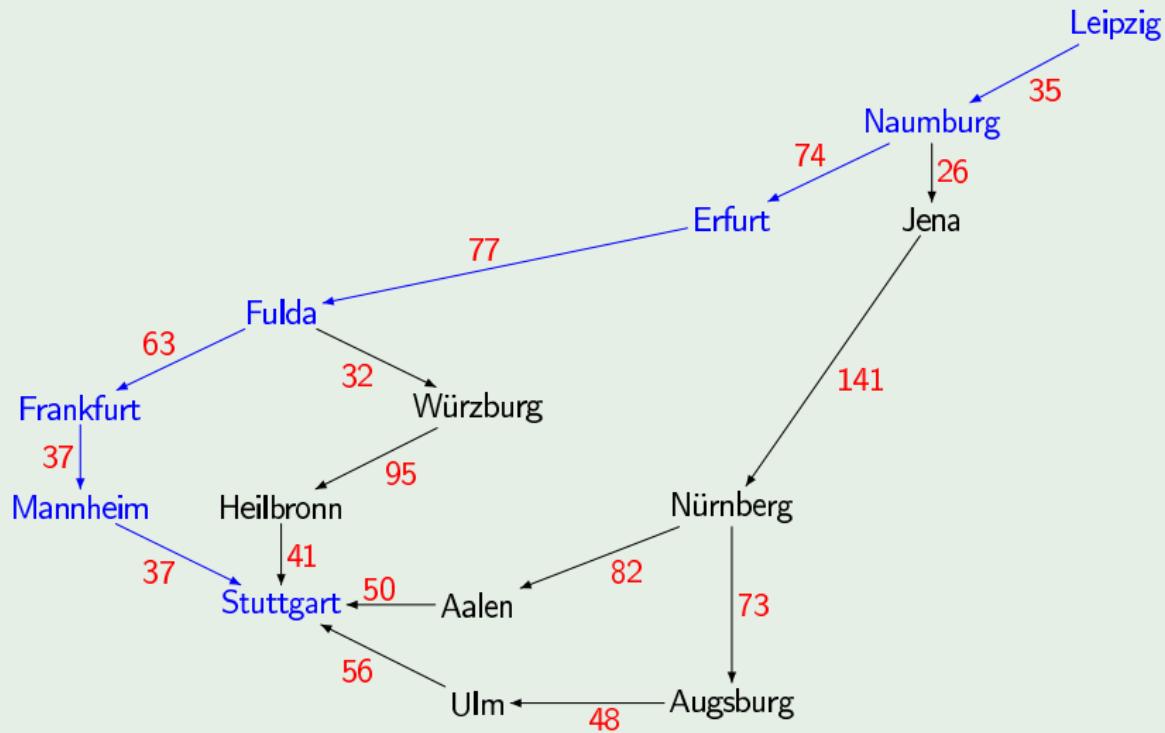
wähle 1; wähle 4; wähle 2; wähle 3; liefere 5

$e$	$d(e)$
1	0
2	4
3	5
4	3

## Entfernungen (in km)



Dauer (in min)



- Adjazenzmatrix
- Erreichbarkeit
- Gewichtete Graphen
- Leichteste Wege

# Diskrete Strukturen

## Vorlesung 14: Arithmetik

Andreas Maletti

3. Februar 2015

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## heutige Vorlesung

- ① Teilbarkeit und größte gemeinsame Teiler
- ② Modulares Rechnen
- ③ EUKLIDischer Algorithmus
- ④ erweiterter EUKLIDischer Algorithmus

Bitte Fragen direkt stellen!

Organisation

## Prüfung

am **20.02.2015** um 09:00 Uhr im Hs. 3 und im AudiMax

- 1 DIN-A4-Blatt mit Notizen als Hilfsmittel zugelassen  
(beliebig beschrieben oder bedruckt)

## Tutorium

- ANDREAS MALETTI: 6. Februar (Fr.), 15 Uhr **im Hs. 5**

Wiederholung: Teilbarkeit

## Inhalt

- ① Aussagen- und Prädikatenlogik
- ② Naive Mengenlehre
- ③ Relationen und Funktionen
- ④ Kombinatorik und Stochastik
- ⑤ Algebraische Strukturen
- ⑥ Bäume und Graphen
- ⑦ Arithmetik

## Motivation

- modulares Rechnen relevant  
(z.B. Rechnen mit Uhrzeiten, Wochentagen, Datumsangaben)
- Körper  $(\mathbb{Z}_p, +_p, \cdot_p)$  für  $p$  prim  
relevant in Kryptographie und Kodierungstheorie
- Einblick in die Natur ganzer Zahlen

## Definition

Sei  $a \in \mathbb{N} \setminus \{0\}$  und  $b \in \mathbb{Z}$ . Dann ist  $a$  **Teiler von  $b$**  gdw.  
ein  $k \in \mathbb{Z}$  existiert, so dass  $b = k \cdot a$ .  
Wir schreiben  $a|b$ , falls  $a$  Teiler von  $b$  ist.

## Beispiele

- $11|121$  denn  $121 = 11 \cdot 11$
- $n|0$  für jedes  $n \in \mathbb{N} \setminus \{0\}$ , denn  $0 = 0 \cdot n$
- $2\nmid121$  denn  $\frac{121}{2} = 60,5 \notin \mathbb{Z}$

## Definition

Sei  $b \in \mathbb{Z}$ . Dann sei

$$T_b = \{a \in \mathbb{N} \setminus \{0\} \mid a|b\}$$

die Menge aller Teiler von  $b$ .

## Beispiele

- $T_8 = \{1, 2, 4, 8\}$
- $T_9 = \{1, 3, 9\}$
- $T_{12} = \{1, 2, 3, 4, 6, 12\}$

## Eigenschaften der Teilbarkeit

## Notizen

- wir wissen bereits, dass  $|$  (Teilbarkeit) auf den positiven natürlichen Zahlen eine Ordnungsrelation ist
- hier betrachten wir  $|$  jedoch als Relation  $| \subseteq (\mathbb{N} \setminus \{0\}) \times \mathbb{Z}$

### §14.1 Theorem

Sei  $m|b$ . Dann gilt  $m|b'$  gdw.  $m|(b + b')$  für alle  $b' \in \mathbb{Z}$ .

#### Beweis.

- ( $\rightarrow$ ) Gelte  $m|b$  und  $m|b'$ . Dann existieren  $k, k' \in \mathbb{Z}$ , so dass  $b = k \cdot m$  und  $b' = k' \cdot m$ . Also gilt  
 $b + b' = km + k'm = (k + k') \cdot m$  und damit  $m|(b + b')$ .
- ( $\leftarrow$ ) Gelte  $m|b$  und  $m|(b + b')$ . Dann existieren  $k, k'' \in \mathbb{Z}$ , so dass  $b = k \cdot m$  und  $b + b' = k'' \cdot m$ . Also gilt  
 $b' = (b + b') - b = k''m - km = (k'' - k) \cdot m$  und damit  $m|b'$ .

□

## §14.2 Korollar

Seien  $a, b \in \mathbb{N} \setminus \{0\}$ . Dann gilt

$$T_a \cap T_b = T_{(a+b)} \cap T_b$$

Beweis.

( $\subseteq$ ) Sei  $m \in T_a \cap T_b$ . Also  $m|a$  und  $m|b$ . Gemäß §14.1 gilt dann  $m|(a+b)$  und damit  $m \in T_{(a+b)} \cap T_b$ .

( $\supseteq$ ) Sei  $m \in T_{(a+b)} \cap T_b$ . Also  $m|(a+b)$  und  $m|b$ . Gemäß §14.1 gilt dann  $m|a$  und damit  $m \in T_a \cap T_b$ . □

Notizen

- $a$  und  $b$  haben die gleichen Teiler wie  $a$  und  $a+b$
- dies gilt sogar für die Teiler von  $a$  und  $b$  und die Teiler von  $a$  und  $a+kb$  für  $k \in \mathbb{N}$

## §14.3 Theorem

Seien  $a, b \in \mathbb{N} \setminus \{0\}$ . Es gilt für alle  $k \in \mathbb{N}$

$$T_a \cap T_b = T_{(a+kb)} \cap T_b$$

Beweis.

Per vollständiger Induktion über  $k$ .

- **Induktionsanfang:** Für  $k = 0$  ist dies offensichtlich.
- **Induktionsschritt:** Sei  $k \in \mathbb{N}$ . Gemäß Induktionshypothese gilt  
 $T_a \cap T_b = T_{(a+kb)} \cap T_b$ . Weiterhin gilt gemäß §14.2

$$\begin{aligned} T_{(a+kb)} \cap T_b &= \underbrace{T_{(a+kb+b)}}_{=T_{(a+(k+1)b)}} \cap T_b \\ &= T_{(a+(k+1)b)} \end{aligned}$$

womit  $T_a \cap T_b = T_{(a+(k+1)b)} \cap T_b$  bereits gezeigt ist. □

## Notizen

- $T_a \cap T_b \neq \emptyset$  für alle  $a, b \in \mathbb{N} \setminus \{0\}$   
denn  $1 \in T_a$  und  $1 \in T_b$
- $T_a \cap T_b$  ist endlich für alle  $a, b \in \mathbb{N} \setminus \{0\}$   
denn  $m \leq a$  und  $m \leq b$  für alle  $m \in T_a \cap T_b$

## §14.4 Definition

Seien  $a, b \in \mathbb{N} \setminus \{0\}$ . Dann ist

$$\text{ggT}(a, b) = \max(T_a \cap T_b)$$

der **größte gemeinsame Teiler von  $a$  und  $b$** .

Die Zahlen  $a$  und  $b$  sind **teilerfremd** gdw.  $\text{ggT}(a, b) = 1$ .

## Beispiele

- $T_8 = \{1, 2, 4, 8\}$  und  $T_9 = \{1, 3, 9\}$  und  
 $T_{12} = \{1, 2, 3, 4, 6, 12\}$
- also ist  $\text{ggT}(8, 12) = 4$  und  $\text{ggT}(8, 9) = 1$
- 1 ist teilerfremd zu jeder positiven natürlichen Zahl

## §14.5 Theorem

Seien  $a, b \in \mathbb{N}$  mit  $b \geq 1$ .

Dann existieren eindeutige  $k, r \in \mathbb{N}$ , so dass

$$a = kb + r \quad \text{und} \quad 0 \leq r < b$$

### Beweis (1/2).

Wir beweisen zunächst die Existenz von  $k$  und  $r$  per vollständiger Induktion über  $a$ .

- Sei  $a = 0$ . Wir setzen  $k = 0$  und  $r = 0$ . Dann gilt  $a = kb + r$  und  $0 \leq r < b$  wie gefordert.
- Gelte die Existenz für  $a$ . Nach Induktionshypothese existieren damit  $k, r \in \mathbb{N}$ , so dass

$$a = kb + r \quad \text{und} \quad 0 \leq r < b$$

Wir unterscheiden nun 2 Fälle.

## Beweis (2/2).

- Sei  $r + 1 = b$ . Dann gilt auch

$$a + 1 = (kb + r) + 1 = kb + b = (k + 1)b + 0$$

Wir setzen also  $k' = (k + 1)$  und  $r' = 0$ .

- Sei  $r + 1 < b$ . Dann gilt auch  $a + 1 = (kb + r) + 1$ . Wir setzen also  $k' = k$  und  $r' = r + 1$ .

Damit ist die Existenz bewiesen. Seien nun  $k, k', r, r' \in \mathbb{N}$ , so dass  $a = kb + r$  und  $a = k'b + r'$  und  $0 \leq r, r' < b$ . Also gilt auch  $kb + r = k'b + r'$  und damit  $(k - k')b = r' - r$ .

- Sei  $k - k' = 0$ . Dann ist  $k = k'$  und es gilt  $0 = r' - r$ , womit auch  $r = r'$  folgt.
- Sei  $k - k' \neq 0$ . Dann ist  $|(k - k')b| \geq b$ , aber  $|r' - r| < b$ . Folglich kann dieser Fall nicht eintreten, denn  $(k - k')b = r' - r$  ist unmöglich. □

## §14.6 Definition

Seien  $a, b \in \mathbb{N}$  mit  $b \geq 1$ . Dann existieren gemäß §14.5 eindeutige  $k, r \in \mathbb{N}$ , so dass  $a = kb + r$  und  $0 \leq r < b$ .

Wir schreiben  $r = a \bmod b$ .

## Beispiele

- $5 \bmod 2 = 1$  und  $12 \bmod 2 = 0$
- $7 \bmod 4 = 3$  und  $9 \bmod 4 = 1$

Modulares Rechnen

## §14.7 Theorem

Seien  $a, b \in \mathbb{N}$  und  $m \in \mathbb{N} \setminus \{0\}$ .

Folgende Aussagen sind äquivalent:

- $r_a = r_b$  wobei  $r_a = a \bmod m$  und  $r_b = b \bmod m$
- $m|(a - b)$

Beweis.

Da  $|r_a - r_b| \leq m$  gilt

$$m|(a - b)$$

gdw.  $(\exists k \in \mathbb{N}).(a - b = km)$

gdw.  $(\exists k \in \mathbb{N}).\left(\left(\lfloor \frac{a}{m} \rfloor \cdot m + r_a\right) - \left(\lfloor \frac{b}{m} \rfloor \cdot m + r_b\right) = km\right)$

gdw.  $(\exists k \in \mathbb{N}).\left(r_a - r_b = (k - \lfloor \frac{a}{m} \rfloor + \lfloor \frac{b}{m} \rfloor) \cdot m\right)$

gdw.  $r_a = r_b$

□

## §14.8 Theorem

Seien  $a, a', b, b' \in \mathbb{N}$  und  $m \in \mathbb{N} \setminus \{0\}$ , so dass  
 $a \bmod m = a' \bmod m$  und  $b \bmod m = b' \bmod m$ . Dann gelten

- ①  $(a + b) \bmod m = (a' + b') \bmod m$
- ②  $(a \cdot b) \bmod m = (a' \cdot b') \bmod m$

## Beweis.

Beide Resultate folgen direkt aus den Resultaten zur  
Repräsentantenunabhängigkeit aus Vorlesung 11, denn  
 $a \bmod m = a' \bmod m$  und  $b \bmod m = b' \bmod m$  liefern  $a \sim_m a'$   
und  $b \sim_m b'$  nach §14.7. Also auch  $a + b \sim_m a' + b'$  und  
 $a \cdot b \sim_m a' \cdot b'$  und damit folgen die Resultate gemäß §14.7. □

## Notizen

- damit haben wir bereits die wesentlichen Rechenregeln für das modulare Rechnen
  - wir können jederzeit mit “kleinen Zahlen” rechnen  
(Zahlen aus  $\{0, 1, \dots, m - 1\}$ )
- modulares Rechnen sogar einfacher als Rechnen mit  $\mathbb{N}$

## §14.9 Theorem

Seien  $a, b, c \in \mathbb{N}$  und  $m \in \mathbb{N} \setminus \{0\}$ , so dass  $c$  und  $m$  teilerfremd sind und  $(a \cdot c) \bmod m = (b \cdot c) \bmod m$ .  
Dann gilt auch  $a \bmod m = b \bmod m$ .

### Beweis.

Gemäß §14.7 folgt  $m|(ac - bc)$  und damit  $m|(a - b)c$ . Da  $m$  und  $c$  teilerfremd sind, muss  $m|(a - b)$  gelten (dies folgt aus der Primfaktorzerlegung). Gemäß §14.7 gilt daher  
 $a \bmod m = b \bmod m$ . □

## EUKLIDischer Algorithmus

## Motivation

- Algorithmus zur Berechnung des größten gemeinsamen Teilers
- sehr effizient
- bereits uralt; EUKLID präsentiert das Verfahren  
(ob er es gefunden hat, ist ungeklärt)
- ältester nicht-trivialer Algorithmus

## EUKLID VON ALEXANDRIA (3. Jhd v. Chr.)

- griech. Mathematiker
- sammelte Wissen der Mathematik
- Vorreiter des strengen Beweises



## §14.10 Theorem

Seien  $a, b \in \mathbb{N} \setminus \{0\}$ . Dann gilt

$$\text{ggT}(a, b) = \text{ggT}(a \bmod b, b)$$

Beweis.

Gemäß §14.5 existiert ein eindeutiges  $k \in \mathbb{N}$ , so dass  $a = kb + r$  wobei  $r = a \bmod b$ . Weiterhin gilt

$$T_{(a \bmod b)} \cap T_b = T_{((a \bmod b) + kb)} \cap T_b$$

nach §14.3. Folglich gilt

$$T_a \cap T_b = \underbrace{T_{((a \bmod b) + kb)}}_{T_a} \cap T_b = T_{(a \bmod b)} \cap T_b ,$$

womit auch deren größte Elemente gleich sind. □

## §14.11 Definition

Sei  $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$ . Wir definieren die Funktion  $e: \mathbb{N}_+ \times \mathbb{N}_+ \rightarrow \mathbb{N}_+$  induktiv für alle  $a, b \in \mathbb{N}_+$  durch

$$e(a, b) = \begin{cases} b & \text{falls } a \bmod b = 0 \\ e(b, a \bmod b) & \text{sonst} \end{cases}$$

## Beispiel

$a$	$b$	$a \bmod b$
127	34	25
34	25	9
25	9	7
9	7	2
7	2	1
2	1	0

- wir berechnen  $e(127, 34)$
- da  $127 \bmod 34 = 25 \rightarrow e(34, 25)$
- da  $34 \bmod 25 = 9 \rightarrow e(25, 9)$
- da  $25 \bmod 9 = 7 \rightarrow e(9, 7)$
- da  $9 \bmod 7 = 2 \rightarrow e(7, 2)$
- da  $7 \bmod 2 = 1 \rightarrow e(2, 1)$
- da  $2 \bmod 1 = 0$  liefern wir 1

## §14.12 Theorem

Für alle  $a, b \in \mathbb{N} \setminus \{0\}$  gilt  $e(a, b) = \text{ggT}(a, b)$ .

Beweis (1/2).

per vollständiger Induktion über  $b$ .

- **Induktionsanfang:** Sei  $b = 1$ . Dann ist offensichtlich  $\text{ggT}(a, b) = b$  und ebenso  $e(a, b) = b$ , denn  $a \bmod b = a \bmod 1 = 0$ .
- **Induktionsschritt:** Die Aussage gelte für  $b \leq m$  und sei  $b' = m + 1$ . Wir unterscheiden mehrere Fälle:
  - Sei  $a \bmod b' = 0$ . Dann gilt  $e(a, b') = b'$  und ebenso  $\text{ggT}(a, b') = b'$ , denn  $b'$  ist Teiler von  $a$  und offensichtlich der größte Teiler von  $b'$ .
  - Sei  $a \bmod b' \neq 0$ . Dann unterscheiden wir zwei weitere Fälle.

## Beweis (2/2).

Wir sind im Induktionsschritt und es gilt  $a \bmod b' \neq 0$ .

- Sei zuerst  $a < b'$ . Dann gilt offensichtlich  $a \bmod b' = a$  und damit  $e(a, b') = e(b', a)$ . Da  $a < b' = m + 1$  gilt  $a \leq m$  und aus der Induktionshypothese folgt  $e(b', a) = \text{ggT}(b', a)$ . Damit folgt

$$e(a, b') = e(b', a) = \text{ggT}(b', a) = \text{ggT}(a, b')$$

- Sei also nun  $a > b'$ . Dann ist  $a \bmod b' < b'$  und damit gilt

$$e(a, b') = e(b', a \bmod b') \quad (\text{Def. } e)$$

$$= \text{ggT}(b', a \bmod b') \quad (\text{IH})$$

$$= \text{ggT}(a \bmod b', b')$$

$$= \text{ggT}(a, b') \quad (\S 14.10)$$

womit die Induktion abgeschlossen ist. □

## Beispiel

wir berechnen  $e(16.607.184, 2.367.488)$

$a$	$b$	$a \bmod b$
16.607.184	2.367.488	34.768
2.367.488	34.768	3.264
34.768	3.264	2.128
3.264	2.128	1.136
2.128	1.136	992
1.136	992	144
992	144	128
144	128	16
128	16	0

## §14.13 Theorem

Für alle  $a, b \in \mathbb{N} \setminus \{0\}$  existieren  $m, n \in \mathbb{Z}$  mit  $e(a, b) = ma + nb$ .

Beweis (1/2).

per vollständiger Induktion über die Anzahl der Iterationen bei der Berechnung von  $e(a, b)$ .

- **Induktionsanfang:** Die Berechnung von  $e(a, b)$  terminiert sofort. Dann gilt  $a \bmod b = 0$  und  $e(a, b) = b$ . Wir setzen  $m = 0$  und  $n = 1$ . Dann gilt  $e(a, b) = b = ma + nb$ .
- **Induktionsschritt:** Es gilt offensichtlich  $e(a, b) = e(b, a \bmod b)$  und gemäß Induktionshypothese existieren  $m, n \in \mathbb{Z}$  mit  $e(b, a \bmod b) = mb + n(a \bmod b)$ .

$$\begin{aligned}mb + n(a \bmod b) &= mb + n(a - \lfloor \frac{a}{b} \rfloor \cdot b) \\&= na + (m - n \cdot \lfloor \frac{a}{b} \rfloor) \cdot b\end{aligned}$$

Beweis (2/2).

Also gilt

$$e(a, b) = \text{ggT}(a, b) \quad (\S 14.12)$$

$$= \text{ggT}(a \bmod b, b) \quad (\S 14.10)$$

$$= \text{ggT}(b, a \bmod b)$$

$$= e(b, a \bmod b) \quad (\S 14.12)$$

$$= mb + n(a \bmod b)$$

$$= na + (m - n \cdot \lfloor \frac{a}{b} \rfloor) \cdot b$$

womit die Aussage für  $m' = n$  und  $n' = m - n \lfloor \frac{a}{b} \rfloor$  bewiesen ist.  $\square$

## Erweiterter EUKLIDischer Algorithmus

## §14.14 Definition

Sei  $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$ . Wir definieren die Funktion

$e': \mathbb{N}_+ \times \mathbb{N}_+ \rightarrow \mathbb{N}_+ \times \mathbb{N}_+ \times \mathbb{N}_+$  induktiv für alle  $a, b \in \mathbb{N}_+$  durch

$$e'(a, b) = \begin{cases} (b, 0, 1) & \text{falls } a \bmod b = 0 \\ (d, n, m - n \lfloor \frac{a}{b} \rfloor) & \text{sonst,} \\ & \text{wobei } (d, m, n) = e'(b, a \bmod b) \end{cases}$$

## Notizen

- Korrektheit ergibt sich direkt aus §14.13
- (wesentlicher Teil) entdeckt von CLAUDE BACHET
- für Polynome von ÉTIENNE BÉZOUT
- wichtig für Berechnung von Inversen (siehe VL 11)

### CLAUDE GASPARD BACHET (\* 1581; † 1638)

- franz. Mathematiker
- arbeitete an Zahlentheorie
- lieferte Werk für FERMATs Notizen



### ÉTIENNE BÉZOUT (\* 1730; † 1783)

- franz. Mathematiker
- inspiriert von LEONHARD EULER
- arbeitete beim Militär



## Beispiel

wir berechnen  $e(16.607.184, 2.367.488)$

$a$	$b$	$a \text{ mod } b$	$d$	$m$	$n$	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768	16	245	-16.683	117.026
2.367.488	34.768	3.264	16	-23	245	-16.683
34.768	3.264	2.128	16	15	-23	245
3.264	2.128	1.136	16	-8	15	-23
2.128	1.136	992	16	7	-8	15
1.136	992	144	16	-1	7	-8
992	144	128	16	1	-1	7
144	128	16	16	0	1	-1
128	16	0				

wir erhalten  $e'(16.607.184, 2.367.488) = (16, -16.683, 117.026)$

- Teilbarkeit und größte gemeinsame Teiler
- Modulares Rechnen
- EUKLIDischer Algorithmus
- erweiterter EUKLIDischer Algorithmus

Sie haben es geschafft.

Vielen herzlichen Dank und viel Erfolg bei der Prüfung!