



UNIVERSITÄT
LEIPZIG

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

1. Ziele dieses Moduls

2. Aussagenlogik

Unsere Beschränkungen und Ziele

- Verschiedene Studiengänge (Informatik, Lehramtsstudenten, Mathematik)
- Einführung in die Mathematik und genaues mathematisches Denken
 - ▶ Was wir genau tun, ist weniger wichtig

- Inhalte:
 - ▶ Logik (später: Strukturen, die in einem Computer programmiert werden können, die Logik darstellen)
 - ▶ Elementarste Mengenlehre, mit einem Blick ins Unendliche (weil wir versuchen, diese Vorlesung so zu organisieren dass sie auch interessant ist und zum Nachdenken anregt)
 - ▶ Mathematische Strukturen, die in einem Computer programmiert und in Algorithmen verwendet werden können (Gruppen, Ringe, Körper, Graphen)

1. Ziele dieses Moduls

2. Aussagenlogik

Ziele für Heute

- Standardnotation lesen & schreiben
- Einführung in mathematisches Denken
- Einführung in die Formalisierung von Begriffen wie "Wahrheit" in der Mathematik
- Einführung in die Art und Weise, wie Computer in der Lage sind, Wissen zu speichern und zu verarbeiten

StGB § 211 – Mord

- Der Mörder wird mit lebenslanger Freiheitsstrafe bestraft.
- Mörder ist, wer
 - ▶ aus Mordlust, zur Befriedigung des Geschlechtstrieb, aus Habgier oder sonst aus niedrigen Beweggründen,
 - ▶ heimtückisch oder grausam oder mit gemeingefährlichen Mitteln oder
 - ▶ um eine andere Straftat zu ermöglichen oder zu verdecken, einen Menschen tötet.

- Aussagen

Anton-ist-Mörder	Anton-tötet-aus-Habgier
Anton-bekommt-lebenslang	Anton-tötet-heimtückisch

- Aussagenkombinationen

Anton-tötet-heimtückisch oder Anton-tötet-aus-Habgier
wenn Anton-ist-Mörder dann Anton-bekommt-lebenslang

- Der letzte Satz erfasst einen Teil des Gesetzes. Er erlaubt uns, eine Folgerung zu ziehen. Wenn wir wissen dass die Aussage Anton-ist-Mörder ist wahr und wir wissen das der letzte Satz ist wahr, dann wissen wir auch dass die Aussage Anton-bekommt-lebenslang ist wahr.

StVO I, § 30(3) – Sonn- & Feiertagsfahrverbot (editiert)

An Sonn- und Feiertagen dürfen (...) Lastkraftwagen nicht verkehren. Dies gilt nicht für

- die Beförderung von frischer Milch und frischen Milcherzeugnissen,
- die Beförderung von frischem Fleisch und frischen Fleischerzeugnissen,
- ...

- Aussagen: "Es ist Sonntag" "L ist ein Lastkraft", "L darf nicht verkehren", "L befördert frische Milch", ...
- Aussagenkombination:
 - ▶ "L befördert frische Milch" **oder** "L befördert frisches Fleisch"
 - ▶ **Wenn** "Es ist Sonntag" **und** ("L befördert frische Milch" **oder** "L befördert frisches Fleisch") **dann nicht wahr** das "L darf nicht verkehren"

Definition (informel). Aussage = Äußerung die entweder wahr oder falsch ist

- genau ein Wahrheitswert; obwohl darf unbekannt sein
- $1 = \text{wahr}$ und $0 = \text{falsch}$
- Beispiele von Aussagen: "LKW L-DS 2022 befördert frische Milch", "16.11.2022 war ein Feiertag in Sachsen", "2 ist prim", " $2 + 2 = 5$ ", "Jede gerade natürliche Zahl $n > 2$ ist Summe zweier Primzahlen"
- nicht Aussage: "Dieser Satz ist falsch".

Am meistens verwenden wir die große Buchstaben A, B, C,... für Aussagen. Junktoren:

- Negation $\neg F$ nicht F
- Konjunktion $F \wedge G$ F und G
- Disjunktion $F \vee G$ F oder G
- Implikation $F \rightarrow G$ wenn F , dann G
- beidseitige Implikation $F \leftrightarrow G$ F genau dann, wenn G (auch Äquivalenz genannt)

Gedankenstütze: Konjunktion $A \wedge B$ (und = unten offen), Disjunktion $A \vee B$ (oder = oben offen)

Wenn wir den Wahrheitswert von Grundaussagen kennen, dann können wir auch sagen, was der Wahrheitswert ihrer beliebigen Kombination ist. Wir verwenden die folgenden Regeln.

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

Die meisten Verständnisschwierigkeiten gehen von der Implikation aus. Eine implikative Aussage $A \rightarrow B$ besteht aus **Vorbedingung A** und **Folgerung B**.

Beispiel. Nehmen wir an, wir haben eine Regel "Wenn es um 8Uhr regnet, dann nehmen Leute einen Regenschirm mit."

- Wenn es regnet und die obige Regel wahr ist, dann wissen wir auch, dass jede Person einen Regenschirm mitnehmen muss.
- Wenn es nicht regnet und die obige Regel wahr ist, dann erlaubt sie uns keine Aussage darüber, ob wir einen Regenschirm mitnehmen oder nicht.
- Es regnet nicht, manche Leute nehmen Rengenschirm mit, manche nicht. Aber die Aussage ist wahr.

Definition (informel) - Atome & Formeln: Atome = primitive Aussagen wie A, B, Formeln = Aussagen inkl. Kombinationen

- Wahrheitswert von Atom = Gültigkeit fachlicher “Aussage”, Formel = ergibt sich aus Wahrheitswert der vorkommenden Atome, unter Anwendung der oben genannten Regeln.

- Heute sind wir insbesondere an Formeln interessiert, die immer wahr sind, unabhängig von den Werten der Atome. Mit den obigen Regeln sehen wir zum Beispiel, dass der Wert von $A \vee \neg A$ immer 1 ist, egal was der Wert von A ist.

Definition. Eine Formel ist

- eine **Tautologie** (oder **tautologisch**), falls sie unabhängig von der Belegung der Atome wahr ist. “Tautologien sind immer wahr”.
- **unerfüllbar** (oder **Kontradiktion**), falls sie unabhängig von der Belegung der Atome falsch ist. “Unerfüllbare Formeln sind immer falsch”
- **erfüllbar**, falls sie nicht unerfüllbar ist, d. h. es gibt eine Belegung der Atome, so dass die Formel wahr ist,
- **widerlegbar**, falls sie keine Tautologie ist., d. h. es gibt eine Belegung der Atome, so dass die Formel falsch ist).

Die einfachste Methode, um zu überprüfen, ob eine gegebene Formel eine Tautologie ist, ist die Verwendung der so genannten **Wahrheitstabelle** - tabellarische Auflistung aller Möglichkeiten. Schritte:

- Identifikation aller vorkommenden Atome A_1, \dots, A_n
- Auflistung aller 2^n Wahrheitswertbelegungen für A_1, \dots, A_n

A_1	A_2	\cdots	A_{n-1}	A_n	\cdots
0	0	\cdots	0	0	\cdots
0	0	\cdots	0	1	\cdots
\cdots	\cdots	\cdots	\cdots	\cdots	\cdots
1	1	\cdots	1	1	\cdots

- Berechnung der Wahrheitswerte der Teilformeln

Beispiel: ist die Formel: $(A \wedge B) \rightarrow A$ eine Tautologie? (d.H. wir zeigen dass diese Formel gilt immer, unabhängig davon was A and B sind)

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

Definition. Zwei Formeln sind äquivalent genau dann, wenn (gdw) deren Wahrheitswerte für alle Belegungen der Atome übereinstimmen.

- Die Formeln $(A \rightarrow B) \rightarrow C$ und $A \rightarrow (B \rightarrow C)$ sind nicht äquivalent.

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

Die Aussagen $A \rightarrow B$ und $\neg A \vee B$ sind äquivalent. Man nennt diese Äquivalenz "Elimination von \rightarrow ". Die Wahrheitstabelle für die Aussage $A \rightarrow B$ haben wir schon gesehen.

Hier ist die Wahrheitstabelle für die Aussage $\neg A \vee B$:

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

Wir sehen also dass die zwei Wahrheitstabellen sind gleich, was bedeutet dass die zwei Aussagen äquivalent sind.

- Ähnlich zeigen wir dass die Formeln $(A \wedge B) \wedge C$ und $A \wedge (B \wedge C)$ äquivalent sind. Diese Äquivalenz heißt “Assoziativität von \wedge ”.
- Wenn wir zwei Formeln haben, F und G , dann sind F und G äquivalent genau dann wenn die Formel $F \leftrightarrow G$ eine Tautologie ist.
 - ▶ Z.B. die Formel $(\neg A \vee B) \leftrightarrow (A \rightarrow B)$ ist eine Tautologie.

- Äquivalente Formeln können füreinander substituiert werden. Dieses Substitutionsprinzip eröffnet uns die Möglichkeit, Formeln durch **Äquivalenzketten** zu vereinfachen. Damit kann man z.B. überprüfen ob eine Formel eine Tautologie ist.
- Jetzt werden wir zwei Folien sehen mit wichtigsten Äquivalenzen, die man in solchen Äquivalenzketten benutzen kann.

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

Vorsicht - keine Assoziativität für " \rightarrow ": $(A \rightarrow B) \rightarrow C$ und $A \rightarrow (B \rightarrow C)$ sind nicht äquivalent, wie wir früher gesehen haben

Äquivalente Formeln		Bezeichnung
$\neg\neg A$	A	Involution \neg
$\neg(A \wedge B)$	$(\neg A) \vee (\neg B)$	De-Morgan-Gesetz für \wedge
$\neg(A \vee B)$	$(\neg A) \wedge (\neg B)$	De-Morgan-Gesetz für \vee
$A \wedge (A \vee B)$	A	Absorptionsgesetz für \wedge
$A \vee (A \wedge B)$	A	Absorptionsgesetz für \vee
$A \rightarrow B$	$\neg A \vee B$	Elimination von \rightarrow
$A \leftrightarrow B$	$(A \rightarrow B) \wedge (B \rightarrow A)$	Elimination von \leftrightarrow

Diese Regeln und das Substitutionsprinzip reichen immer aus, um zu zeigen, dass zwei Formeln äquivalent sind. Das ist nicht offensichtlich! Jedoch es ist so.

Beispiel: Äquivalenzkette und Substitutionsprinzip

Wir zeigen dass die Aussagen $((A \wedge B) \vee (A \wedge C)) \wedge A$ und $A \wedge (B \vee C)$ äquivalent sind.

Wir fangen mit $((A \wedge B) \vee (A \wedge C)) \wedge A$ an.

- Äquivalent zu $(A \wedge (B \vee C)) \wedge A$ (**Distributivität \wedge**)
- Äquivalent zu $A \wedge (A \wedge (B \vee C))$ (**Kommutativität \wedge**)
- Äquivalent zu $(A \wedge A) \wedge (B \vee C)$ (**Assoziativität \wedge**)
- Äquivalent zu $A \wedge (B \vee C)$ (**Idempotenz \wedge**)

Also wir sehen dass die Aussagen $((A \wedge B) \vee (A \wedge C)) \wedge A$ und $A \wedge (B \vee C)$ äquivalent sind.



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski

Mathematisches Institut

grabowski@math.uni-leipzig.de



UNIVERSITÄT
LEIPZIG

Vorlesung 2 - Aussagenlogik und Sprache der Prädikatenlogik

Diskrete Strukturen (WS 2023-24)

Łukasz Grabowski

Mathematisches Institut

1. Wiederholung
2. Vorlesungsziele
3. Beweisprinzip: Beweis von Äqivalenz
4. Beweisprinzip: Kontraposition
5. Beweisprinzipien: Modus Ponens und Fallunterscheidung
6. Beweisprinzip: Kettenschluss
7. Beweisprinzip: Indirekter Beweise oder „Beweis durch Widerspruch“
8. Die Sprache der Prädikatenlogik
9. Beweisstrategien für Sätze mit Prädikaten und Quantoren

- Atome A, B, C, \dots die Wert entweder 0 “falsch” oder 1 “wahr” haben können
- Mit Atome und Junktoren $\neg, \wedge, \vee, \rightarrow, \iff$ können wir Formeln bauen, z.B. $(A \rightarrow B) \vee C$. Die Wahrheitswerte kann man aus den Wahrheitswerten der Atome berechnet, mitte der Tabelle:

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

- Die einfachste Methode, eine gegebene Aussageformel zu untersuchen, ist anhand ihrer "Wahrheitstabelle". z.B. die Wahrheitstabelle für $\neg A \vee B$:

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

- eine **Tautologie** ist ein Formel die immer wahr ist, unabhängig davon, was sind die Werte von Atomen. Z.B. $(A \wedge B) \rightarrow A$.

- Wir sagen dass zwei Formeln F und G äquivalent sind, wenn F und G haben die gleiche Wahrheitswerte für alle Belegungen der Atome. Z.B. die Formeln $A \rightarrow B$ und $\neg A \vee B$ sind äquivalent.
 - ▶ Anders gesagt, F und G sind äquivalent, gdw die Formel $F \leftrightarrow G$ ist eine Tautologie.
- Die einfachste Methode zu checken ob zwei Formel äquivalent sind : Vergleich der Wahrheitstabellen.
- Äquivalenz ist nicht das gleiche als Gleichheit. Z.B. Die Formeln $(A \vee B) \vee C$ and $A \vee (B \vee C)$ sind äquivalent, aber dies sind zwei verschiedenen Formeln.

- Wenn wir eine große Formel F haben und darin eine Unterformel U sehen, können wir U durch eine äquivalente Unterformel U' ersetzen und erhalten so eine neue Formel F' die zu F äquivalent ist.
- Dieser “Substitutionsprinzip” eröffnet uns die Möglichkeit die Formeln zu vereinfachen, und zu zeigen dass zwei Formeln äquivalent sind, durch Äquivalenzketten.

Beispiel: Äquivalenzkette und Substitutionsprinzip

Wir zeigen dass die Aussagen $((A \wedge B) \vee (A \wedge C)) \wedge A$ und $A \wedge (B \vee C)$ äquivalent sind.

Wir fangen mit $((A \wedge B) \vee (A \wedge C)) \wedge A$ an.

- Äquivalent zu $(A \wedge (B \vee C)) \wedge A$ (**Distributivität \wedge**)
- Äquivalent zu $A \wedge (A \wedge (B \vee C))$ (**Kommutativität \wedge**)
- Äquivalent zu $(A \wedge A) \wedge (B \vee C)$ (**Assoziativität \wedge**)
- Äquivalent zu $A \wedge (B \vee C)$ (**Idempotenz \wedge**)

Also wir sehen dass die Aussagen $((A \wedge B) \vee (A \wedge C)) \wedge A$ und $A \wedge (B \vee C)$ äquivalent sind.

- Insbesondere, die Formel $((A \wedge B) \vee (A \wedge C)) \wedge A \leftrightarrow A \wedge (B \vee C)$ ist eine Tautologie.

- Im Allgemeinen ist es sehr schwierig, algorithmisch zu entscheiden, ob eine gegebene Formel eine Tautologie ist oder ob zwei gegebene Formeln äquivalent sind (dies sind so-genannte NP-komplette Probleme)

1. Wiederholung

2. Vorlesungsziele

3. Beweisprinzip: Beweis von Äqivalenz

4. Beweisprinzip: Kontraposition

5. Beweisprinzipien: Modus Ponens und Fallunterscheidung

6. Beweisprinzip: Kettenschluss

7. Beweisprinzip: Indirekter Beweise oder „Beweis durch Widerspruch“

8. Die Sprache der Prädikatenlogik

9. Beweisstrategien für Sätze mit Prädikaten und Quantoren

- Beweisprinzipien, insbesondere Kontraposition und “Beweiss durch Widerspruch”
- Warum Aussagenlogik reicht nicht - Prädikate und kurz über Prädikatenlogik

1. Wiederholung
2. Vorlesungsziele
- 3. Beweisprinzip: Beweis von Äquivalenz**
4. Beweisprinzip: Kontraposition
5. Beweisprinzipien: Modus Ponens und Fallunterscheidung
6. Beweisprinzip: Kettenschluss
7. Beweisprinzip: Indirekter Beweise oder „Beweis durch Widerspruch“
8. Die Sprache der Prädikatenlogik
9. Beweisstrategien für Sätze mit Prädikaten und Quantoren

- Gemäß der Eliminationsregel sind die Formeln $A \iff B$ und $A \rightarrow B \wedge B \rightarrow A$ äquivalent. Wir betrachten diese Regel als ein “Beweisprinzip”.
 - ▶ Um irgenwelchen Satz zu beweisen der sagt dass sagt $A \iff B$, können wir stattdessen beweisen dass $A \rightarrow B$ und $B \rightarrow A$.
- Z.B betrachten wir den Satz “Eine natürliche Zahl n ist genau dann durch 3 teilbar, wenn die Summe ihrer Dezimalziffern durch 3 teilbar ist”.
 - ▶ Da die Formeln $A \iff B$ und $(A \rightarrow B) \wedge (B \rightarrow A)$ äquivalent sind, ist dieser Satz äquivalent dem Satz “Wenn n durch 3 teilbar ist, dann ist die Summe seiner Dezimalstellen durch 3 teilbar. Und wenn die Summe seiner Dezimalziffern durch 3 teilbar ist, dann ist n durch 3 teilbar”.
- Die erste Formulierung ist natürlich kürzer und wird daher normalerweise bei der Darstellung des Ergebnisses verwendet. Bei der eigentlichen Beweisführung wäre es jedoch bequemer, mit der zweiten Formulierung zu arbeiten. Den Studenten wird im Allgemeinen geraten, beim Beweis von Äquivalenzen immer beide Implikationen zu beweisen.

1. Wiederholung
2. Vorlesungsziele
3. Beweisprinzip: Beweis von Äqivalenz
- 4. Beweisprinzip: Kontraposition**
5. Beweisprinzipien: Modus Ponens und Fallunterscheidung
6. Beweisprinzip: Kettenschluss
7. Beweisprinzip: Indirekter Beweise oder „Beweis durch Widerspruch“
8. Die Sprache der Prädikatenlogik
9. Beweisstrategien für Sätze mit Prädikaten und Quantoren

- Ein wichtiges Beweisprinzip für die Implikation ist die **Kontraposition**. Anstelle des Beweises einer Aussage $A \rightarrow B$ kann ein Beweis für die Aussage $\neg B \rightarrow \neg A$ geführt werden, da beide Aussagen äquivalent sind.

Satz. Die Formeln $A \rightarrow B$ und $\neg B \rightarrow \neg A$ sind äquivalent.

Beweis.

- $A \rightarrow B$ ist äquivalent zu $\neg A \vee B$ (**Elimination \rightarrow**)
- $\neg A \vee B$ ist äquivalent zu $\neg A \vee \neg \neg B$ (**Involution \neg**)
- $\neg A \vee \neg \neg B$ ist äquivalent zu $\neg \neg B \vee \neg A$ (**Kommutativität \vee**)
- $\neg \neg B \vee \neg A$ ist äquivalent zu $\neg B \rightarrow \neg A$ (**Elimination \rightarrow**)

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

Beweis. Anstelle von

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

beweisen wir die Kontraposition

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

Sei n eine Ganzzahl, die nicht gerade, also ungerade, ist. Dann gilt $n = 2k + 1$ für eine ganze Zahl k . Jetzt können wir schreiben

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

womit n^2 wieder ungerade (nicht gerade) ist. Damit ist die Kontraposition nachgewiesen und da die Ursprungsaussage äquivalent ist, ist diese ebenso bewiesen.



1. Wiederholung
2. Vorlesungsziele
3. Beweisprinzip: Beweis von Äqivalenz
4. Beweisprinzip: Kontraposition
- 5. Beweisprinzipien: Modus Ponens und Fallunterscheidung**
6. Beweisprinzip: Kettenschluss
7. Beweisprinzip: Indirekter Beweise oder „Beweis durch Widerspruch“
8. Die Sprache der Prädikatenlogik
9. Beweisstrategien für Sätze mit Prädikaten und Quantoren

Satz (Modus Ponens). Die Formel $(A \wedge (A \rightarrow B)) \rightarrow B$ ist eine Tautologie.

Beweis. Wir beweisen es mit Hilfe der Wahrheitstabelle. Anstatt sie explizit aufzuschreiben, ist es praktisch, die folgenden Fälle zu betrachten.

- Falls B wahr ist, dann ist $F = \cdots \rightarrow B$ wahr.
- Falls B falsch ist, dann ist entweder
 - ▶ (i) A wahr, womit $A \wedge (A \rightarrow B)$ falsch ist oder
 - ▶ (ii) A falsch, womit $A \wedge (A \rightarrow B)$ auch falsch ist. In beiden Unterfällen ist also $F' = A \wedge (A \rightarrow B)$ falsch und damit $F = F' \rightarrow B$ wahr.
- In beiden Fällen ist also, F wahr. Da es keine weiteren Fälle gibt, ist die Aussage bewiesen.

- Wir haben gerade ein weiteres Beweisprinzip benutzt : die **Fallunterscheidung**. Innerhalb eines Beweises befinden wir uns in einem von mehreren möglichen Fällen. In jedem möglichen Fall können wir eine zusätzliche Annahme benutzen.
- Zur Ausnutzung dieses Umstandes sind zwei Schritte zu erfüllen:
 - ▶ Vollständige Aufstellung der möglichen Fälle
 - ▶ Einzelbetrachtung eines jeden Falls mit Angabe eines Beweises unter Ausnutzung der zusätzlichen Annahme
- Wir können dieses Prinzip als die folgende Tautologie betrachten:
 $((A \rightarrow C) \wedge (B \rightarrow C) \wedge (A \vee B)) \rightarrow C.$

1. Wiederholung
2. Vorlesungsziele
3. Beweisprinzip: Beweis von Äqivalenz
4. Beweisprinzip: Kontraposition
5. Beweisprinzipien: Modus Ponens und Fallunterscheidung
- 6. Beweisprinzip: Kettenschluss**
7. Beweisprinzip: Indirekter Beweise oder „Beweis durch Widerspruch“
8. Die Sprache der Prädikatenlogik
9. Beweisstrategien für Sätze mit Prädikaten und Quantoren

Satz (Kettenschluss). Die Formel $((A \rightarrow B) \wedge (B \rightarrow C)) \rightarrow (A \rightarrow C)$ ist eine Tautologie.

Beweis. Wir zeigen die Kontraposition $\neg(A \rightarrow C) \rightarrow \underbrace{\neg((A \rightarrow B) \wedge (B \rightarrow C))}_{F'}$.

Fallunterscheidung:

- Falls $\neg(A \rightarrow C)$ falsch ist, dann die ganze Implikation wahr ist.
- Falls $\neg(A \rightarrow C)$ wahr ist, dann ist $A \rightarrow C$ falsch, woraus A wahr und C falsch folgen.
Betrachten wir zwei Unterfälle:
 - ▶ (i) Sei B falsch. Dann ist $A \rightarrow B$ falsch und damit F' wahr. (ii) Sei B wahr. Dann ist $B \rightarrow C$ falsch und damit F' wahr.
- In beiden Unterfällen ist F' wahr ist, also auch die ganze Implikation ist wahr.

1. Wiederholung
2. Vorlesungsziele
3. Beweisprinzip: Beweis von Äqivalenz
4. Beweisprinzip: Kontraposition
5. Beweisprinzipien: Modus Ponens und Fallunterscheidung
6. Beweisprinzip: Kettenschluss
7. **Beweisprinzip: Indirekter Beweise oder „Beweis durch Widerspruch“**
8. Die Sprache der Prädikatenlogik
9. Beweisstrategien für Sätze mit Prädikaten und Quantoren

Satz (*Reduction ad absurdum, indirekter Beweis, Beweis durch Widerspruch*): Die Formel

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

ist eine Tautologie.

Interpretation: Eine Behauptung gilt als bewiesen, wenn aus ihrer Negation ein Widerspruch hergeleitet werden kann.

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

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

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

$$2 = x^2 = \left(\frac{m}{n}\right)^2 = \frac{m^2}{n^2}$$

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

- Es gilt $2n^2 = m^2 = (2k)^2 = 4k^2$, also $n^2 = 2k^2$
- Also ist auch n^2 gerade und damit auch n . Da m und n gerade sind, sind sie nicht teilerfremd.

- Es gibt also eine teilerfremde Darstellung und gleichzeitig kann es diese nicht geben. Widerspruch. Folglich gilt die Behauptung. □
- Zur Analyse der Beweisstruktur betrachten wir die folgenden Aussagen:

- ▶ $\underbrace{\text{Es existiert eine rationale Zahl } x \text{ mit } x^2 = 2}_{\neg A}$
- ▶ $\underbrace{\text{Es existieren teilerfremde ganze Zahlen } m \text{ und } n \text{ mit } n \neq 0 \text{ und } (\frac{m}{n})^2 = 2}_{B}$

Wir zeigten nacheinander die Aussagen $\neg A \rightarrow B$ und $\neg A \rightarrow \neg B$ durch direkte Beweise, und wir leiten daraus ab, dass A gilt.

- Beachten Sie jedoch, dass bei realer Beweisführung eine passende Aussage B erst gefunden werden muss

1. Wiederholung
2. Vorlesungsziele
3. Beweisprinzip: Beweis von Äqivalenz
4. Beweisprinzip: Kontraposition
5. Beweisprinzipien: Modus Ponens und Fallunterscheidung
6. Beweisprinzip: Kettenschluss
7. Beweisprinzip: Indirekter Beweise oder „Beweis durch Widerspruch“
- 8. Die Sprache der Prädikatenlogik**
9. Beweisstrategien für Sätze mit Prädikaten und Quantoren

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

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

- Anders gesagt: wir haben die Aussage P = “jede ganze Zahl n hat die Eigenschaft dass wenn n^2 gerade ist dann ist auch n gerade.”
- Was ist die Negation? N = “Existiert eine ganze Zahl n mit der Eigenschaft dass n^2 gerade ist, aber n ungerade ist”.
- Problem: Es gibt keine Regeln der Aussagenlogik die uns sagen dass das tatsächlich N die Negation von P ist.

Unsere Beobachtungen motivieren die Einführung von pb **Variablen** und **Prädikaten**, die als "Aussagenschablonen" betrachtet werden können.

- **Quantoren** (oder Quantifikatoren) zur Modellierung der Beschränkung bzw. Wahl der Variablen.
- Intuitiv sind Prädikaten abstrakte Aussagen, in denen Variablen zugelassen sind, so dass für jede Belegung der Variablen eine konkrete Aussage entsteht.

Beispiel. Wir identifizieren

- *QuadratGerade(n) als Aussagenschablone mit*
“Das Quadrat der Zahl n ist gerade.”
- *Gerade(n) als Aussagenschablone mit*
“Die Zahl n ist gerade.”

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

- Durch Einsetzen eines konkreten Objektes erhält man eine Aussage.
- Wir führen doch noch eine Möglichkeit ein, wie man aus einem Prädikat eine Aussage erhält: **Quantifizierung**.

- Der **Allquantor** \forall fordert die Gültigkeit der Aussagenschablone für **alle** möglichen Belegungen einer Variable,
- der **Existenzquantor** \exists fordert die Gültigkeit der Aussagenschablone für **mindestens eine** Belegung einer Variable.
- Dabei nehmen wir entweder implizit ein Universum aller Objekte an, oder wir geben im Kontext der Formeln explizit einen Grundbereich für die Variablen.

Mithilfe der neuen Ausdrucksmittel erreichen wir die Formalisierung

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

wenn wir explizit den Bereich der ganzen Zahlen betrachten.

- Oder wir könnten auch schreiben

$$\forall n \left(\text{GanzeZahl}(n) \rightarrow (\text{QuadratGerade}(n) \rightarrow \text{Gerade}(n)) \right),$$

wobei $\text{GanzeZahl}(n)$ ist das Prädikat “ n ist eine ganze Zahl”.

Beispiel. Wir formalisieren die Aussage

“Es gibt keine rationale Zahl x mit $x^2 = 2$ ”

als

$$\neg \exists x (Rat(x) \wedge QuadratGleich2(x)),$$

wobei $Rat(x)$ das Prädikat “ x ist eine Rationale Zahl” ist, und $QuadratGleich2(x)$ die Prädikat “ $x^2 = 2$ ” ist.

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

$$\forall \epsilon > 0 \ \exists n \in \mathbb{N} \ \forall i, \ell \in \mathbb{N} \quad (i \geq n) \wedge (\ell \geq n) \rightarrow (|x_\ell - x_i| < \epsilon)$$

1. Wiederholung
2. Vorlesungsziele
3. Beweisprinzip: Beweis von Äqivalenz
4. Beweisprinzip: Kontraposition
5. Beweisprinzipien: Modus Ponens und Fallunterscheidung
6. Beweisprinzip: Kettenschluss
7. Beweisprinzip: Indirekter Beweise oder „Beweis durch Widerspruch“
8. Die Sprache der Prädikatenlogik
9. Beweisstrategien für Sätze mit Prädikaten und Quantoren

Weitere äquivalente Formeln		Bezeichnung
$\neg \forall x F$	$\exists x \neg F$	Negation Allquantor
$\neg \exists x F$	$\forall x \neg F$	Negation Existenzquantor

Z.B. die folgenden Aussagen sind äquivalent:

- ▶ “Es ist nicht wahr, dass jede natürliche Zahl durch 7 teilbar ist”
- ▶ “Es gibt eine natürliche Zahl n , die nicht durch 7 teilbar ist”
- ▶ Die Formalisierungen lauten jeweils $\neg \forall n P(n)$, und $\exists n \neg P(n)$, wobei $P(n)$ ist die Aussage: $7 \mid n$.

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

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

Formalisierung für das Universum natürlicher Zahlen:

$$\forall n \exists m (\text{Gerade}(m) \wedge (m > n))$$

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

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

Ein korrektes Beweis. Sei n eine beliebige natürliche Zahl.

Wir definieren $m = 2(n + 1)$.

Dann ist m offenbar durch 2 teilbar und damit gerade.

Weiterhin gilt $m - n = 2(n + 1) - n = n + 2 > 0$ und damit ist $m > n$. □



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski

Mathematisches Institut

grabowski@math.uni-leipzig.de



UNIVERSITÄT
LEIPZIG

Vorlesung 3 - Naive Mengenlehre

Diskrete Strukturen (WS 2023-24)

Łukasz Grabowski

Mathematisches Institut



Beweisprinzipien, insbesondere

- Kontraposition. Anstelle des Beweises einer Aussage $A \rightarrow B$ kann ein Beweis für die Aussage $\neg B \rightarrow \neg A$ geführt werden.
 - ▶ Als Beispiel betrachten wir den Satz “Sei n eine beliebige ganze Zahl. Falls n^2 gerade ist, so ist auch n gerade.”
 - ▶ : Beweis: Angenommen n ist nicht gerade. Also $n = 2k + 1$ mit $k \in \mathbb{Z}$, und $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Deswegen ist n^2 nicht gerade, was im Widerspruch mit der Annahme steht, dass n^2 gerade ist.

- „Beweis durch Widerspruch“. Eine Behauptung gilt als bewiesen, wenn aus ihrer Negation ein Widerspruch hergeleitet werden kann.
- $e = 1 + \frac{1}{2!} + \dots$ ist eine irrationelle Zahl.
 - Beweis durch Widerspruch. Nehmen wir an, dass e rational ist, also $e = \frac{a}{b}$ für einige teilerfremde Zahlen a, b . Sei $N \geq b$.
 - Betrachten wir die Zahl $\alpha := N!(1 + \frac{1}{2!} + \dots + \frac{1}{N!})$. Dies ist eine natürliche Zahl.
 - Wir können es aber auch schreiben als

$$\alpha = N!(e - \frac{1}{(N+1)!} - \frac{1}{(N+2)!} - \dots) = N!(\frac{a}{b} - \frac{1}{(N+1)!} - \frac{1}{(N+2)!} - \dots)$$
 - Nun ist $N! \cdot \frac{a}{b}$ eine ganze Zahl, und $N!(\frac{1}{(N+1)!} + \dots) = \frac{1}{(N+1)} + \frac{1}{(N+1)(N+2)} + \dots < \frac{1}{N+1} + \frac{1}{(N+1)^2} + \dots = \frac{1}{1 - \frac{1}{N+1}} - 1 = \frac{1}{N} < 1$.
 - Dies zeigt, dass α keine natürliche Zahl ist. Dieser Widerspruch zeigt, dass e nicht rational ist.

- Es gibt keine größte Primzahl
 - ▶ Beweis durch Widerspruch. Nehmen wir an, dass es die größte Primzahl p gibt. Dann lassen sich alle Primzahlen wie folgt auflisten $2 = p_1, 3 = p_2, \dots, p = p_n$.
 - ▶ Betrachten wir die Zahl $N := p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$.
 - ▶ Diese Zahl ist größer als p ist also nicht prim.
 - ▶ Es gibt also eine Primzahl, die N teilt. Dies ist eine der oben aufgeführten Primzahlen, nennen wir sie p_k .
 - ▶ Aber N kann als $ap + 1$ geschrieben werden, also p teilt N nicht. Dieser Widerspruch zeigt unsere These.

- Wenn wir die Behauptung direkt aus der Annahme beweisen, nennen wir so einen Beweis ein direkter Beweis.
 - ▶ Wenn n gerade ist, dann ist n^2 gerade.
 - ▶ Beweis: Wenn n gerade ist, dann können wir $n = 2k$ für irgendein k schreiben, und daher $n^2 = 4k^2 = 2 \cdot 2k^2$, was zeigt, dass n^2 gerade ist.

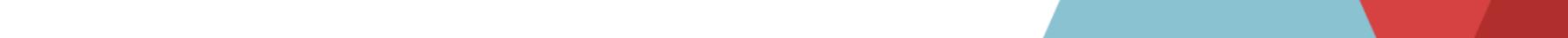
Prädikaten - “Aussagenschablonen” Intuitiv sind Prädikaten abstrakte Aussagen, in denen Variablen zugelassen sind, so dass für jede Belegung der Variablen eine konkrete Aussage entsteht.

- **Beispiel.** Für jede natürliche Zahl existiert eine echt größere gerade natürliche Zahl.
- Formalisierung für das Universum natürlicher Zahlen:

$$\forall n \exists m (\text{Gerade}(m) \wedge (m > n))$$

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

□



- Einführung in die Mengenlehre
- Beziehungen zwischen Mengen (Gleichheit, Teilmengen)
- Standardoperationen auf Mengen



Wir beginnen mit einer "naiven" Definition des Begriffs 'Menge'. Diese Definition erfasst sehr gut unsere Intuition was Mengen sein sollen. Es ist allerdings zu beachten, dass diese Definition präzisiert werden müsste, um den Normen der modernen Mathematik zu genügen. Deswegen benutzt man Begriff "naive Mengenlehre" manchmal.

Definition. (Georg Cantor 1895) Eine **Menge** M ist eine Zusammenfassung von unterscheidbaren Objekten zu einem Ganzen. Die zusammengefassten Objekte heißen **Elemente** von M .

Beispiele und Notation.

- Lkw sei die Menge aller Lastkraftwagen.
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ bezeichnen jeweils die Mengen aller natürlichen Zahlen, aller ganzen Zahlen, aller rationalen Zahlen und aller reellen Zahlen. In diesem Modul wird angenommen, dass $0 \in \mathbb{N}$.
- Vollständige oder unvollständige Aufzählung: $\{1, 2, 3\}$ bzw. $\{0, 1, 2, \dots\}$ Das Muster muss klar erkennbar sein.
- $\{1, 2, 3\} = \{1, 2, 3, 2\} = \{2, 3, 1\}$,
- Leere Menge: \emptyset enthält keine Elemente.
- $\{\emptyset\}$ ist eine Menge mit genau einem Element. Dieses Element ist die leere Menge.

- Für eine Menge M ist jedes Objekt x entweder ein Element von M (kurz $x \in M$) oder nicht (kurz $x \notin M$).
- Insbesondere kann ein Element nicht mehrfach in einer Menge enthalten sein.
 $\{1, 1, 2\} = \{1, 2\}$
- Die Elemente einer Menge können unterschiedlichen Typs und sogar selbst wieder Mengen sein. $\{\mathbb{R}, 2, \emptyset\}$
- Die Elemente einer Menge haben keine Anordnung; ihre Reihenfolge ist irrelevant.
 $\{1, 2, 3\} = \{2, 3, 1\}$
- Außerdem gilt: Jede Menge ist unterscheidbar von jedem ihrer Elemente, auch wenn Sie genau ein Element enthält. $\{3\} \neq 3$.
- Wir verkürzen “ $x \in M$ und $y \in M$ ” einfach zu “ $x, y \in M$ ”. Wenn wir $x, y, z \in \{1, 2, 3\}$ schreiben, durchaus $x = y = z$ gelten kann.

Beispiel. Welche Aussagen gelten für

$$M = \{\emptyset, \{\emptyset\}\}$$

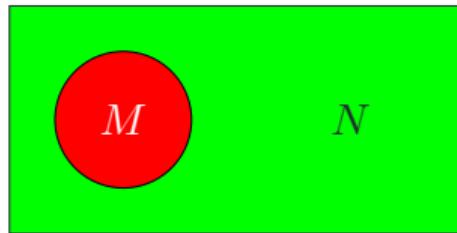
?

- $\emptyset \in M$
- $\{\emptyset\} \in M$
- $\{\{\emptyset\}\} \in M$ falsch

- Zwei Mengen M und N sind **gleich**, kurz $M = N$, wenn sie genau die gleichen Elemente enthalten.
- Insbesondere gibt es genau eine Menge die enthält keine Elemente, nämlich \emptyset .
- Eine Menge M ist eine **Teilmenge** von der Menge N , kurz $M \subseteq N$, falls jedes Element von M auch Element von N ist. Formal:

$$M \subseteq N \iff \forall m ((m \in M) \rightarrow (m \in N)).$$

$$M = N \iff \forall m ((m \in M) \rightarrow (m \in N)) \wedge \forall n ((n \in N) \rightarrow (n \in M)),$$



- Man schreibt gelegentlich auch $N \supseteq M$ (anstelle $M \subseteq N$) und nennt N Obermenge von M .
- Wir sprechen von einer echten Teilmenge und schreiben $M \subsetneq N$, falls $M \subseteq N$ und $M \neq N$.
- $\emptyset \subseteq M$ und $M \subseteq M$ für jede Menge M ,
- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$. Alle Inklusionen sind hier echt.

Satz. Für alle Mengen M und N gilt: $M = N \iff M \subseteq N \text{ und } N \subseteq M$.

Beweis. Durch Einsetzen der Definitionen:

$$M = N$$

ist äq. zu

$$\forall m ((m \in M) \rightarrow (m \in N)) \wedge \forall n ((n \in N) \rightarrow (n \in M))$$

ist äq. zu

$$(M \subseteq N) \wedge (N \subseteq M)$$

□



Die einstelligen Prädikaten sind die Prädikaten der Form $P(x)$, die sagen ob eine spezielle Eigenschaft P für ein geg. Objekt x vorliegt.

- z.B. $\text{GanzeZahl}(x)$, $\text{Gerade}(x)$, $\text{Rat}(x)$
- Wir können die Objekte, für die $P(x)$ wahr ist, in eine Menge zusammenfassen.
- Beispiele
 - ▶ $\{L \in \text{Lkw} \mid \text{hatFisch}(L)\}$ oder $\{L \in \text{Lkw} : \text{hatFisch}(L)\}$
Die Menge enthält genau die Elemente L von Lkw, für die $\text{hatFisch}(L)$ wahr ist.
 - ▶ $\{n \in \mathbb{N} \mid \text{Gerade}(n)\} = \{n \in \mathbb{N} \mid n \text{ durch } 2 \text{ teilbar}\} = \{n \in \mathbb{N} \mid \exists h(h \in \mathbb{N} \wedge n = 2h)\}.$
 - ▶ Wir haben auch $\{n \in \mathbb{N} \mid \text{Gerade}(n)\} \subseteq \{n \in \mathbb{N} \mid n \text{ ist durch } 2 \text{ teilbar}\},$
 - ▶ $\{n \in \mathbb{N} \mid n \text{ ist durch } 4 \text{ teilbar}\} \subseteq \{n \in \mathbb{N} \mid \text{Gerade}(n)\}.$

Manchmal verwenden wir informell andere Methoden zur Definition von Mengen, die der obigen Methode mit Prädikaten ähneln, aber bei näherer Betrachtung anders sind, z.B.

- $\{a + b \in \mathbb{R} : a \in \mathbb{Q}, b \in \{\sqrt{2}, \sqrt{3}\}\}$. Wenn wir es ganz formal schreiben wollen, würden wir schreiben

$$\{x \in \mathbb{R} : \exists a \in \mathbb{Q}, b \in \{\sqrt{2}, \sqrt{3}\} \text{ so dass } x = a + b\}.$$

- Bei der Mengennotation bedeutet das Zeichen , immer “und”. Z.B. $\{a \in \mathbb{Z} : 3 | a, 7 \nmid a\}$



Seien M und N Mengen.

- Die **Vereinigung** von M und N besteht aus den Elementen, die Element von M **oder** Element von N sind:

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

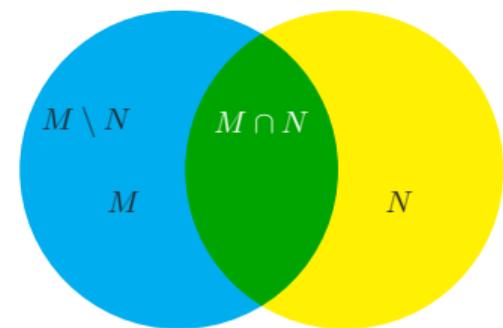
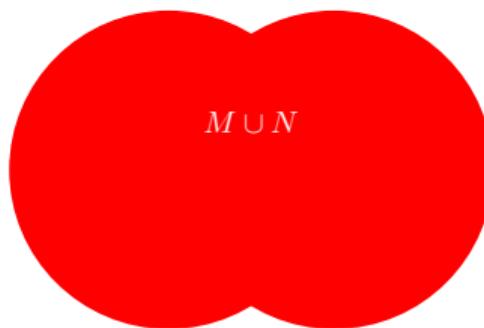
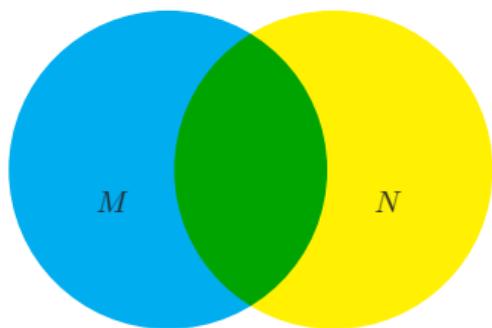
- Der **Schnitt** von M und N besteht aus den Elementen, die Element von M **und** von N sind:

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

- Die **Differenz** von M ohne N besteht aus den Elementen, die Element von M , aber **nicht** Element von N sind:

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

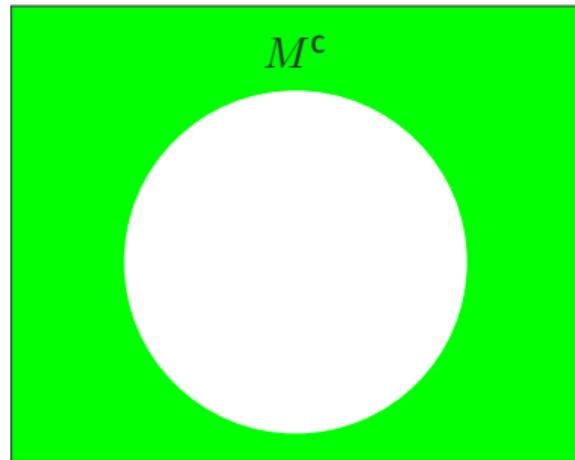
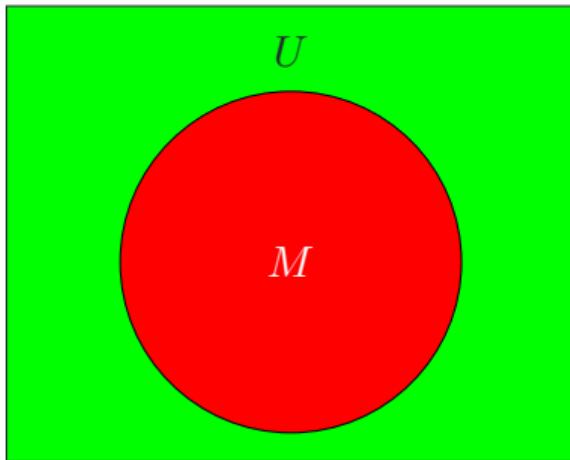
Venn-Diagramme illustrieren diese Definitionen.



Im Kontext von Mengenoperationen gehen wir oft von einer Grundmenge U aus, in der alle betrachteten Mengen enthalten sind.

- Jede Menge M teilt U implizit in zwei Teile. Das **Komplement** von $M \subseteq U$ beinhaltet genau die Elemente von U , die nicht Elemente von M sind:

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



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 . ^c
$(A \cap B)^c$	$A^c \cup B^c$	De-Morgan-Gesetz für \cap
$(A \cup B)^c$	$A^c \cap B^c$	De-Morgan-Gesetz für \cup

Wegen z.B. So rechtfertigt das Assoziativgesetz schreiben wir oft $A \cup B \cup C$ statt $A \cup (B \cup C)$.

Beispiel - Beweis (Distributivitat) Durch Anwendung der Definitionen erhalten wir:

$$M \cup (N \cap P) = \{x \mid (x \in M) \vee (x \in N \cap P)\}$$

$$= \{x \mid (x \in M) \vee (x \in \{y \mid (y \in N) \wedge (y \in P)\})\}$$

$$= \{x \mid (\underbrace{x \in M}_A) \vee (\underbrace{(x \in N)}_B \wedge \underbrace{(x \in P)}_C)\}$$

$$= \{x \mid (\underbrace{(x \in M)}_A \vee \underbrace{(x \in N)}_B) \wedge (\underbrace{(x \in M)}_A \vee \underbrace{(x \in P)}_C)\}$$

$$= \{x \mid (x \in M \cup N) \wedge (x \in M \cup P)\} = (M \cup N) \cap (M \cup P) \quad \square$$

Beispiel. Seien M, N und U Mengen, so dass $M \subseteq U$ und $N \subseteq U$. Dann gilt

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

Beweis.

$$(M^c \cup N)^c = (M^c)^c \cap N^c \quad \text{De Morgan}$$

$$= M \cap N^c \quad \text{Involution}$$

$$= \{x \mid (x \in M) \wedge (x \in N^c)\} = \{x \mid (x \in M) \wedge (x \notin N)\} = M \setminus N.$$

□



Hier sind einige weitere Beispiele für die Übersetzung von logischen Eigenschaften in Mengeneigenschaften.

Eigenschaft	Bezeichnung
$A \cup A^c = U$	Ausgeschlossenes Drittes
$((A \subseteq B) \wedge (B \subseteq C)) \rightarrow (A \subseteq C)$	Transitivität von \subseteq
$(A \subseteq B) \iff (B^c \subseteq A^c)$	Kontraposition
$(A \cap B) \subseteq A$	Abschwächung für \cap
$A \subseteq (A \cup B)$	Abschwächung für \cup

- Beweisen wir z.B. dass $((A \subseteq B) \wedge (B \subseteq C)) \rightarrow (A \subseteq C)$.
- Wir definieren 3 Prädikate $P(X) : x \in A$, $Q(x) : x \in B$, $R(x) : x \in C$. Dann ist die Aussage $A \subseteq B$ äquivalent der Aussage $\forall x P(x) \rightarrow Q(x)$, usw. Also wir sollen beweisen

$$\forall x ((P(x) \rightarrow Q(x)) \wedge Q(x) \rightarrow R(x))) \rightarrow (P(x) \rightarrow R(x)).$$

Diese Eigenschaft stimmt, da es ist die prädikatlogische Variante der Tautologie $((X \rightarrow Y) \wedge (Y \rightarrow Z)) \rightarrow (X \rightarrow Z)$.

□

- Der folgende Beweis zeigt die üblichste Art, wie man Eigenschaften von Mengen beweist.

Satz (Monotonie von \subseteq). Seien $M \subseteq M'$ und $N \subseteq N'$. Dann gelten

$$(M \cap N) \subseteq (M' \cap N')$$

und

$$(M \cup N) \subseteq (M' \cup N')$$

Beweis. Wir beweisen beide Inklusionen.

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 $x \in (M' \cup N')$. □



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski

Mathematisches Institut

grabowski@math.uni-leipzig.de



UNIVERSITÄT
LEIPZIG

Vorlesung 4 - Naive Mengenlehre und vollständige Induktion

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

1. Wiederholung

2. Verallgemeinerung von Vereinigung und Schnitt

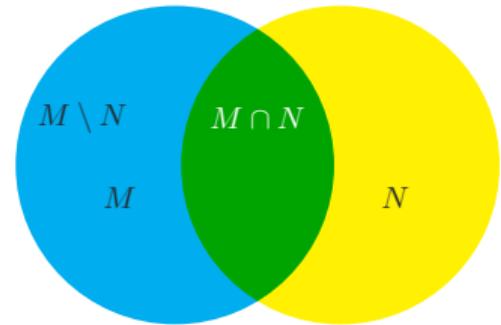
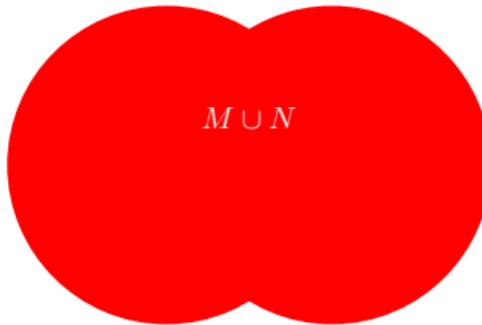
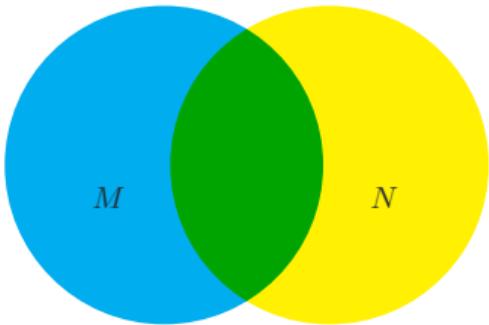
3. Kardinalität von endlichen Mengen, Potenzmenge

4. Vollständige Induktion und Induktionsbeweise

Beispiele von Mengen.

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ bezeichnen jeweils die Mengen aller natürlichen Zahlen, aller ganzen Zahlen, aller rationalen Zahlen und aller reellen Zahlen.
- Vollständige oder unvollständige Aufzählung: $\{1, 2, 3\}$ bzw. $\{0, 1, 2, \dots\}$ Das Muster muss klar erkennbar sein.
- $\{1, 2, 3\} = \{1, 2, 3, 2\} = \{2, 3, 1\}$,
- Leere Menge: \emptyset enthält keine Elemente.
- $\{\emptyset\}$ ist die Menge mit genau einem Element. Dieses Element ist die leere Menge.
- Definition mit einem Prädikat, z.B. $\{n \in \mathbb{N} \mid \text{Gerade}(n)\}$
- M ist eine Teilmenge von N , geschrieben $M \subset N$, genau dann wenn $\forall x x \in M \rightarrow x \in N$.
- Für alle Mengen M und N gilt: $M = N \iff M \subseteq N \text{ und } N \subseteq M$.

- Hauptoperationen auf Mengen.



Die Vereinigung $M \cup N$, der Schnitt $M \cap N$, die Differenz $M \setminus N$, das Komplement M^c (nur wenn wir irgendwelches Universum U fixieren)

- Wenn $M \cap N = \emptyset$ dann sagen wir dass M und N **disjunkt** sind.

Beweisen wir zum Beispiel, dass $(A \cap B)^c = A^c \cup B^c$ (De-Morgan-Gesetz).

- Zuerst nehmen wir an, dass $x \in (A \cap B)^c$, d.h. $x \notin A \cap B$. D.h. entweder $x \notin A$ oder $x \notin B$. Also $x \in A^c$ oder $x \in B^c$. Das bedeutet aber genau $x \in A^c \cup B^c$. Wir haben also bewiesen, dass $(A \cap B)^c \subset A^c \cup B^c$.
- Nehmen wir nun an, dass $x \in (A^c \cup B^c)$. Also $x \in A^c$ oder $x \in B^c$. D.h. $x \notin A$ oder $x \notin B$. Das heißt aber $x \notin A \cap B$, also $x \in (A \cap B)^c$. Wir haben jetzt bewiesen, dass $(A \cap B)^c \subset A^c \cap B^c$.
- Also $(A \cap B)^c = A^c \cup B^c$. □

Satz. Für alle Mengen M und N sind folgende Aussagen äquivalent:

- (1) $M \subset N$
- (2) $M \cap N = M$
- (3) $M \cup N = N$

Beweis.

- Wir zeigen $(1) \rightarrow (2)$, $(2) \rightarrow (3)$, und $(3) \rightarrow (1)$.
- $(1) \rightarrow (2)$: Da $M \subset N$, folgt

$$M = M \cap M \subset M \cap N.$$

Mit Abschwächung gilt $M \cap N \subset M$. Das bedeutet, dass $M \cap N = M$.

- $(2) \rightarrow (3)$: $N \subset M \cup N$ ist klar (“Abschwächung”). Sei $x \in M \cup N$. Dann $x \in N$ oder $x \in M$, also $x \in N$ oder $x \in M \cap N$. Durch Abschwächung, das impliziert, dass $x \in N$. Also $M \cup N \subset N$.

Satz. Für alle Mengen M und N sind folgende Aussagen äquivalent:

- (1) $M \subset N$
- (2) $M \cap N = M$
- (3) $M \cup N = N$

Beweis (Fortsetzung).

- (3) \rightarrow (1): Sei $x \in M$. Dann $x \in M \cup N$ und, da (3) angenommen ist, auch $x \in N$. Das zeigt, dass $M \subset N$. □

1. Wiederholung

2. Verallgemeinerung von Vereinigung und Schnitt

3. Kardinalität von endlichen Mengen, Potenzmenge

4. Vollständige Induktion und Induktionsbeweise

- Wir haben Vereinigung und Schnitt bisher zweistellig definiert.
 - ▶ Analog zum Summenzeichen \sum verallgemeinern wir die Definition auf beliebig viele Argumente.
- Sei I eine Menge und M_i eine Menge für jedes $i \in I$. Wir definieren

$$\bigcup_{i \in I} M_i := \{x \mid \text{es existiert } i \in I, \text{ so dass } x \in M_i\} = \{x \mid \exists i ((i \in I) \wedge (x \in M_i))\}$$

und

$$\bigcap_{i \in I} M_i := \{x \mid \text{für alle } i \in I \text{ gilt } x \in M_i\} = \{x \mid \forall i \in I \ x \in M_i\}$$

- Sonderfälle für $I = \emptyset$:
 - ▶ $\bigcup_{i \in \emptyset} M_i = \emptyset$
 - ▶ $\bigcap_{i \in \emptyset} M_i = U$ für Grundmenge U , sonst undefiniert.
- Erinnerung/Definition: die leere Summe wird als null definiert, z.B. $\sum_{i=5}^3 i = 0$.

Beispiele.

- Für jede Menge M gilt $M = \bigcup_{m \in M} \{m\}$.
- Das geschlossene Intervall $[u, o]$ für $u, o \in \mathbb{R}$ mit $u \leq o$ ist definiert durch

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

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

- ▶ Wir zeigen $\mathbb{R} \subseteq \bigcup_{n \in \mathbb{N}} [-n, n] \subseteq \bigcup_{r \in \mathbb{R}_{\geq 0}} [-r, r] \subseteq \mathbb{R}$. Es folgt dass alle diese Mengen gleich sind - "Ringinklusion".
- ▶ Zu $\mathbb{R} \subseteq \bigcup_{n \in \mathbb{N}} [-n, n]$: Sei $r \in \mathbb{R}$ und $n := \lceil |r| \rceil$ (aufrunden). 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 $\bigcup_{n \in \mathbb{N}} [-n, n] \subseteq \bigcup_{r \in \mathbb{R}_{\geq 0}} [-r, r]$: Klar aus dem Abschwächungsprinzip, da $\mathbb{N} \subseteq \mathbb{R}_{\geq 0}$.
- ▶ Zu $\bigcup_{r \in \mathbb{R}_{\geq 0}} [-r, r] \subseteq \mathbb{R}$: Es ist $[-r, r] \subseteq \mathbb{R}$ für alle $r \in \mathbb{R}_{\geq 0}$, also folgt aus der Monotonie.

□

- Wichtige Notationsvarianten. Für $I = \{u, u + 1, \dots, o\} \subseteq \mathbb{N}$ schreiben wir auch
 - ▶ $\bigcup_{i=u}^o M_i := \bigcup_{i \in I} M_i$
 - ▶ $\bigcap_{i=u}^o M_i := \bigcap_{i \in I} M_i$
- Liegt eine Menge von Mengen vor, so lassen wir die Laufvariable auch ganz weg:
 - ▶ $\bigcup \{M_i \mid i \in I\} := \bigcup_{i \in I} M_i$
 - ▶ $\bigcap \{M_i \mid i \in I\} := \bigcap_{i \in I} M_i$
- Beispiele
 - ▶ $\bigcup \{\{1, 3, 5\}, \{1, 2, 3\}, \{2, 3, 5\}\} = \{1, 2, 3, 5\}$
 - ▶ $\bigcap \{\{1, 3, 5\}, \{1, 2, 3\}, \{2, 3, 5\}\} = \{3\}$

- Beispiel “Distributivitat von \cap ”: $M \cap (\bigcup_{i \in I} M_i) = \bigcup_{i \in I} (M \cap M_i)$
- Beweis:

- ▶ Sei $x \in M \cap (\bigcup_{i \in I} M_i)$. Also $x \in M$ und $x \in (\bigcup_{i \in I} M_i)$. D.h. $x \in M$ und $\exists i \in I$ mit $x \in M_i$. Deswegen $\exists i \in I$ mit $x \in M \cap M_i$, also $x \in \bigcup_{i \in I} (M \cap M_i)$.
- ▶ Sei $x \in \bigcup_{i \in I} (M \cap M_i)$. Also $\exists i \in I$ mit $x \in M \cap M_i$. Deswegen $x \in M$ und $\exists i \in I$ mit $x \in M_i$. D.h. $x \in M$ und $x \in (\bigcup_{i \in I} M_i)$, und es folgt
 $x \in M \cap (\bigcup_{i \in I} M_i)$.

□

1. Wiederholung
2. Verallgemeinerung von Vereinigung und Schnitt
3. Kardinalität von endlichen Mengen, Potenzmenge
4. Vollständige Induktion und Induktionsbeweise

- Jede Menge kann entweder **endlich** oder **unendlich** sein.
- Für endliche Mengen M bezeichnen wir mit $|M|$ die Anzahl ihrer Elemente, auch **Kardinalität** genannt.
- Ist M unendlich, so schreiben wir auch $|M| \geq \infty$.
- Für alle endlichen Mengen M und N gilt

$$|M \cup N| \leq |M| + |N|.$$

- Wenn M und N disjunkt sind, also $M \cap N = \emptyset$, so haben wir die Gleichheit

$$|M \cup N| = |M| + |N|.$$

- Beispiele.
 - Die Mengen $\{1, 2, 3\}$ und $\{2, 4, 6\}$ sind nicht disjunkt und es gilt
$$|\{1, 2, 3\} \cup \{2, 4, 6\}| = 5 < 6 = 3 + 3 = |\{1, 2, 3\}| + |\{2, 4, 6\}|.$$
 - Die Mengen $\{1, 2, 3\}$ und $\{4, 5, 6\}$ sind disjunkt und es gilt
$$|\{1, 2, 3\} \cup \{4, 5, 6\}| = 6 = 3 + 3 = |\{1, 2, 3\}| + |\{4, 5, 6\}|.$$

Für eine Menge M ist die **Potenzmenge** $\mathcal{P}(M)$ die Menge aller Teilmengen von M :

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

- $\mathcal{P}(\emptyset) = \{\emptyset\}$,
- $\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.
- $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

- Wie viele Elemente enthält die Potenzmenge einer endlichen Menge M ? (d.h. was ist die Kardinalität von $\mathcal{P}(M)$?)
- Durch systematisches Probieren gelangt man zu der Hypothese

$$|\mathcal{P}(M)| = 2^{|M|}.$$

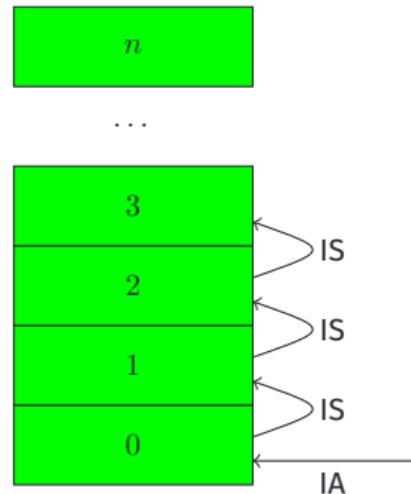
- Der Grund dafür ist, dass die Definition einer Teilmenge S von M gleichbedeutend damit ist, für jedes $x \in M$ zu entscheiden, ob es in S enthalten ist oder nicht.
Da es $2^{|M|}$ solche Auswahlmöglichkeiten gibt, ist dies auch die Anzahl der Teilmengen von M .
- Um solche Argumente präzis schreiben zu können, benötigen wir eine neue Beweistechnik “Induktion”.

1. Wiederholung
2. Verallgemeinerung von Vereinigung und Schnitt
3. Kardinalität von endlichen Mengen, Potenzmenge
4. Vollständige Induktion und Induktionsbeweise

- Wir betrachten die folgende Aussage. Für alle $n \in \mathbb{N}$ gilt $\sum_{i=0}^n i = \frac{n(n+1)}{2}$.
- Obwohl der Beweis dieser Aussage für eine konkrete Zahl n unproblematisch ist, stellt der Beweis für alle $n \in \mathbb{N}$ eine Hürde dar, da wir nicht unendlich viele Beweise angeben können.
- Das folgende Prinzip ist ein Beweisprinzip das wir hier nützen können.

Prinzip der vollständigen Induktion Sei $F(x)$ eine Prädikat mit einer Variable x . Gelten die Aussagen

- $F(0)$ und
- $F(n) \rightarrow F(n + 1)$ für alle $n \in \mathbb{N}$,
dann gilt $F(x)$ für alle $x \in \mathbb{N}$.



- Ein Induktionsbeweis funktioniert wie folgt.
 - ▶ Zunächst zeigen wir die Behauptung für den Fall $n = 0$ (**Induktionsanfang**).
 - ▶ Anschließend folgt Induktionsschritt: wir wählen eine beliebige natürliche Zahl n und setzen voraus, dass die Behauptung für n bereits gezeigt ist (**Induktionshypothese**).
Dann beweisen wir die **Induktionsbehauptung**: die Behauptung für den Nachfolger $n + 1$. Im Beweis können wir die Induktionshypothese nutzen.

Als Beispiel zeigen wir dass für alle $n \in \mathbb{N}$ gilt $\sum_{i=0}^n i = \frac{n(n+1)}{2}$.

Beweis.

- **Induktionsanfang:** Es gilt $\sum_{i=0}^0 i = 0 = \frac{0 \cdot 1}{2}$.
- **Induktionshypothese:** Sei $n \in \mathbb{N}$, nehmen wir an dass $\sum_{i=1}^n i = \frac{n(n+1)}{2}$ wahr ist.
- **Induktionsbehauptung:** Zu zeigen ist, dass $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$.
- Beweis der IB: Es gilt

$$\begin{aligned}\sum_{i=0}^{n+1} i &= \sum_{i=0}^n i + (n+1) \stackrel{\text{IH}}{=} \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}\end{aligned}$$

Nach dem Prinzip der vollständigen Induktion folgt die Behauptung. □

Beispiel. Wenn M ist eine endliche Menge, dann gilt $|\mathcal{P}(M)| = 2^{|M|}$.

Beweis. Vollständige Induktion über $n = |M|$.

$$\forall n \left(\forall M (|M| = n \rightarrow |\mathcal{P}(M)| = 2^n) \right)$$

- Induktionsanfang. Sei Menge M beliebig, mit $|M| = 0$. Die einzige solche Menge ist $M = \emptyset$. Zusätzlich $\mathcal{P}(\emptyset) = \{\emptyset\}$, also gilt $|\mathcal{P}(\emptyset)| = |\{\emptyset\}| = 1 = 2^0 = 2^{|\emptyset|}$.
- Induktionshypothese. Sei $n \in \mathbb{N}$ und wir nehmen an dass $|\mathcal{P}(N)| = 2^n$ für alle Mengen N mit $|N| = n$.

- Induktionsbehauptung. Sei M eine Menge mit $|M| = n + 1$. Zu zeigen ist dass $|\mathcal{P}(M)| = 2^{n+1}$.
 - ▶ Wähle $x \in M$ beliebig und sei $N = M \setminus \{x\}$.
 - ▶ Wir unterteilen alle Teilmengen von M in
 - (a) diejenigen, die x nicht enthalten, und somit Teilmengen von N sind, und
 - (b) diejenigen, die x enthalten und somit von der Form $S \cup \{x\}$ sind, wobei S eine Teilmenge von N ist.
 - ▶ Wenn beispielsweise $M = \{1, 2, 3\}$ und $x = 3$, dann ist $N = \{1, 2\}$, und
 - (a) die Teilmengen, die x nicht enthalten, sind $\emptyset, \{1\}, \{2\}, \{1, 2\}$
 - (b) die Teilemengen, die x enthalten, sind $\{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}$.

- Im Allgemeinen könnten wir schreiben

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

- Unter Beachtung der Disjunktheit gilt

$$|\mathcal{P}(M)| = |\mathcal{P}(N)| + |\mathcal{P}(N)| = 2 \cdot |\mathcal{P}(N)| \stackrel{\text{IH}}{=} 2 \cdot 2^n = 2^{n+1} = 2^{|M|},$$

wobei $|\mathcal{P}(N)| = 2^n$. Nach dem Prinzip der vollständigen Induktion folgt die Behauptung. □

Der Beginn der Induktion muss nicht bei $n = 0$ liegen. Beispiel: für alle $n \in \mathbb{N}$ mit $n > 2$ gilt $n^2 > n + 5$.

Beweis.

- Induktionsanfang. Für $n = 3$ haben wir $n^2 = 9 > 8 = n + 5$.
- Induktionshypothese. Sei $n > 2$ beliebig. Dann $n^2 > n + 5$.
- Induktionsbehauptung. Zu zeigen ist $(n + 1)^2 > (n + 1) + 5$
 - Wir haben $(n + 1)^2 = n^2 + 2n + 1 \stackrel{\text{IH}}{>} n + 5 + 2n + 1 > (n + 1) + 5$. Nach dem Prinzip der vollständigen Induktion folgt die Behauptung. □

- Beispiel: Für alle $n \in \mathbb{N}, n \geq 4$ gilt: $n! > 2^n$.
- Lösung:

- ▶ Induktionsanfang: Sei $n = 4$, dann gilt $4! = 24 > 16 = 2^4$
- ▶ Induktionshypothese: Sei $n \in \mathbb{N}, n \geq 4$ mit $n! > 2^n$.
- ▶ Induktionsbehauptung: Zu zeigen ist, dass $(n + 1)! > 2^{n+1}$.

$$(n + 1)! = n! \cdot (n + 1) \stackrel{IH}{>} 2^n \cdot (n + 1)$$

Da $n \geq 4$, gilt $n + 1 \geq 2$, und damit

$$2^n \cdot (n + 1) > 2^n \cdot 2 = 2^{n+1}.$$

Es gilt also $(n + 1)! > 2^{n+1}$ und damit die obige Behauptung gilt für alle $n \in \mathbb{N}$.



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski

Mathematisches Institut

grabowski@math.uni-leipzig.de



UNIVERSITÄT
LEIPZIG

Vorlesung 5 - Relationen

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

1. Wiederholung

2. Was jetzt? Alles aus Mengen bauen.

3. Relationen - Definitionen und erste Beispiele

4. Eigenschaften von Relationen

5. Operationen auf Relationen

6. Äquivalenzrelationen

Mengenlehre

- Für eine Menge M ist die **Potenzmenge** $\mathcal{P}(M)$ die Menge aller Teilmengen von M
- Jede Menge kann entweder **endlich** oder **unendlich** sein. Für endliche Mengen M bezeichnen wir mit $|M|$ die Anzahl ihrer Elemente, auch **Kardinalität** genannt.
-

$$|\mathcal{P}(M)| = 2^{|M|}.$$

Vollständige Induktion und Induktionsbeweise

- Zunächst zeigen wir die Behauptung für den Fall $n = 0$ (Induktionsanfang).
- Anschließend wählen wir eine beliebige natürliche Zahl n und setzen voraus, dass die Behauptung für n bereits gezeigt ist (Induktionshypothese).
- Dann zeigen wir die Induktionsbehauptung - die Behauptung für den Fall $n + 1$ unter Rückgriff auf die Induktionshypothese.

- Beispiel: Jede natürliche Zahl $n > 1$ hat eine Primzahlzerlegung

Beweis. Wir verwenden die Induktion über die natürlichen Zahlen n , beginnend mit 2

- Induktionsanfang: Die Behauptung ist wahr, wenn $n = 2$, da 2 eine Primzahl ist.
- Induktionshypothese: jede natürliche Zahl m mit $2 \leq m \leq n$ hat eine Primzahlzerlegung.
- Induktionsbehauptung: Wir müssen zeigen, dass $n + 1$ eine Primzahlzerlegung hat.
- Beweis der Induktionsbehauptung:
 - ▶ Wenn $n + 1$ eine Primzahl ist, dann hat insbesondere $n + 1$ eine Primzahlzerlegung.
 - ▶ Wenn nicht, dann können wir $n + 1 = ab$ schreiben, mit $a, b \leq n$.
 - ▶ Nach der Induktionshypothese, haben a und b eine Primzahlzerlegung, d.h. $a = p_1, \dots, p_l$, $b = q_1, \dots, q_k$ für einige Primzahlen $p_1, \dots, p_l, q_1, \dots, q_k$.
 - ▶ Dann ist $n + 1 = p_1 \dots p_l q_1 \dots q_k$, was bedeutet, dass $n + 1$ eine Primzahlzerlegung hat.

1. Wiederholung
2. Was jetzt? Alles aus Mengen bauen.
3. Relationen - Definitionen und erste Beispiele
4. Eigenschaften von Relationen
5. Operationen auf Relationen
6. Äquivalenzrelationen

- Wir haben unsere grundlegende Einführung in die Mengenlehre abgeschlossen.
- Alle mathematischen Strukturen können mit Hilfe von Mengen definiert werden. Doch wenn wir über Strukturen wie Zahlen, Graphen usw. nachdenken, gehen wir fast nie bis zu den Mengen zurück.
- Dies ist sehr analog zu der Situation mit modernen Computern: Einerseits stimmt es, dass jeder Computer in seinem Kern 0/1-Variablen mit den Grundoperationen \wedge , \vee und \neg manipuliert. Wir brauchen uns damit aber nicht zu befassen wenn wir ein Dokument bearbeiten, im Internet surfen oder Musik auf dem Computer hören.
- Neue Struktur: **geordnetes Paar**. Gegeben sind zwei Objekte A und B , Wir können das geordnete Paar (A, B) .

Unterschiede von (A, B) im Vergleich zur Menge $\{A, B\}$.

- Wenn $A \neq B$, dann spielt die Reihenfolge eine Rolle, d.h. $(A, B) \neq (B, A)$,
- Wenn $A = B$, dann $\{A, B\} = \{A\}$, Nichts ähnliches gescheht für das geordnete Paar.
Z.B. Wir können die geordnete Paare $(2, 2)$, $(3, 3)$, (\mathbb{R}, \mathbb{R}) , usw. betrachten.

- Mit Mengen als Bausteinen: “Kuratowskis geordnetes Paar”: Bei gegebenen Objekten A und B definieren wir $(A, B) := \{\{A\}, \{A, B\}\}$.
- Schlüsseleigenschaft: $(A, B) = (C, D)$, genau dann, wenn $A = C$ und $B = D$.
- Es gibt auch andere mögliche mengentheoretische Definitionen. Manchmal betrachtet man das geordnete Paar als ein Grundbegriff, ähnlich wie die Mengen.
- Aber das ist uns nicht wichtig. Die Analogie zur Informatik ist: Wenn wir im Internet surfen, ist es uns ziemlich egal, welchen Webbrowsert wir benutzen und wie genau sein Quellcode aussieht, solange er uns den Zugriff auf die für uns wichtigen Webdienste ermöglicht.

- **Kartesisches Produkt** Seien M und N zwei Mengen. Dann

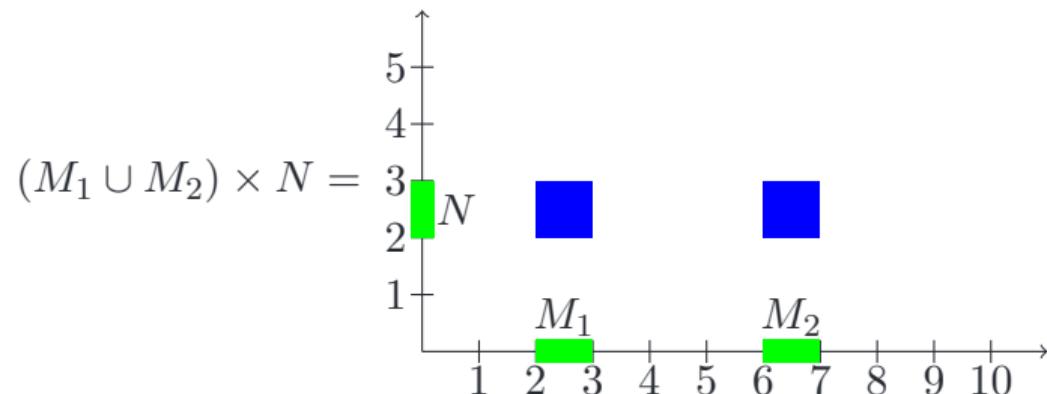
$$M \times N := \{(m, n) \mid m \in M, n \in N\} .$$

- $M \times N$ ist die Menge aller geordneten Paare von einem Element m aus M gefolgt von einem Element n aus N .
- Wir betonen dass wenn $M \neq N$ dann auch $M \times N \neq N \times M$.

- Beispiel: $M = \{1, 2, 3\}$, $N = \{1, 3\}$

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

- Beispiel: $M_1 = [2, 3]$, $M_2 = [6, 7]$, $N = [2, 3]$.



1. Wiederholung
2. Was jetzt? Alles aus Mengen bauen.
- 3. Relationen - Definitionen und erste Beispiele**
4. Eigenschaften von Relationen
5. Operationen auf Relationen
6. Äquivalenzrelationen

- Seien M und N zwei Mengen (möglicherweise mit $M = N$). 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 .
- Statt $(m, n) \in R$ schreiben wir auch $m R n$ oder $R(m, n)$ oder $m \sim_R n$. Analog $m \not R n$ oder $m \not\sim_R n$ wenn $(m, m) \notin R$.
- Relationszeichen bindet stärker als die logischen Junktoren:

$$(x \sim y \wedge y \sim x) \rightarrow x = y \quad \text{heißt} \quad ((x \sim y) \wedge (y \sim x)) \rightarrow (x = y).$$

- Relationen sind sehr nützlich, um andere mathematische Strukturen zu definieren, und um die Strukturen der realen Welt zu modellieren.

- Die leere Relation $\emptyset \subseteq M \times N$ und $M \times N$ selbst sind Relationen von M nach N .
- Sei B die Menge der Bundesbürger. Die Menge

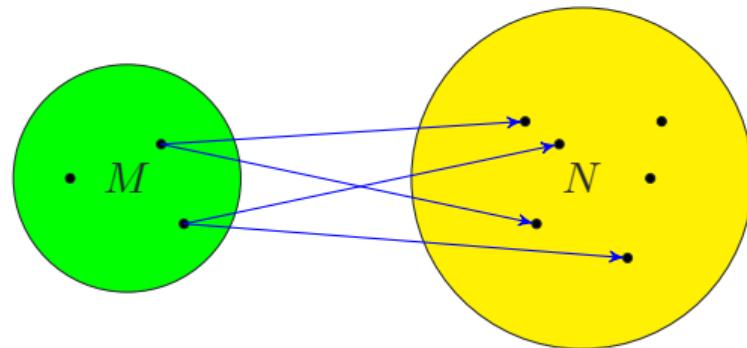
$$\{(p, n) \in B \times \mathbb{N} \mid p \text{ hat Identifikationsnummer } n\}$$

ist eine Relation von B nach \mathbb{N} .

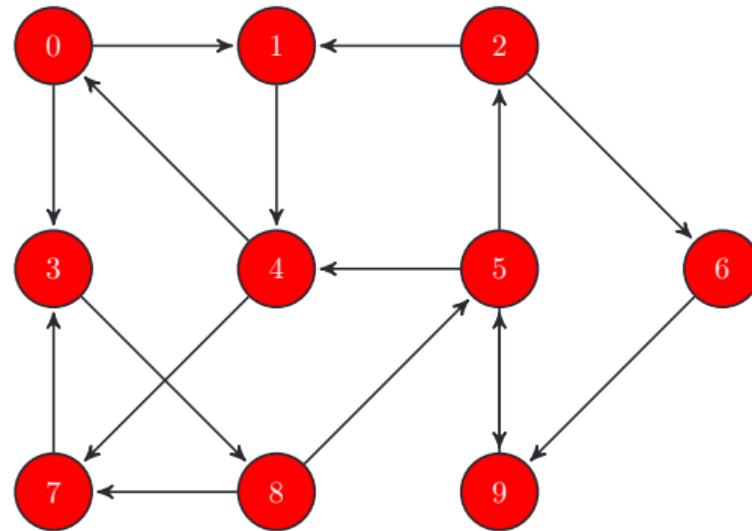
- Die Menge $\{(n, n') \in \mathbb{N} \times \mathbb{N} \mid n \leq n'\}$ ist eine Relation auf \mathbb{N} .
- Die Teilmengerelation \subseteq ist eine Relation auf $\mathcal{P}(M)$.

- Die Freund-Relation auf der Menge F der Facebook-Nutzer
$$\{(x, y) \in F \times F \mid x \text{ ist Facebook-Freund von } y\}$$
ist eine Relation.
- Für jede Menge M ist die **Identität** $\text{id}_M = \{(m, m) \mid m \in M\}$ eine Relation auf M .Gewöhnlich schreibt man $x = y$ statt $x \sim_{\text{id}_M} y$.

Relation von M nach N



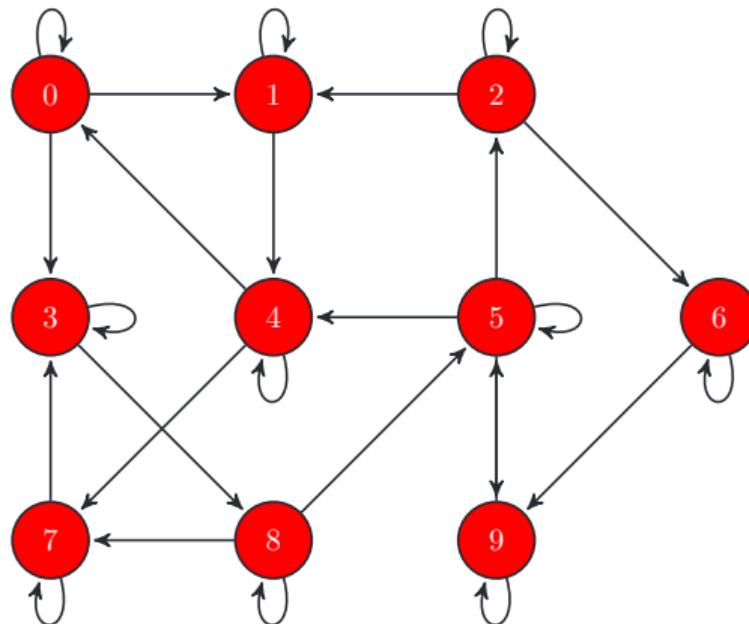
Relation auf $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$



1. Wiederholung
2. Was jetzt? Alles aus Mengen bauen.
3. Relationen - Definitionen und erste Beispiele
4. Eigenschaften von Relationen
5. Operationen auf Relationen
6. Äquivalenzrelationen

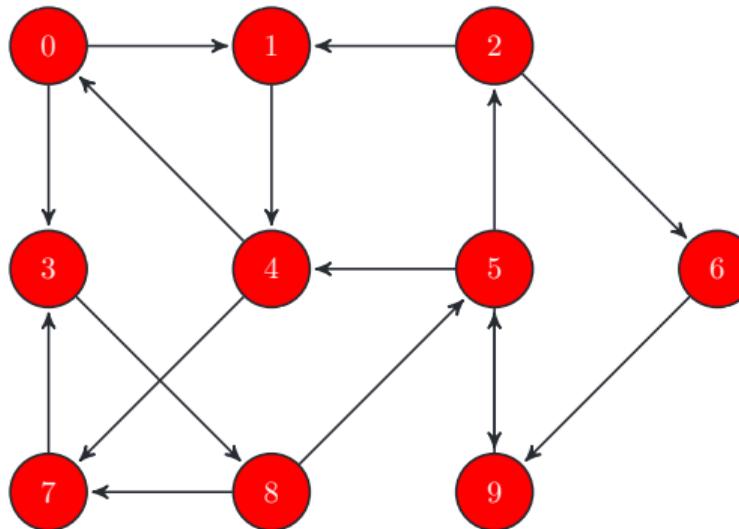
Sei $R \subseteq M \times M$ ein Relation auf M . R heißt

- **reflexiv**, falls jedes Element x von M steht in Relation zu sich selbst.
 $\forall x(x \in M \rightarrow (x, x) \in R)$,



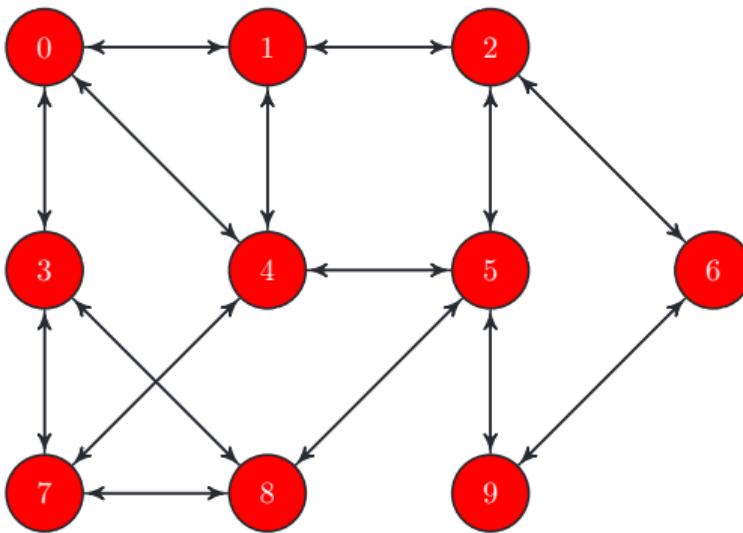
- Reflexivität: Alle Elemente haben Schleifen. z. B. $=$ ist reflexiv, $<$ ist nicht reflexiv, \subseteq ist reflexiv,

- **irreflexiv**, falls kein Element x von M steht in Relation zu sich selbst.
 $\forall x(x \in M \rightarrow (x, x) \notin R)$,



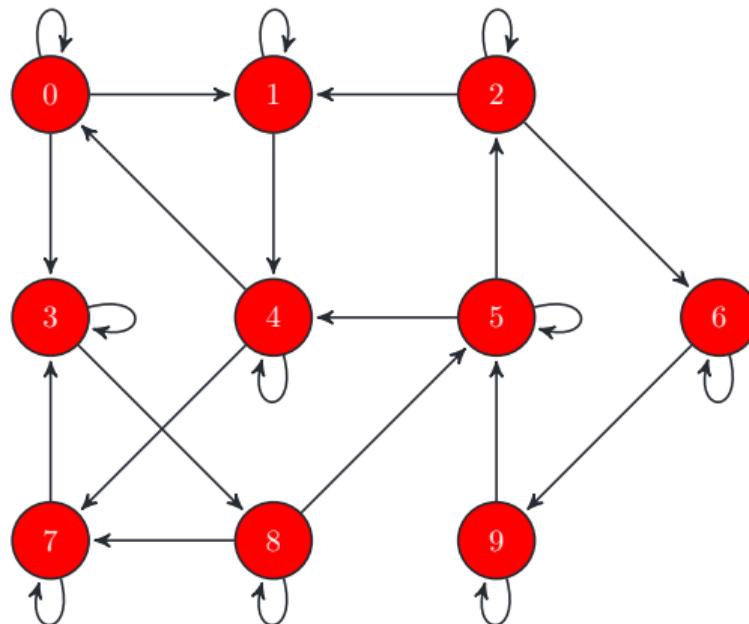
- Irreflexivitat: Kein Element hat Schleifen.
- z.B. $<$ is irreflexiv

- **symmetrisch**, falls wenn x in Relation zu y steht, dann steht auch y in Relation zu x .
 $\forall x, y ((x, y) \in R \rightarrow (y, x) \in R),$



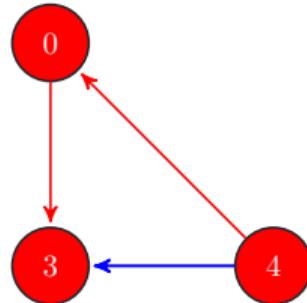
- Symmetrie: Jeder Pfeil ist beidseitig. Z.B. = is symmetrisch, Facebook-freundschaft ist symmetrisch.

- **antisymmetrisch**, falls wenn $x \sim y$ und $y \sim x$ dann $x = y$.
 $\forall x, y ((x, y) \in R \wedge (y, x) \in R) \rightarrow x = y$,



- Antisymmetrie: Kein Pfeil ist beidseitig, mit Ausnahme von Schleifen. Z.B. $<$, \leq und \subseteq sind antisymmetrisch.

- **transitiv**, falls $x \sim y$ und $y \sim z$ impliziert $x \sim z$.
 $\forall x, y, z ((x, y) \in R \wedge (y, z) \in R) \rightarrow (x, z) \in R$.



- Transitivität: “Für jeden Weg existiert auch der direkte Weg.” Z.B. $<$ und \leq sind transitiv.

- **vollständig**, falls für alle verschiedene Elemente $x, y \in M$ steht x in Relation zu y oder y in Relation zu x $\forall x, y \in M (x, y) \in R \vee (y, x) \in R$
- Z.B. \leq ist vollständig, $<$ ist nicht vollständig.

1. Wiederholung
2. Was jetzt? Alles aus Mengen bauen.
3. Relationen - Definitionen und erste Beispiele
4. Eigenschaften von Relationen
5. Operationen auf Relationen
6. Äquivalenzrelationen

- Sei $R \subseteq M \times N$ eine Relation. Die **inverse Relation** R^{-1} von R :

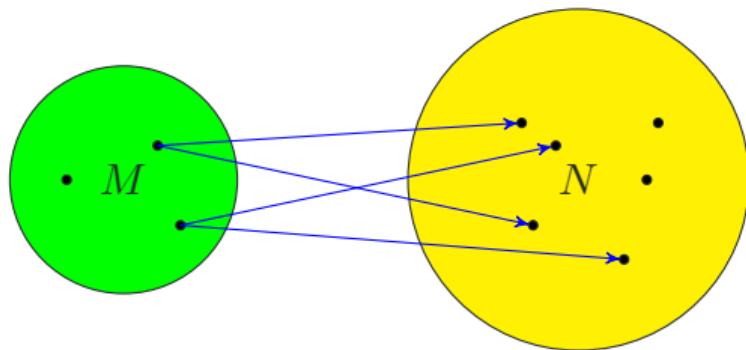
$$R^{-1} := \{(n, m) \in N \times M \mid (m, n) \in R\}.$$

- Die Inversion bewirkt also einen Tausch der Komponenten bzw. eine Umkehr der Pfeile.
- Beispiel: Sei $R := \{(1, 1), (1, 3), (2, 2), (2, 4), (3, 2)\}$. Dann ist

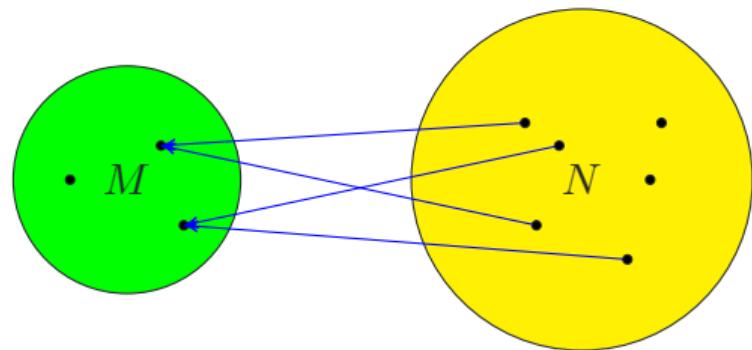
$$R^{-1} = \{(1, 1), (3, 1), (2, 2), (4, 2), (2, 3)\}.$$

- Beispiel: Die inverse Relation von $<$ ist $>$.

R - Relation von M nach N



R^{-1} - Relation von N nach M



- Seien $R \subseteq M \times N$ und $R' \subseteq N \times P$ Relationen.
- Die **Komposition** von R gefolgt von R' , geschrieben als $R ; R'$:

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

- Beispiel. Seien

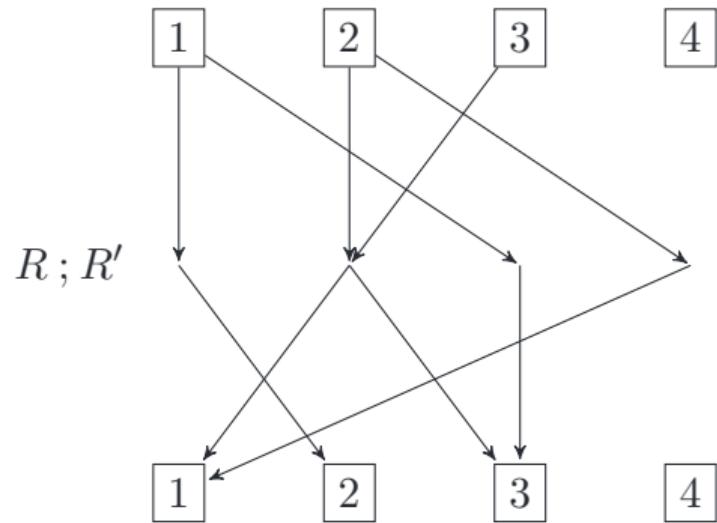
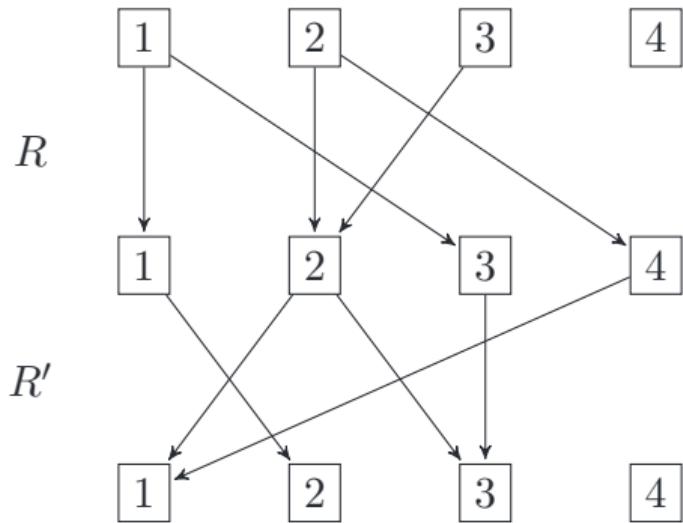
$$R := \{(1, 1), (1, 3), (2, 2), (2, 4), (3, 2)\}$$

und

$$R' := \{(1, 2), (2, 1), (2, 3), (3, 3), (4, 1)\}.$$

Dann ist

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



1. Wiederholung
2. Was jetzt? Alles aus Mengen bauen.
3. Relationen - Definitionen und erste Beispiele
4. Eigenschaften von Relationen
5. Operationen auf Relationen
6. Äquivalenzrelationen

- Motivation: Häufig haben wir eine Menge von Objekten, zum Beispiel verschiedene Farbprodukte. Wir interessieren uns aber nur für eine bestimmte Eigenschaft, z. B. die Farbe.
 - ▶ In diesem Fall könnten wir sagen, dass zwei Farbprodukte “gleich” sind, wenn sie die gleiche Farbe haben.
 - ▶ In einem Geschäft könnte es 50 verschiedene Farbprodukte geben, aber wenn es nur zwei Farben gibt, rot und blau, dann könnten wir sagen, dass das Geschäft nur rote und blaue Farbprodukte verkauft.
- Wir könnten uns nur für die Parität einer gegebenen natürlichen Zahl interessieren. In diesem Fall gibt es natürliche Zahlen nur in zwei Arten: gerade und ungerade.
- Wir könnten uns nur für die Anzahl der verschiedenen Primteiler einer natürlichen Zahl interessieren. Dann wären 30 und 105 voneinander ununterscheidbar.

- Es gibt zwei gleichwertige mathematische Möglichkeiten zu sagen, dass wir bestimmte Objekte als “gleich” betrachten. Wir beginnen mit den Äquivalenzrelationen.
- Sei M eine Menge und sei \sim eine Relation auf M . Wir sagen, dass M eine **Äquivalenzrelation** ist, wenn M hat die folgenden Eigenschaften:
 - ▶ reflexiv (Jedes Objekt a ist ununterscheidbar von a selbst),
 - ▶ symmetrisch (Wenn a ununterscheidbar von b ist, dann ist auch b ununterscheidbar von a), und
 - ▶ transitiv (Wenn a ununterscheidbar von b und b ununterscheidbar von c ist, dann ist auch a ununterscheidbar von c .

- Oft benutzen wir das Zeichen \equiv für Äquivalenzrelationen.
- Für $m \in M$ beliebig ist

$$[m]_{\equiv} := \{x \in M : m \equiv x\}$$

- $[m]_{\equiv}$ heißt die **Äquivalenzklasse** von m , (oder die \equiv -Äquivalenzklasse von m).
- Wir sagen auch dass m ein Vertreter oder Repräsentant von der Klasse $[m]_{\equiv}$ ist. Sofern \equiv sich aus dem Kontext ergibt, schreiben wir einfach $[m]$ statt $[m]_{\equiv}$.
- Beispiel: Identität ist eine Äquivalenzrelation.
- Keine Äquivalenzrelationen: $<$ auf \mathbb{N} , \subseteq auf $\mathcal{P}(M)$ mit $M \neq \emptyset$.

- Beispiel: die Relation $R_2 := \{(n, n') \in \mathbb{N} \times \mathbb{N}: 2 \mid n - n'\}$ ist eine Äquivalenzrelation.

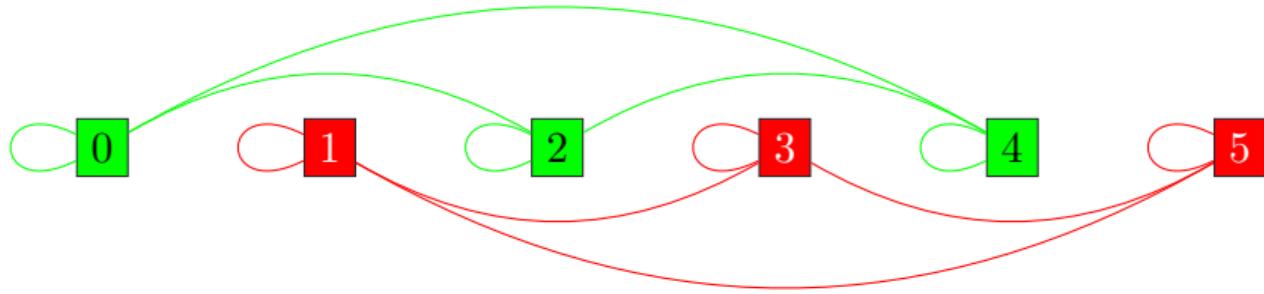
Beweis.

- **Reflexivität:** Für alle $x \in \mathbb{N}$ $2 \mid x - x = 0$, also $(x, x) \in R_2$.
- **Symmetrie:** Seien $x, y \in \mathbb{N}$ mit $(x, y) \in R_2$. Also $2 \mid x - y$. Dann auch $2 \mid y - x$, womit auch $(y, x) \in R_2$.
- **Transitivität:** Seien $x, y, z \in \mathbb{N}$, so dass $(x, y) \in R_2$ und $(y, z) \in R_2$. Daher $2 \mid x - y$, und $2 \mid y - z$. Dann $2 \mid (x - y) + (y - z) = x - z$. D.h. $2 \mid x - z$, womit auch $(x, z) \in R_2$. \square
- Äquivalenzklassen von R_2 :

$$[0]_{R_2} = \{0, 2, 4, 6, \dots\}$$

$$[1]_{R_2} = \{1, 3, 5, 7, \dots\}$$

$$[2]_{R_2} = \{0, 2, 4, 6, \dots\}$$



- Die Relation R_2 teilt die Zahlen in gerade und ungerade.

Theorem

Für jede Äquivalenzrelation \equiv auf einer Menge M und Elemente $x, y \in M$ gilt

$$x \equiv y \iff [x] = [y].$$

Beweis.

- (\rightarrow) Sei $x \equiv y$. Zu zeigen ist $[x] = [y]$. Wir zeigen zwei Teilmengenbeziehungen.
 - (\subseteq) Sei $z \in [x]$. Dann gilt $x \equiv z$. Mit Symmetrie folgt aus $x \equiv y$ auch $y \equiv x$ und mit Transitivität gilt damit $y \equiv z$. Folglich $z \in [y]$.
 - (\supseteq) Sei $z \in [y]$. Dann gilt $y \equiv z$. Mit Transitivität gilt $x \equiv z$. Folglich $z \in [x]$.
- (\leftarrow) Sei $[x] = [y]$. Gemäß Reflexivität gilt $y \in [y] = [x]$, also $x \equiv y$. □

- Sei \equiv eine Äquivalenzrelation auf M . Wir definieren

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

- Also M/\equiv ist die Menge aller Äquivalenzklassen von \equiv .
- M/\equiv wird auch **Quotient** von M durch \equiv genannt.
- Beispiel: $(\mathbb{N}/=) = \{\{0\}, \{1\}, \{2\}, \dots\}$
- Beispiel: $(\mathbb{N}/R_2) = \{\{0, 2, 4, 6, \dots\}, \{1, 3, 5, 7, \dots\}\}$



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski

Mathematisches Institut

grabowski@math.uni-leipzig.de



UNIVERSITÄT
LEIPZIG

Vorlesung 6 - Relationen und Funktionen

Diskrete Strukturen (WS 2023-24)

Łukasz Grabowski

Mathematisches Institut

1. Wiederholung

2. Äquivalenzrelationen und Zerlegungen

3. Funktionen - Definition

4. Injektivität, Surjektivität, Bijektivität

5. Komposition von Funktionen

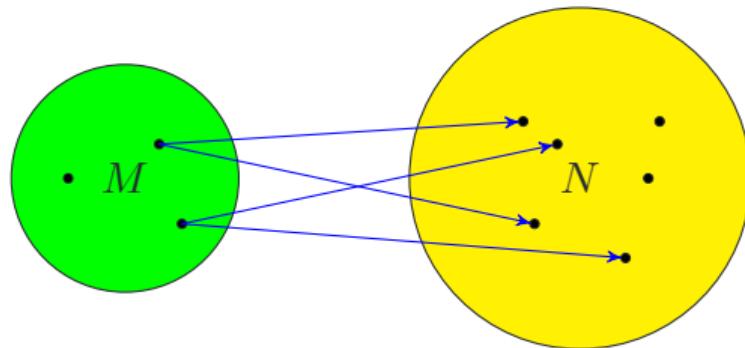
6. Invertierung von Funktionen

- Seien M und N zwei Mengen (möglicherweise mit $M = N$). 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 .
- Statt $(m, n) \in R$ schreiben wir auch $m R n$ oder $R(m, n)$ oder $m \sim_R n$. Analog $m \not R n$.
- Beispiel: die Menge $\{(n, n') \in \mathbb{N} \times \mathbb{N} \mid n \leq n'\}$ ist eine Relation auf \mathbb{N} .
- Beispiel: die Freund-Relation auf der Menge F der Facebook-Nutzer

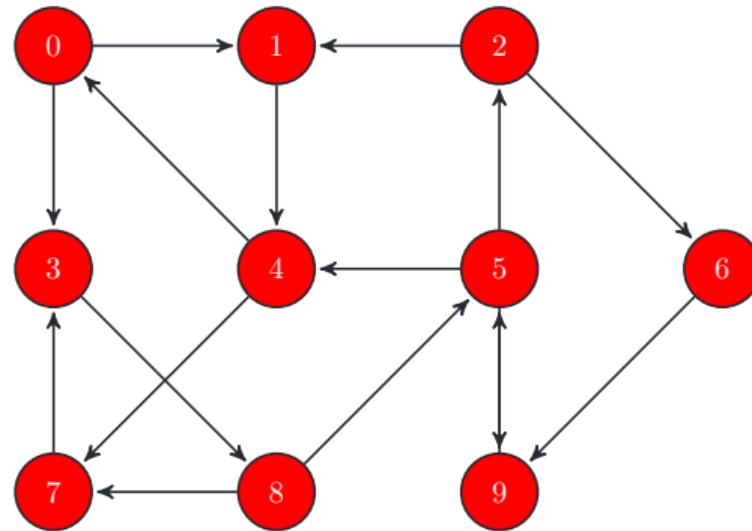
$$\{(x, y) \in F \times F \mid x \text{ ist Facebook-Freund von } y\}$$

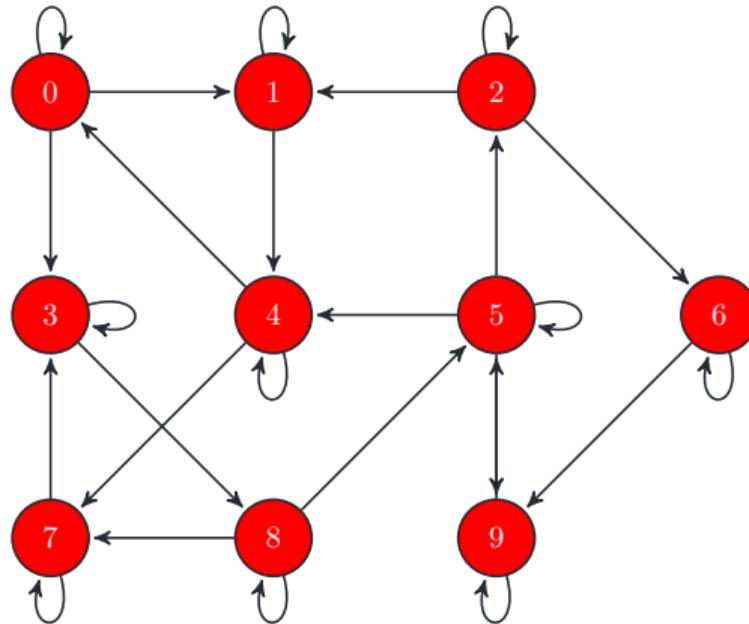
ist eine Relation.

Relation von M nach N

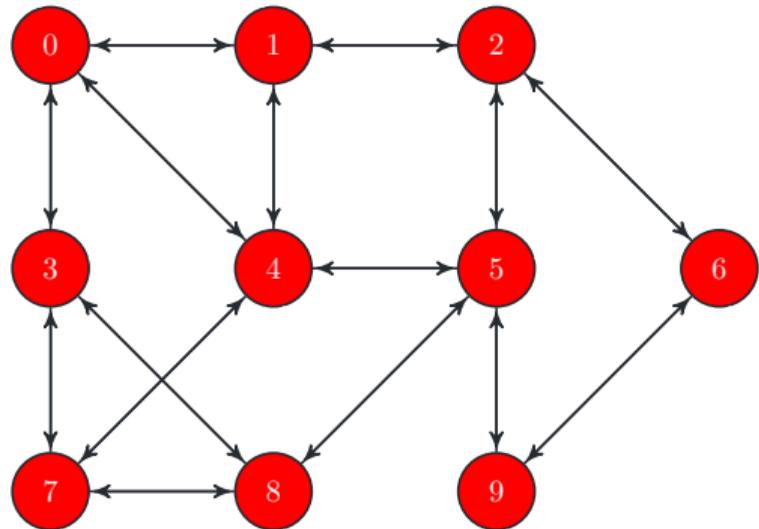


Relation auf $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

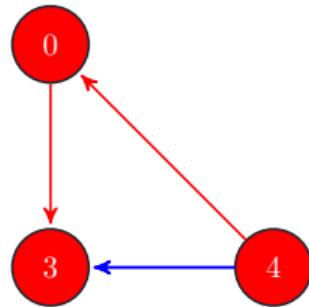




Reflexivität: Alle Elemente haben Schleifen.

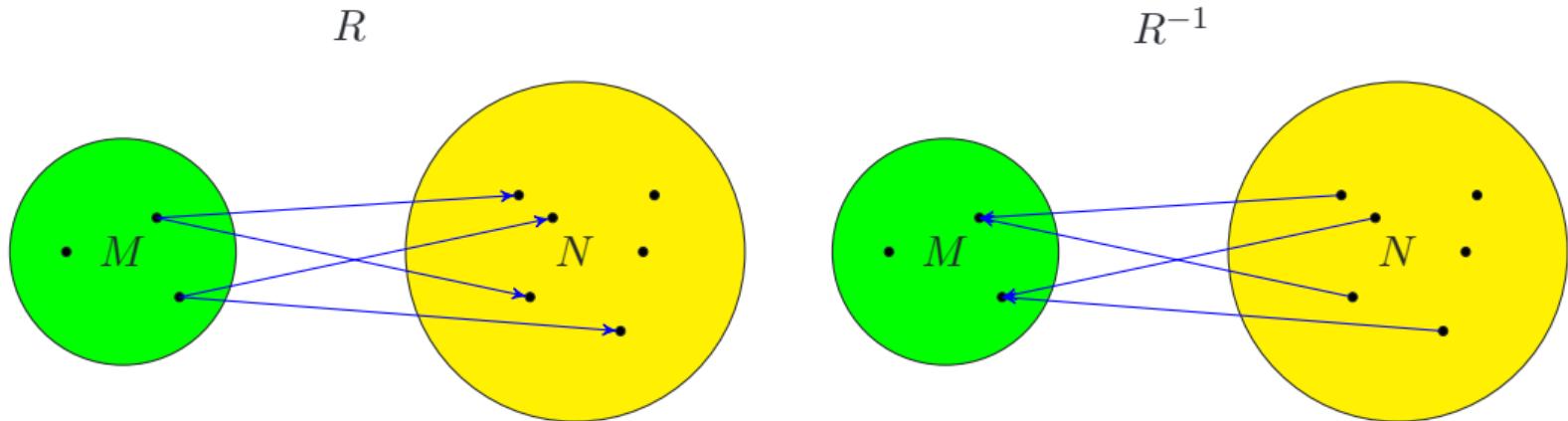


Symmetrie: Jeder Pfeil ist beidseitig.

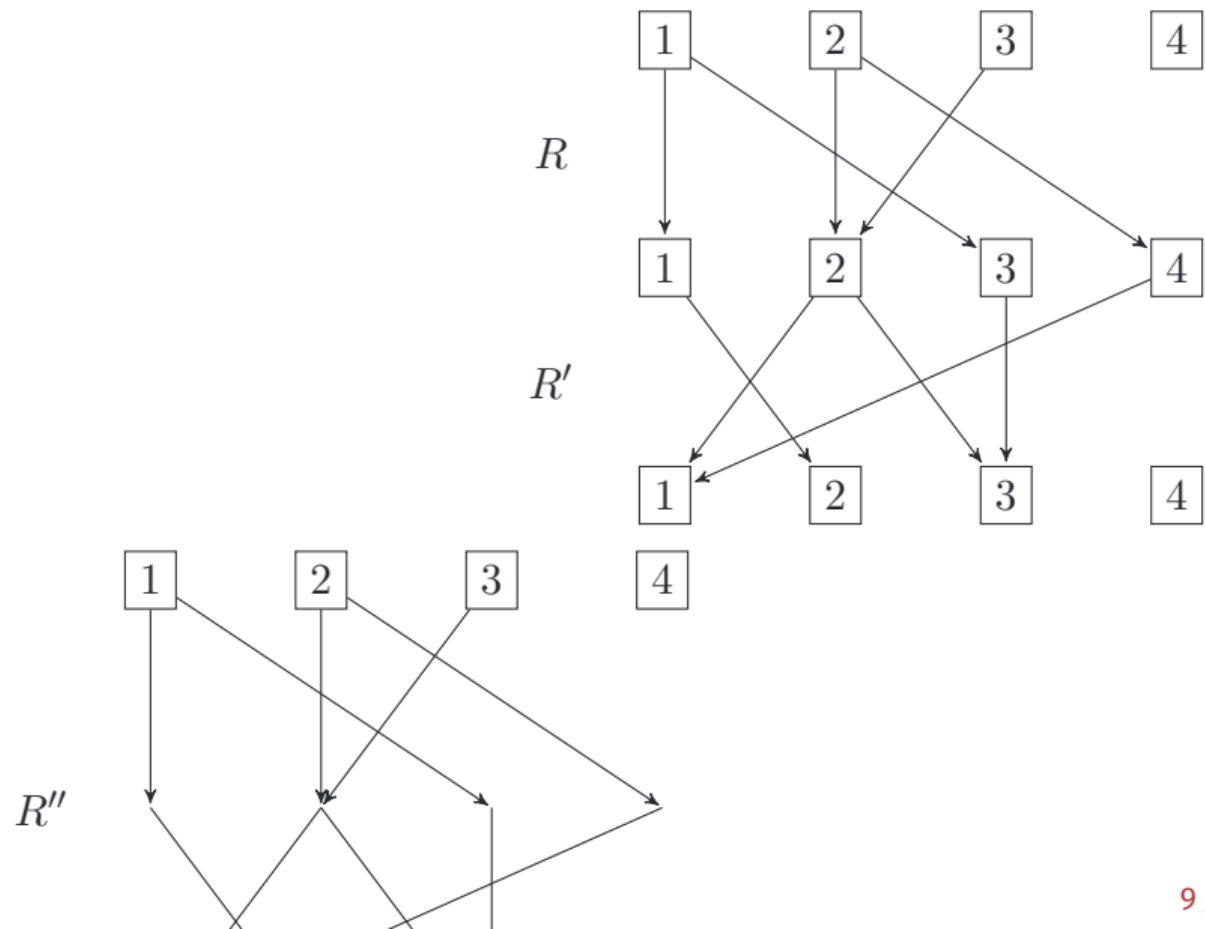


Transitivität: Für jeden Weg existiert auch der direkte Weg.

Operation: Inversion R^{-1} von einer Relation R .



Operation: Komposition von R gefolgt von R' , wobei $R \subseteq M \times N$ und $R' \subseteq N \times P$.



1. Wiederholung
2. Äquivalenzrelationen und Zerlegungen
3. Funktionen - Definition
4. Injektivität, Surjektivität, Bijektivität
5. Komposition von Funktionen
6. Invertierung von Funktionen

- Eine Relation \equiv auf M ist eine **Äquivalenzrelation**, falls sie reflexiv, symmetrisch und transitiv ist.
- Für $m \in M$, die **Äquivalenzklasse** von m ist die Menge:

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

- Wir definieren

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

“**Quotient** von M durch \equiv ”.

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

- In der letzter Vorlesung haben wir den folgenden Satz bewiesen.

Theorem

Sei M eine nicht leere Menge und sei \equiv eine Äquivalenzrelation auf M . Dann ist (M/\equiv) eine Zerlegung von M .

- Jetzt werden wir sehen, dass für jede Zerlegung kann man eine Äquivalenzrelation definieren, deren Äquivalenzklassen geben uns die ursprüngliche Zerlegung.

Theorem

Sei M eine nicht leere Menge, und sei \mathcal{K} eine Zerlegung von M . Dann die folgende Relation ist eine Äquivalenzrelation auf M :

$$x \equiv y \iff \exists N \in \mathcal{K}: x, y \in N$$

Anders geschrieben:

$$\equiv := \{(x, y) \in M \times M : \exists N \in \mathcal{K} \text{ mit } x, y \in N\}$$

Theorem

Sei M eine nicht leere Menge, und sei \mathcal{K} eine Zerlegung von M . Dann die folgende Relation ist eine Äquivalenzrelation auf M :

$$x \equiv y \iff \exists N \in \mathcal{K}: x, y \in N$$

Beweis. Offensichtlich ist \equiv eine Relation auf M .

- **Reflexivität:** Sei $x \in M$. Da $M = \bigcup \mathcal{K}$ gibt es eine Menge $N \in \mathcal{K}$ mit $x \in N$. Also $x \equiv x$.
- **Symmetrie:** Sei $x \equiv y$. Dann existiert $N \in \mathcal{K}$ mit $\{x, y\} \subseteq N$. Folglich auch $y \equiv x$.
- **Transitivität:** Seien $x \equiv y$ und $y \equiv z$. Also existieren $N, N' \in \mathcal{K}$ mit $\{x, y\} \subseteq N$ und $\{y, z\} \subseteq N'$. Da $y \in N \cap N'$, sind N und N' nicht disjunkt, und so gilt $N = N'$. Folglich $\{x, z\} \subseteq N$ und damit $x \equiv z$.

□

1. Wiederholung

2. Äquivalenzrelationen und Zerlegungen

3. Funktionen - Definition

4. Injektivität, Surjektivität, Bijektivität

5. Komposition von Funktionen

6. Invertierung von Funktionen

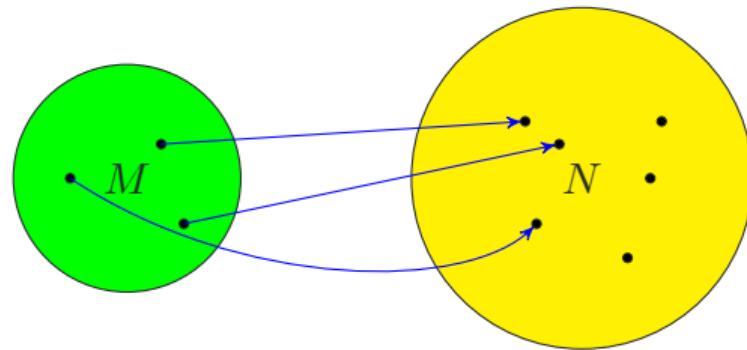
- Seien M und N Mengen. Eine **Funktion** (oder eine **Abbildung**) ist eine Relation $R \subseteq M \times N$ mit der Eigenschaft dass für jedes $m \in M$ genau ein $n \in N$ existiert, so dass $(m, n) \in R$.
- Anders gesagt: Für jedes $m \in M$ gibt es mindestens ein $n \in N$ (**Totalität**) und höchstens ein $n \in N$ mit $m R n$ (**Eindeutigkeit**)

► Totalität:

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

► Eindeutigkeit:

$$\forall m \in M, x, y \in N: R(m, x) \wedge R(m, y) \rightarrow x = y$$



Beispiele.

- Sei B die Menge der Bundesbürger. Wir haben die Relation

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

von B nach \mathbb{N} . Das ist eine Funktion.

- Keine Funktion: die Freund-Relation

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

auf der Menge der Facebook-Nutzer F . Es wäre eine Funktion nur wenn jeder Facebook-Benutzer genau einen Freund hätte.

- Die Relation $R = \{(n, n') \mid n \in \mathbb{N}, n' = 2n\}$ ist eine Funktion. $f(x) = 2x$.
- Die Identität id_M ist eine Funktion.

Notation/Wortschatz.

- $f \subseteq M \times N$ eine Funktion, dann schreiben wir $f: M \rightarrow N$.
- Für $(m, n) \in f$ schreiben wir entweder $n = f(m)$ oder $m \xrightarrow{f} n$.
 - ▶ n ist dann das **Bild** von m
 - ▶ m ist ein **Urbild** von n .
- Die Menge M heißt **Definitionsbereich** und die Menge N **Bildbereich** oder **Wertebereich** von f .

- Für eine Teilmenge $M' \subset M$ definieren wir

$$f(M') := \{f(m) \mid m \in M'\}.$$

Das ist die Menge aller Bilder von Elementen aus M' , **Bild** von M' unter f .

- Für eine Teilmenge $N' \subset N$ definieren wir

$$f^{-1}(N') := \{m \in M \mid f(m) \in N'\}$$

die Menge aller Urbilder von Elementen aus N' , **Urbild** von N' unter f .

Beispiele.

- Betrachten wir $\text{id}_M: M \rightarrow M$. Diese Funktion könnte man auch so definieren:

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

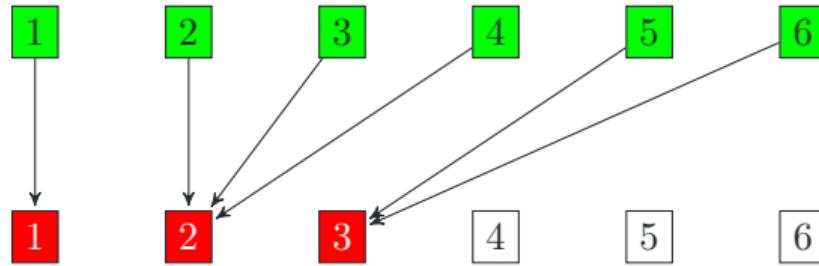
Für alle $M' \subseteq M$ gilt $\text{id}_M(M') = M'$ und $\text{id}_M^{-1}(M') = M'$

- Sei verdoppeln: $\mathbb{N} \rightarrow \mathbb{N}$ die Funktion

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

für alle $n \in \mathbb{N}$. Es gilt $\text{verdoppeln}(\mathbb{N}) = \{2x \mid x \in \mathbb{N}\}$ und
 $\text{verdoppeln}^{-1}(\{2k + 1 \mid k \in \mathbb{N}\}) = \emptyset$.

- Sei $M := \{1, 2, 3, 4, 5, 6\}$. Wir definieren $f: M \rightarrow M$ durch $m \mapsto \lceil \sqrt{m} \rceil$ für alle $m \in M$.



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

1. Wiederholung
2. Äquivalenzrelationen und Zerlegungen
3. Funktionen - Definition
4. Injektivität, Surjektivität, Bijektivität
5. Komposition von Funktionen
6. Invertierung von Funktionen

- $f: M \rightarrow N$ heißt **injektiv** gdw. alle verschiedenen Elemente von M auch verschiedene Bilder unter f haben.

$$\forall x, y \in M: x \neq y \rightarrow f(x) \neq f(y)$$

Manchmal schreibt man $f: M \hookrightarrow N$.

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

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

Manchman schreibt man $f: M \twoheadrightarrow N$.

- Sind beide Eigenschaften erfüllt, so heißt f **bijektiv**.
- Man sagt auch dass f eine Injektion, Surjektion, oder Bijektion ist. Eine Bijektion auf einer Menge M wird auch **Permutation** von M genannt.
- Beispiele:
 - ▶ $\text{id}_M: M \rightarrow M$ ist eine Bijektion.
 - ▶ Die Funktion verdoppeln: $\mathbb{N} \rightarrow \mathbb{N}$ ist injektiv, aber nicht surjektiv.
 - ▶ Die Funktion $f: \mathbb{N} \rightarrow \mathbb{N}$ mit $f(n) = \lceil \sqrt{n} \rceil$ ist surjektiv, aber nicht injektiv, denn es gilt $f(2) = f(3)$.
 - ▶ Die Funktion $q: \mathbb{R} \rightarrow \mathbb{R}$, mit $q(x) := x^2$ definiert, ist weder injektiv noch surjektiv.

1. Wiederholung
2. Äquivalenzrelationen und Zerlegungen
3. Funktionen - Definition
4. Injektivität, Surjektivität, Bijektivität
5. Komposition von Funktionen
6. Invertierung von Funktionen

Funktionen sind Relationen, also können wir Funktionen komponieren. Wir schreiben auch $g \circ f(m)$ oder $g(f(m))$ statt $f; g(m)$.

Theorem

Die Komposition zweier Funktionen ist wieder eine Funktion.

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

- Eindeutigkeit. Falls $(a, b) \in f; g$ und $(a, c) \in f; g$ dann $\exists x, y \in N$ mit $(a, x) \in f$, $(x, b) \in g$, $(a, y) \in f$, $(y, c) \in g$. Da f ist eindeutig, haben wir $x = y$. Aber da g ist auch eindeutig, haben wir $b = c$.
- Totalität. Sei $a \in M$. Da f ist total, existiert $b \in N$ mit $(a, b) \in f$. Da g ist total, existiert $c \in P$ mit $(b, c) \in g$. Es folgt dass $(a, c) \in f; g$.

Komposition ist assoziativ (auch gilt für dir Komposition von Relationen)

Theorem

Für Abbildungen $f: M \rightarrow N$, $g: N \rightarrow P$ und $h: P \rightarrow Q$ gilt

$$(f ; g) ; h = f ; (g ; h)$$

Beweis.

- Sei $y := (f; g); h(x)$. Zu zeigen ist dass $y = f; (g; h)(x)$.
- Dann existiert a mit $(a, y) \in h$, $(x, a) \in f; g$. Deswegen existiert auch b mit $(x, b) \in f$ und $(b, a) \in g$.
- Es folgt $(b, y) \in g; h$, und deswegen auch $(x, y) \in f; (g; h)$. □

Theorem

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

- Wenn f und g injektiv sind, dann ist $f ; g$ injektiv.
- Wenn f und g surjektiv sind, dann ist $f ; g$ surjektiv.
- Wenn f und g bijektiv sind, dann ist $f ; g$ bijektiv.

Beweis.

- 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 $g(f(m)) \neq g(f(m'))$. Also ist $f ; g$ injektiv.

- (Surjektivität) 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.

- (Bijektivität) Das ist eine Folgerung aus den zwei ersten Punkten. □

1. Wiederholung
2. Äquivalenzrelationen und Zerlegungen
3. Funktionen - Definition
4. Injektivität, Surjektivität, Bijektivität
5. Komposition von Funktionen
6. Invertierung von Funktionen

- Manchmal möchte man eine Funktionsanwendung rückgängig machen können, zum Beispiel bei der Verschlüsselung und Kompression von Daten.
- Eine Funktion $f: M \rightarrow N$ ist **invertierbar** gdw. eine Funktion $g: N \rightarrow M$ existiert, so dass

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

und

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

- Äquivalent gesagt: für alle $m \in M$ gilt $g(f(m)) = m$ und für alle $n \in N$ gilt $f(g(n)) = n$.

Beispiele

- Die Identität id_M ist offensichtlich invertierbar. $\text{id}_M; \text{id}_M = \text{id}_M$.
- Die Funktion verdoppeln ist nicht invertierbar. Welchen Wert soll die inverse Funktion der Zahl 3 zuweisen?
- Die Funktion f mit $f(n) = \lceil \sqrt{n} \rceil$ ist nicht invertierbar. Welchen Wert soll die inverse Funktion der Zahl 2 zuweisen?



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski

Mathematisches Institut

grabowski@math.uni-leipzig.de



UNIVERSITÄT
LEIPZIG

Vorlesung 7 - Funktionen und Ordnungsrelationen

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

1. Wiederholung

2. Invertierung von Funktionen

3. Einseitige Inversen

4. Ordnungsrelationen

5. Schranken, Maxima und Minima

6. Infima und Suprema

- Sei \equiv eine Äquivalenzrelation auf M , dann ist M/\equiv eine Zerlegung von M . Umgekehrt, wenn wir eine Zerlegung \mathcal{K} von M haben, dann können wir eine Äquivalenzrelation definieren, sodass die Äquivalenzklassen gleich zu \mathcal{K} sind.
- Funktionen sind spezielle Relationen. Nämlich, $f \subset M \times N$ ist eine Funktion gdw für jedes $m \in M$ existiert genau ein Element $n \in N$ so dass $(m, n) \in f$. Wir schreiben $f(m) = n$, oder $m \mapsto n$.
- $f: M \rightarrow N$ ist injektiv gdw $\forall x, y \in M: x \neq y \rightarrow f(x) \neq f(y)$
- $f: M \rightarrow N$ ist surjektiv gdw $\forall b \in N \exists a \in M \mid f(a) = b$
- $f: M \rightarrow N$ ist bijektive gdw f ist injektiv und surjektiv.

- Funktionen sind Relationen, und Relation können wir komponieren. Deswegen können wir auch Funktionen komponieren. Wir haben bewiesen dass wenn $f: M \rightarrow N, g: N \rightarrow P$ sind zwei Funktionen dann $f;g: M \rightarrow P$ ist auch eine Funktion.
- Es gilt $f;g(x) = g(f(x))$.
- Komposition ist assoziativ: $(f;g);h = f;(g;h)$.
- Wenn f, g beide injektiv (bzw. surjektiv oder bijektiv) sind, dann hat auch $f;g$ die entsprechende Eigenschaft.

1. Wiederholung
2. Invertierung von Funktionen
3. Einseitige Inversen
4. Ordnungsrelationen
5. Schranken, Maxima und Minima
6. Infima und Suprema

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

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

und

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

- Äquivalent gesagt: für alle $m \in M$ gilt $g(f(m)) = m$ und für alle $n \in N$ gilt $f(g(n)) = n$.

- Kandidat für die inverse Funktion: Die inverse Relation f^{-1}

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

- $(m, m) \in f; f^{-1}$
- $(f^{-1}; f \subset id_N)$. Wenn f surjektiv ist, dann $(f^{-1}; f = id_N)$.

Beweis.

- $(m, f(m)) \in f, (f(m), m) \in f^{-1}$. Deswegen $(m, m) \in f; f^{-1}$.
- Sei $(n, x) \in f^{-1}; f$. Dann $(n, a) \in f^{-1}, (a, x) = (a, f(a)) \in f$. Weil $(n, a) \in f^{-1}$, schließen wir $f(a) = n$. Das zeigt dass $f^{-1}; f \subset id_N$.

Wenn f surjektiv ist und $n \in N$, dann existiert $m \in M$ mit $(m, n) \in f$. Dann auch $(n, m) \in f^{-1}$, und deswegen $(n, n) \in f^{-1}; f$. Das zeigt dass $id_N \subset f^{-1}; f$.

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

Beweis. (\rightarrow) Sei f invertierbar. Dann existiert eine Funktion $g: N \rightarrow M$, so dass $f ; g = \text{id}_M$ und $g ; f = \text{id}_N$.

- Injektivität von f : Seien $x, y \in M$ mit $f(x) = f(y)$. Zu zeigen: $x = y$. Es gilt

$$x = g(f(x)) = g(f(y)) = y.$$

- Surjektivität von f . Sei $n \in N$ beliebig. Dann ist $f(g(n)) = n$. Also existiert ein $m \in M$, so dass $f(m) = n$, nämlich $m := g(n)$.

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

← Sei f bijektiv. Wir zeigen, dass f^{-1} eine Funktion ist.

- Totalität von f^{-1} : Sei $n \in N$ beliebig. Da f surjektiv ist, existiert $m \in M$ mit $f(m) = n$. Also $(n, m) \in f^{-1}$.
- Eindeutigkeit. Seien $(n, x) \in f^{-1}$ und $(n, y) \in f^{-1}$. Folglich gilt $f(x) = n = f(y)$. Da f injektiv ist, folgt $x = y$.

Aus dem Lemma wissen wir $f^{-1}; f = \text{id}_N$, und $\text{id}_N \subset f; f^{-1}$. Da $f; f^{-1}$ eine Funktion, folgt aus der Eindeutigkeit $\text{id}_N = f; f^{-1}$.

□

Satz. (Eindeutigkeit der inversen Funktion) Sei $f: M \rightarrow N$ und seien $g, g': N \rightarrow M$ mit

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

und

$$f ; g' = \text{id}_M, \quad g' ; f = \text{id}_N.$$

Dann gilt $g = g'$.

Beweis. Wegen der Assoziativität der Komposition gilt

$$g = g ; \text{id}_M = g ; (f ; g') = (g ; f) ; g' = \text{id}_N ; g' = g'.$$

□

1. Wiederholung
2. Invertierung von Funktionen
3. Einseitige Inversen
4. Ordnungsrelationen
5. Schranken, Maxima und Minima
6. Infima und Suprema

In Anwendungen wie zum Beispiel die Verschlüsselung sind die Funktionen, mit denen wir arbeiten, häufig nicht bijektiv, sondern nur injektiv. In diesem Fall spricht man von einer einseitigen Inverse.

Satz. Für jede injektive Funktion $f: M \rightarrow N$ existiert eine Funktion $g: N \rightarrow M$, so dass $f; g = \text{id}_M$.

Beweis. Die Relation f^{-1} ist eindeutig (doch generell nicht total, also keine Funktion). Wir zeigen es wie früher: Seien $(n, x) \in f^{-1}$ und $(n, y) \in f^{-1}$. Folglich gilt $f(x) = n = f(y)$ und da f ist injektiv, folgt $x = y$.

Sei $m_0 \in M$ beliebig. Wir definieren $g: N \rightarrow M$ wie folgt: wenn $n \in f(M)$ dann $g(n) := f^{-1}(n)$, und sonst $g(n) := m_0$.

Zu zeigen: wenn $m \in M$ dann $f; g(m) = g(f(m)) = m$, Da $f(m) \in f(M)$, folgt $g(f(m)) = f^{-1}(f(m)) = m$.

□

Einseitige Inversen haben wir auch für surjektive Funktionen (doch zu bemerken ist dass die Inverse "auf der anderen Seite" ist, im Vergleich zu surjektiven Funktionen)

Satz. Für jede surjektive Funktion $f: M \rightarrow N$ existiert eine Funktion $g: N \rightarrow M$, so dass $g ; f = \text{id}_N$.

- Da die Funktion f nicht immer injektiv ist, ist unser Kandidat f^{-1} im Allgemeinen nicht eindeutig, also auch keine Funktion.
- Der Beweis folgt nun einer simplen Idee: Wir wählen für jedes Element $n \in N$ ein beliebiges Urbild $m_n \in f^{-1}(\{n\})$, und bauen so aus f^{-1} die gesuchte Funktion g .

Satz. Für jede surjektive Funktion $f: M \rightarrow N$ existiert eine Funktion $g: N \rightarrow M$, so dass $g ; f = \text{id}_N$.

Beweis. (nutzt “Auswahlaxiom”) Sei $n \in N$ beliebig. Da f surjektiv ist, existiert $m \in M$ mit $f(m) = n$. Also $f^{-1}(\{n\}) \neq \emptyset$.

Wähle ein $m_n \in f^{-1}(\{n\})$ für jedes $n \in N$. Wir definieren die Funktion $g: N \rightarrow M$ durch $g(n) := m_n$.

Zu zeigen: $g ; f = \text{id}_N$. Für alle $n \in N$ gilt

$$f(g(n)) = f(m_n) = n.$$

□

Im Allgemeinen ist es nicht möglich, die Funktion g im vorherigen Beweis explizit ("algorithmish") zu definieren. Die Urbilde von Elementen können "ununterscheidbar" sein.

- In vielen konkreten Situationen ist dies möglich - zum Beispiel können wir eine surjektive Funktion $f: \mathbb{N} \rightarrow \mathbb{N}$ haben. In diesem Fall könnten wir die einseitige Inverse $g: \mathbb{N} \rightarrow \mathbb{N}$ definieren, indem wir das kleinste Element im Vorbild wählen.
- Aber im Allgemeinen, wenn wir die gesamte Mathematik aufbauen würden, indem wir alle "ersten Prinzipien" (so-genannte "Axiome"), die wir verwenden, sorgfältig angeben, müssten wir auch das Auswahlaxiom explizit aufnehmen.

(Auswahlaxiom, Zermelo 1904) Für jede Menge \mathcal{X} von nicht-leeren Mengen gibt es eine **Auswahlfunktion**, d.h. Funktion $c: \mathcal{X} \rightarrow \bigcup \mathcal{X}$ mit $c(M) \in M$ für alle $M \in \mathcal{X}$.

- In der Konstruktion der einseitigen Inverse, nehmen wir $\mathcal{X} := \{f^{-1}(n): n \in N\}$

1. Wiederholung
2. Invertierung von Funktionen
3. Einseitige Inversen
4. Ordnungsrelationen
5. Schranken, Maxima und Minima
6. Infima und Suprema

Wir haben die Relationen \leq auf \mathbb{Z} und \subseteq auf $\mathcal{P}(M)$, wo M eine beliebige Menge ist. Diese sind Beispiele von Ordnungsrelationen. Die algemeine Definition ist wie folgt.

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

- Das Paar (M, \preceq) heißt dann eine geordnete Menge, oder auch eine **teilweise geordnete Menge**.
- Ist \preceq auch vollständig, dann heißt (M, \preceq) auch **total geordnete Menge**, **linear geordnete Menge** oder eine **Kette**.
- Die Schreibweise (M, \preceq) bedeutet dass wir uns die Menge M nun geordnet vorstellen. Das ist ein Beispiel von einer mathematischen Struktur

Beispiele

- Die Identität id_M ist eine Ordnungsrelation, aber nicht vollständig.
- (\mathbb{N}, \leq) ist eine total geordnete Menge.
- Für jede Menge M ist $(\mathcal{P}(M), \subseteq)$ eine teilweise geordnete Menge.
- Die Teilbarkeitsrelation $| = \{(n, n') \in \mathbb{N}_+ \times \mathbb{N}_+ \mid n \text{ teilt } n'\}$ ist eine Ordnungsrelation.
 - ▶ **Reflexivität:** Für alle $x \in \mathbb{N}_+$ teilt x sich selbst, also $x | x$.
 - ▶ **Antisymmetrie:** Seien $x | y$ und $y | x$. Dann gelten $x \leq y$ und $y \leq x$, womit $x = y$.
 - ▶ **Transitivität:** Seien $x | y$ und $y | z$. D.h. es existieren $k, n \in \mathbb{N}_+$, so dass $kx = y$ und $ny = z$. Also $z = ny = n(kx) = (nk)x$, womit auch $x | z$ gilt.

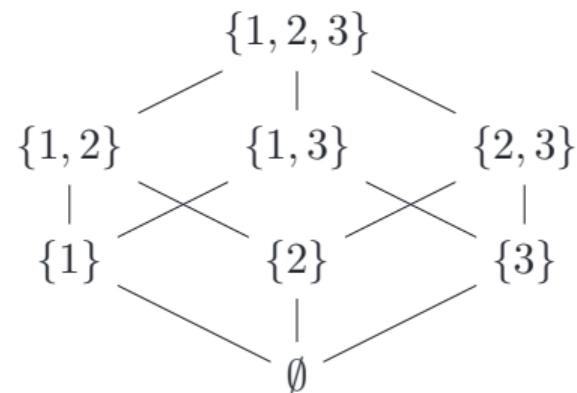
Teilweise geordnete Mengen lassen sich durch Hasse-Diagramme visualisieren.

Hasse-Diagramm für (\mathbb{N}, \leq) :



- Alle Kanten sind per Konvention nach oben gerichtet.
- Eine Kante von x nach y bedeutet dass (x, y) ist in der Ordnungsrelation also $x \preceq y$.
- Kanten aus id_M (Schleifen) werden nicht dargestellt
- Ebenso Kanten, die sich mittels Transitivität aus anderen Kanten ergeben.

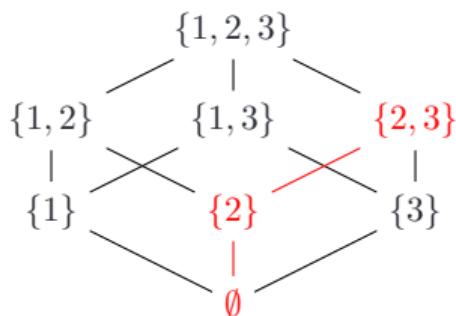
Hasse-Diagramm für $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$:



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

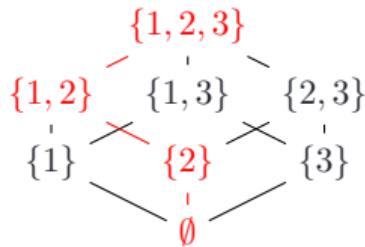
Beispiele

- Die Menge \mathbb{N} ist eine Teilkette von (\mathbb{Z}, \leq)
- Die Menge $\{\emptyset, \{2\}, \{2, 3\}\}$ ist eine Teilkette von $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$

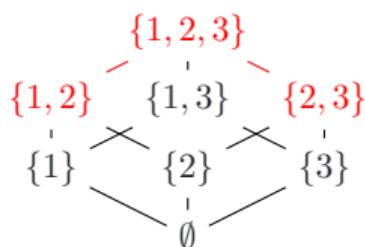


Beispiele

- Die Menge $\{\emptyset, \{2\}, \{1, 2\}, \{1, 2, 3\}\}$ ist eine Teilkette von $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$



- Die Menge $\{\{1, 2\}, \{1, 2, 3\}, \{2, 3\}\}$ ist keine Teilkette von $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$.



- Wir dürfen jedoch die geordnete Menge $(\{\{1, 2\}, \{1, 2, 3\}, \{2, 3\}\}, \subseteq)$ betrachten.

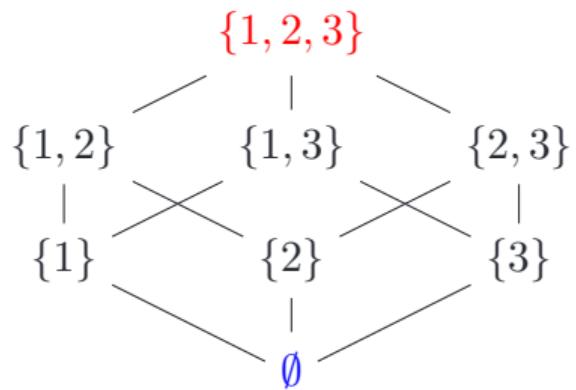
1. Wiederholung
2. Invertierung von Funktionen
3. Einseitige Inversen
4. Ordnungsrelationen
5. Schranken, Maxima und Minima
6. Infima und Suprema

Sei (M, \preceq) eine teilweise geordnete Menge. Ein Element $x \in M$ ist

- **maximal** gdw. $x \not\preceq m$ für alle $m \in M$ mit $m \neq x$; d.h. es gibt keine echt größeren Elemente,
- **minimal** gdw. $m \not\preceq x$ für alle $m \in M$ mit $m \neq x$; d.h. es gibt keine echt kleineren Elemente.

Beispiele

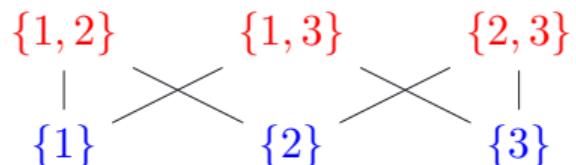
- In (\mathbb{N}, \leq) haben wir 0 als einziges minimales Element und keine maximalen Elemente.
- $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$



maximale Elemente: $\{1, 2, 3\}$ minimale Elemente: \emptyset

Beispiele

- $(\mathcal{P}(\{1, 2, 3\}) \setminus \{\emptyset, \{1, 2, 3\}\}, \subseteq)$



maximale Elemente: $\{1, 2\}$, $\{1, 3\}$ und $\{2, 3\}$, minimale Elemente: $\{1\}$, $\{2\}$ und $\{3\}$

Sei (M, \preceq) eine teilweise geordnete Menge und $X \subseteq M$. Ein Element $m \in M$ ist

- eine **obere Schranke** für X gdw. $x \preceq m$ für alle $x \in X$; d. h. größer als alle Elemente aus X ,
- das **größte Element** von X gdw. $m \in X$ und m obere Schranke für X ist;
- Die Begriffe **untere Schranke** und **kleinstes Element** werden analog definiert. Ein Element m ist eine untere Schranke falls $\forall x \in X$ gilt $m \preceq x$. Und m ist das kleinste Element von X wenn $m \in X$ und m ist eine untere Schranke.
- Es gibt höchstens ein größtes (bzw. kleinstes) Element von X . Wenn m, n sind beide die größten Elemente, dann $m \preceq n$ und $n \preceq m$, also $m = n$.
- Wir bezeichnen mit $\uparrow X$ und $\downarrow X$ jeweils die Menge der oberen und unteren Schranken. Mit $\max X$ und $\min X$ bezeichnen wir jeweils das größte and das kleinste Element von X (wenn sie existieren).

Beispiele

- In (\mathbb{Z}, \leq) hat die Mengen \mathbb{N}
 - ▶ obere Schranken: keine
 - ▶ größtes Element: keins
- In (\mathbb{Z}, \leq) hat $\{-1, 2\}$
 - ▶ obere Schranken: $\{z \in \mathbb{Z} \mid z \geq 2\}$
 - ▶ größtes Element: 2
- In $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$ hat $\{\{1\}, \{2\}\}$
 - ▶ obere Schranken: $\{1, 2\}$ und $\{1, 2, 3\}$
 - ▶ größtes Element: keins, maximale Elemente $\{1\}, \{2\}$.

1. Wiederholung
2. Invertierung von Funktionen
3. Einseitige Inversen
4. Ordnungsrelationen
5. Schranken, Maxima und Minima
6. Infima und Suprema

- Sei (M, \preceq) eine teilweise geordnete Menge und $X \subseteq M$.
- Das **Supremum** $\sup X$ von X ist das kleinste Element von $\uparrow X$. Also die kleinste obere Schranke für X .
- Das **Infimum** $\inf X$ von X ist das größte Element von $\downarrow X$. Also die größte untere Schranke für X .

- Wir betrachten $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$.
 - ▶ Das Supremum von $\{\{2\}\}$ ist $\{2\}$, es gilt $\sup\{\{2\}\} = \{2\}$.
 - ▶ Es gilt $\sup\{\{1\}, \{2\}\} = \{1, 2\}$.
- Suprema/Infima existieren nicht immer. Als Beispiel betrachten wir \mathbb{R} mit üblicher Ordnungsrelation. Dann \mathbb{R} selbst hat kein Supremum und kein Infimum.
- Supremum von $[0, 1)$ in (\mathbb{R}, \leq) ist 1.
- Sei $M \subseteq \mathcal{P}(\mathbb{N})$ die Menge von allen endlichen Teilmengen von \mathbb{N} , mit der Teilmengerelation \subseteq . Dann hat M kein Supremum in M . Jedoch M hat ein Supremum als eine Teilmenge von $\mathcal{P}(\mathbb{N})$.

Satz. Sei M eine Menge, und sei $X \subset \mathcal{P}(M)$. Dann X hat Supremum und Infimum in $\mathcal{P}(M)$, und es gilt $\sup X = \bigcup X$, $\inf X = \bigcap X$.

Beweis. Z.B. zeigen wir $\sup X = \bigcup X$. Wir zeigen zunächst, dass $\bigcup X$ eine obere Schranke für X ist. Sei $Y \in X$ beliebig. Dann gilt $Y \subseteq \bigcup X$, womit $\bigcup X$ obere Schranke ist.

Jetzt zeigen wir das $\bigcup X$ die kleinste obere Schranke ist. Sei S irgendeine andere obere Schranke. Dann für jede $Y \in X$ gilt $Y \subset S$, wobei auch $\bigcup X \subset S$. □

- Dieser Satz motiviert die folgende Notation: Sei (M, \subseteq) eine geordnete Menge, und $x, y \in M$. Dann schreiben wir $x \vee y := \sup(\{x, y\})$, $x \wedge y := \inf(\{x, y\})$.
- (M, \subseteq) heißt **Verband** gdw. für alle $x, y \in M$ haben $x \vee y$ und $x \wedge y$ existieren.
- (M, \subseteq) heißt **vollständiger Verband** gdw. für alle $X \subseteq M$ haben $\sup X$ und $\inf X$ existieren.



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski

Mathematisches Institut

grabowski@math.uni-leipzig.de



UNIVERSITÄT
LEIPZIG

Vorlesung 8 - Vergleichen der Größen von Mengen, Satz von
Cantor-Schröder-Bernstein

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

1. Wiederholung
2. Wann haben zwei Mengen gleich viele Elemente - Kardinalitäten
3. $|\mathbb{N}| \neq |\mathbb{R}|$
4. Ordnungsrelation auf Kardinalitäten
5. Formulierung des Satzes von Cantor-Schröder-Bernstein
6. Erster Beweis
7. Kontinuum und Kontinuumshypothese

Für uns die symbole $M \subseteq N$ und $M \subset N$ bedeuten das gleiche, d.h. M ist eine Teilmenge von N

- $f: M \rightarrow N$ ist injektiv gdw. $(\forall a, b \in M, a \neq b \rightarrow f(a) \neq f(b))$.
- $f: M \rightarrow N$ ist surjektiv gdw. $\forall b \in N \exists a \in M \mid f(a) = b$
- $f: M \rightarrow N$ ist bijektiv gdw. f ist injektiv und surjektiv.
- Eine Funktion $f: M \rightarrow N$ ist **invertierbar** gdw. eine Funktion $g: N \rightarrow M$ existiert, so dass

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

und

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

- Äquivalent gesagt: für alle $m \in M$ gilt $g(f(m)) = m$ und für alle $n \in N$ gilt $f(g(n)) = n$.

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

Satz. (Eindeutigkeit des Inversen) Sei $f: M \rightarrow N$ und seien $g, g': N \rightarrow M$ mit

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

und

$$f ; g' = \text{id}_M, \quad g' ; f = \text{id}_N.$$

Dann gilt $g = g'$.

Satz. Für jede injektive Funktion $f: M \rightarrow N$ existiert eine Funktion $g: N \rightarrow M$, so dass $f; g = \text{id}_M$.

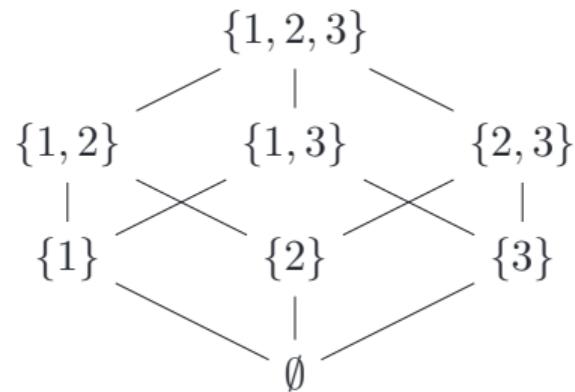
Satz. Für jede surjektive Funktion $f: M \rightarrow N$ existiert eine Funktion $g: N \rightarrow M$, so dass $g; f = \text{id}_N$.

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

- (M, \preceq) heißt eine geordnete Menge oder eine teilweise geordnete Menge.
- Ist \preceq auch vollständig, dann heißt (M, \preceq) auch **total geordnete Menge**, **linear geordnete Menge** oder eine **Kette**.
- Insbesondere ist jede total geordnete Menge auch eine teilweise geordnete Menge.

Teilweise geordnete Mengen lassen sich durch Hasse-Diagramme visualisieren.

Hasse-Diagramm für $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$:



1. Wiederholung
2. Wann haben zwei Mengen gleich viele Elemente - Kardinalitäten
3. $|\mathbb{N}| \neq |\mathbb{R}|$
4. Ordnungsrelation auf Kardinalitäten
5. Formulierung des Satzes von Cantor-Schröder-Bernstein
6. Erster Beweis
7. Kontinuum und Kontinuumshypothese

Satz. Sei M eine endliche Menge und sei $f: M \rightarrow M$ eine Funktion. Dann f ist surjektiv gdw f ist injektiv.

Beweis. Wir betrachten die Menge $\mathcal{K} := \{f^{-1}(\{m\}) \mid m \in f(M)\}$. Offenbar ist \mathcal{K} eine Zerlegung von M .

- Für $m \in M$, sei $c_m := |f^{-1}(\{m\})|$. Es gilt $c_m \geq 1$ und $|M| = \sum_{m \in f(M)} c_m$.
- (\rightarrow) Sei f surjektiv, aber nicht injektiv. Dann ist $f(M) = M$ und $c_m \geq 2$ für ein $m \in M$. Es folgt jedoch $\sum_{m \in M} c_m > |M|$. Widerspruch.
- (\leftarrow) Sei f injektiv, aber nicht surjektiv. Dann ist $c_m = 1$ für alle $m \in f(M)$ und $|f(M)| < |M|$. Also auch $\sum_{m \in f(M)} c_m = |f(M)| < |M|$. Widerspruch.
- Dieses Resultat gilt nicht für unendliche Mengen.
 - ▶ Z.B. $f: \mathbb{N} \rightarrow \mathbb{N}$ mit $f(x) = 2x$ ist zwar injektiv, aber nicht surjektiv.
 - ▶ $f: \mathbb{N} \rightarrow \mathbb{N}$ mit $f(x) = \lceil \sqrt{x} \rceil$ ist surjektiv, aber nicht injektiv.

- Zwei Mengen M und N sind **gleichmächtig**, kurz $|M| = |N|$, gdw. eine bijektive Funktion $f: M \rightarrow N$ existiert.
- Heute werden wir insbesondere sehen dass es gibt unendlich viele Unendlichkeiten.
- Erste Beispiele
 - ▶ $|\emptyset| \neq |M|$ für alle nicht-leeren Mengen M
 - ▶ $|\{1, 2, 3\}| = |\{6, 9, 11\}|$ via z.B. $\{(1, 6), (2, 9), (3, 11)\}$
 - ▶ $|\mathbb{Z}| = |\mathbb{N}|$ via Bijektion $f: \mathbb{Z} \rightarrow \mathbb{N}$ mit

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

Sei \mathcal{U} ein Universum von Mengen. Dann die Gleichmächtigkeit ist eine Äquivalenzrelation auf \mathcal{U} .

- Reflexivität: id_M ist eine Bijektion $M \rightarrow M$ Symmetrie: $f: M \rightarrow N$ bijektiv, dann $f^{-1}: N \rightarrow M$ bijektiv, Transitivität: $f: A \rightarrow B$ $g: B \rightarrow C$ Bijektionen, dann $f; g$ ist auch bijektiv.

Die Äquivalenzklassen heißen **Kardinalitäten**.

- Beispiel: die Kardinalität von $\{6, 9, 11\}$ heißt “drei”.

- Sind alle unendlichen Mengen gleichmächtig? Andersgesagt: gibt es nur eine unendliche Kardinalität?
- Bevor wir diese Frage beantworten, eine kleine Erinnerung: die Klasse \mathcal{U} aller Mengen ist selbst keine Menge (“Russell Paradox”).
 - ▶ Nehmen wir an, dass \mathcal{U} eine Menge ist. Dann definieren wir $V := \{M \in \mathcal{U} : M \notin M\}$. Nun haben wir zwei Möglichkeiten: $V \in V$ oder $V \notin V$.
 - ▶ Wenn $V \in V$, dann schliessen wir, durch die Definition von V , dass $V \notin V$. Wenn wir $V \notin V$ annehmen, dann folgt, dass $V \in V$. Das ist ein Widerspruch.

1. Wiederholung
2. Wann haben zwei Mengen gleich viele Elemente - Kardinalitäten
3. $|\mathbb{N}| \neq |\mathbb{R}|$
4. Ordnungsrelation auf Kardinalitäten
5. Formulierung des Satzes von Cantor-Schröder-Bernstein
6. Erster Beweis
7. Kontinuum und Kontinuumshypothese

Beweis. Um einen Widerspruch zu bekommen, nehmen wir an dass $|\mathbb{N}| = |\mathbb{R}|$. Dann existiert eine bijektive Funktion $b: \mathbb{N} \rightarrow \mathbb{R}$. Schreibe Bilder als Dezimalzahlen

$$\begin{aligned} b(0) &= a_0 , \quad d_{00} \quad d_{01} \quad d_{02} \quad \cdots \quad d_{0n} \quad \cdots \\ b(1) &= a_1 , \quad d_{10} \quad d_{11} \quad d_{12} \quad \cdots \quad d_{1n} \quad \cdots \\ b(2) &= a_2 , \quad d_{20} \quad d_{21} \quad d_{22} \quad \cdots \quad d_{2n} \quad \cdots \\ &\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \ddots \quad \vdots \quad \vdots \\ b(n) &= a_n , \quad d_{n0} \quad d_{n1} \quad d_{n2} \quad \cdots \quad d_{nn} \quad \cdots \\ &\vdots \quad \vdots \quad \ddots \end{aligned}$$

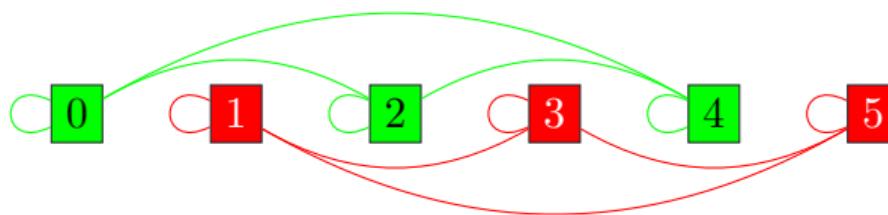
Für jedes $i \in \mathbb{N}$, wähle eine Ziffer $d_i \in \{1, \dots, 8\} \setminus \{d_{ii}\}$. Da b surjektiv ist, existiert ein $n \in \mathbb{N}$ mit $b(n) = 0, d_0 d_1 d_2 d_3 \dots$

Was können wir über die n -te Stelle von $b(n)$ sagen? Es gilt $d_n = d_{nn} \neq d_{nn}$. Dieser Widerspruch zeigt, dass b kann nicht existieren. □

- Das war ein “diagonales Argument”.
- Die Kardinalität von \mathbb{N} heißt “aleph-0”: \aleph_0 .
- Die Kardinalität von \mathbb{R} heißt “continuum”: \mathfrak{c} .

1. Wiederholung
2. Wann haben zwei Mengen gleich viele Elemente - Kardinalitäten
3. $|\mathbb{N}| \neq |\mathbb{R}|$
4. **Ordnungsrelation auf Kardinalitäten**
5. Formulierung des Satzes von Cantor-Schröder-Bernstein
6. Erster Beweis
7. Kontinuum und Kontinuumshypothese

- Wir definieren $|M| \leq |N|$ genau dann wenn es gibt eine Injektion $f: M \rightarrow N$. Wir möchten erst argumentieren, dass diese Relation wohldefiniert ist.
- Warum könnte diese Relation überhaupt nicht wohldefiniert sein? Betrachten wir ein Beispiel.



- Die Relation $[i] \prec [j]$ gdw. $i < j$ ist nicht wohldefiniert: $[1] \prec [2] = [0]$ aber auch $[1] \not\prec [0] = [2]$.

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

Beweis.

- (\rightarrow) Sei $f: M \rightarrow N$ injektiv. Aufgrund der Annahme $|M| = |X|$ und $|N| = |Y|$. existieren Bijektionen $b: X \rightarrow M$ und $c: N \rightarrow Y$.
Dann ist die Funktion $(b ; f ; c: X \rightarrow Y$ injektiv.
- (\leftarrow) Durch die Symmetrie der Aussage

□

Wortschatz: Wir sagen auch dass eine Menge N **mächtiger als** eine Menge M ist, gdw. $|M| \leq |N|$, also gdw. es existiert eine injektive Funktion $f: M \rightarrow N$.

- Für endliche Kardinalitäten erhalten wir die normale Ordnungsrelation $|\{1, 2\}| \leq |\{2, 3, 4\}|$
- $|\mathbb{N}| \leq |\mathbb{Z}|$ vermittels $\iota: \mathbb{N} \rightarrow \mathbb{Z}$ mit $\iota(n) = n$. Wir haben auch $|\mathbb{N}| = |\mathbb{Z}|$.
- $|\mathbb{N}| \leq |\mathbb{R}|$, und $|\mathbb{N}| \neq |\mathbb{R}|$.
- Sei $M \subseteq N$. Dann gilt $|M| \leq |N|$, da $\iota: M \rightarrow N$, mit $\iota(m) = m$, ist injektiv.
- Sei $f: M \rightarrow N$ surjektiv. Dann $|N| \leq |M|$. In der Tat, sei $g: N \rightarrow M$ mit $g; f = \text{id}_M$. Dann g ist injektiv: wenn x, y sind so dass $g(x) = g(y)$, dann auch $x = f(g(x)) = f(g(y)) = y$.

- Ist das überhaupt eine Ordnungsrelation?
 - ▶ Reflexivitt: $\text{id}_M: M \rightarrow M$ ist injektiv, also $|M| \leq |M|$
 - ▶ Transitivitt: $f: A \rightarrow B$, $g: B \rightarrow C$ - Injektionen, dann $f; g: A \rightarrow C$ auch Injektion. Also $|A| \leq |B|$ und $|B| \leq |C|$ impliziert $|A| \leq |C|$.
 - ▶ Antisymmetrie: $f: A \rightarrow B$ Injektion, $g: B \rightarrow A$ Injektion (also $|A| \leq |B|$ und $|B| \leq |A|$). Gibt es eine Bijektion $A \rightarrow B$? Das ist nicht klar.

1. Wiederholung
2. Wann haben zwei Mengen gleich viele Elemente - Kardinalitäten
3. $|\mathbb{N}| \neq |\mathbb{R}|$
4. Ordnungsrelation auf Kardinalitäten
5. Formulierung des Satzes von Cantor-Schröder-Bernstein
6. Erster Beweis
7. Kontinuum und Kontinuumshypothese

Satz. (Cantor-Schröder-Bernstein) Seien $f: M \rightarrow N$ und $g: N \rightarrow M$ injektive Funktionen. Dann existiert eine bijektive Funktion $B: M \rightarrow N$.

Wir sehen heute zwei Beweise. 1) Beweis mit der Relation die durch f und g erzeugt ist
2) mit Fix-Punkte.

1. Wiederholung
2. Wann haben zwei Mengen gleich viele Elemente - Kardinalitäten
3. $|\mathbb{N}| \neq |\mathbb{R}|$
4. Ordnungsrelation auf Kardinalitäten
5. Formulierung des Satzes von Cantor-Schröder-Bernstein
- 6. Erster Beweis**
7. Kontinuum und Kontinuumshypothese

Satz. (Cantor-Schröder-Bernstein) Seien $f: M \rightarrow N$ und $g: N \rightarrow M$ injektive Funktionen. Dann existiert eine bijektive Funktion $B: M \rightarrow N$.

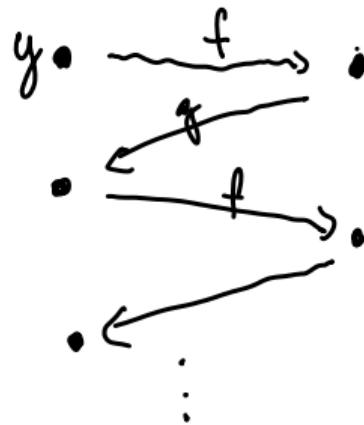
Beweis. Wir können annehmen, dass M und N disjunkt sind.

► Wenn das nicht der Fall ist, dann betrachten wir die Mengen $M' := \{(m, 0) : m \in M\}$, $N' := \{(n, 0) : n \in N\}$. Wir haben Bijektionen $M' \rightarrow M$, $N' \rightarrow N$, also eine Bijektion zwischen M und N existiert gdw eine Bijektion zwischen M' und N' existiert.

- Wir betrachten die zwei Relationen f und g auf $M \cup N$, und die Relation V - die kleinste Äquivalenzrelation die f und g enthält.
- Sei $K \subset M \cup N$ eine Äquivalenzklasse von V . Es reicht uns, eine Bijektion $b_K: K \cup M \rightarrow K \cup N$ zu konstruieren. In der Tat, falls wir das schaffen, dann definieren wir $b: M \rightarrow N$ durch $b(x) := b_K(x)$ wenn $x \in K$. Weil $\{K \cap M : K \in M \cup N/V\}$ eine Zerlegung von M ist, schließen wir, dass b eine Bijektion ist.

Sei K eine Äquivalenzklasse von V .

- In $K : \text{gibt's } y \in M \text{ mit } y \notin g(N)$.



- Für $z \in M \cap K$ definieren wir $b_K(z) := f(z)$.

- b_K ist eine Bijektion: Tatsätzlich, $K = \{y, f(y), gf(y), fgf(y), \dots\}$. Alle diese Elemente sind unterschiedlich.
- Erst beweisen wir $y, gf(y), (gf)^2(y), \dots$ sind unterschiedlich.
 - ▶ Induktionsbeweis: IA: $y, gf(y)$ sind unterschiedlich, da $y \notin g(N)$.
 - ▶ IH: $y, gf(y), \dots (gf)^k(y)$ sind unterschiedlich.
 - ▶ IB: Zu zeigen ist, dass $y, gf(y), \dots (gf)^k(y)$ sind unterschiedlich. Durch Widerspruch: sei $(gf)^{k+1}(y) = (gf)^l(y)$, mit $l \leq k$. Da $y \notin g(N)$, folgt $l \geq 1$. Da gf injektiv, folgt $(gf)^k(y) = gf^{l-1}(y)$. Widerspruch mit IA.
- Da g eine Injektion ist, sehen wir, dass $y, f(y), gf(y), fgf(y), \dots$ sind unterschiedliche Elemente. Es folgt dass b eine Bijection ist.

- In K gibt's $y \in N$ mit $y \notin f(M)$.



- Für $z \in M \cap K$ definieren wir $b_K(z) := g^{-1}(z)$.

- Für alle $z \in M \cap K$ gilt $z \in g(N)$, und für alle $N \cap K$ gilt $z \in f(M)$.



- Für $z \in M \cap K$ definieren wir $b_K(z) := f(z)$.

□

Konsequenz von CSB:

Satz. Die Relation \leq ist eine Ordnungsrelation auf Kardinalitäten.

Beweis. Transitivität und Reflexivität haben wir schon gesegen.

- **Antisymmetrie:** Seien $|M| \leq |N|$ und $|N| \leq |M|$. Also existieren injektive Funktionen $f: M \rightarrow N$ und $g: N \rightarrow M$. Dann existiert auch eine bijektive Funktion $h: M \rightarrow N$ nach CSB und damit $|M| = |N|$.

□

Ist \leq auf Kardinalitäten total? D.h. wenn wir zwei Mengen M und N haben, gibt's immer eine Injektion $M \rightarrow N$ oder eine injektion $N \rightarrow M$?

Satz. (Satz von Hartogs, benutzt das Auswahlaxiom) Die Kardinalitäten \mathcal{K} bilden eine total geordnete Menge (\mathcal{K}, \leq)

- Ähnlich man kann auch beweisen dass $|\mathbb{N}|$ ist die kleinste unendliche Kardinalität, manchmal auch \aleph_0 genannt.

- Wir sagen dass eine Menge M ist **abzählbar** gdw. $|M| \leq |\mathbb{N}|$; d. h. wenn sie höchstens die Kardinalität von \mathbb{N} hat. Jede endliche Menge, \mathbb{Z} und \mathbb{Q} sind also abzählbar, aber \mathbb{R} hingegen nicht.
- Echt mächtigere Mengen nennen wir auch **überabzählbar**.

Gibt es unendlich viele unendliche Kardinalitäten?

Satz. (Cantor) Für jede Menge M gelten $|M| \leq |\mathcal{P}(M)|$ und $|M| \neq |\mathcal{P}(M)|$.

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

Wir zeigen nun $|M| \neq |\mathcal{P}(M)|$ indirekt. Sei also $|M| = |\mathcal{P}(M)|$. Damit existiert eine bijektive Funktion $g: M \rightarrow \mathcal{P}(M)$.

Sei

$$X := \{x \in M \mid x \notin g(x)\} .$$

Da g surjektiv ist, existiert $m \in M$, so dass $g(m) = X$. Ist $m \in g(m) = X$? Wenn ja dann durch Definition von X folgt $m \notin g(m)$. Ähnlich wenn $m \notin g(m) = X$ dann folgt $m \in g(m)$. Widerspruch. □

Es gibt also unendlich viele unendliche Kardinalitäten:

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

1. Wiederholung
2. Wann haben zwei Mengen gleich viele Elemente - Kardinalitäten
3. $|\mathbb{N}| \neq |\mathbb{R}|$
4. Ordnungsrelation auf Kardinalitäten
5. Formulierung des Satzes von Cantor-Schröder-Bernstein
6. Erster Beweis
7. Kontinuum und Kontinuumshypothese

- Die Kardinalität $|\mathbb{R}|$ nennt man auch Kontinuum und bezeichnet man sie mit dem Symbol c .
- Gibt es Kardinalitäten zwischen $\aleph_0 = |\mathbb{N}|$ und $c = |\mathbb{R}|$? Ein Kandidat wäre das reelle Intervall $(-\frac{1}{2}, \frac{1}{2})$. Doch $|(0, 1)| = |\mathbb{R}|$ mit Hilfe von $f(x) := \tan(\pi x)$
- Eine weiterer Kandidat wäre die Potenzmenge von \mathbb{N} .

Satz. [Cantor 1874] Es gilt $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

Beweis. Nach CSB brauchen wir zwei Injektionen zu konstruieren.

- Jede reelle Zahl $x \in (0, 1)$ lässt sich eindeutig als $x = [0, d_1d_2d_3d_4 \dots]_{10}$ mit den Ziffern $d_1, d_2, \dots \in \{0, 1, \dots, 9\}$ darstellen, so dass kein $n \in \mathbb{N}$ existiert mit $d_i = 9$ für alle $i \in \mathbb{N}$ mit $i \geq n$. Dann sei $f(x) := \{[d_1]_{10}, [d_1d_2]_{10}, [d_1d_2d_3]_{10}, \dots\}$. Diese Funktion f ist injektiv.
- Sei $X \subseteq \mathbb{N}$. Wir konstruieren die reelle Zahl $g(X) := [0, 1b_0b_1b_2 \dots]_{10}$ mit $b_i \in \{0, 5\}$, so dass $b_i = 5$ gdw. $i \in X$ für alle $i \in \mathbb{N}$. Offenbar ist auch diese Funktion g injektiv. \square

- Es scheint schwer zu sein eine Menge M mit $|\mathbb{N}| < M < |\mathbb{R}|$ zu finden. Dies brachte Georg Cantor in 1878 dazu, die folgende Frage zu stellen, die als "Kontinuumshypothese" bekannt ist: Ist es wahr, dass eine Menge A von reellen Zahlen entweder die gleiche Anzahl von Elementen hat wie die gesamte reelle Linie \mathbb{R} , oder die gleiche Anzahl von Elementen hat wie die natürlichen Zahlen \mathbb{N} ?
- In den folgenden Jahrzehnten wurde diese Frage als eine der dringendsten mathematischen Fragen betrachtet. David Hilbert setzte sie im Jahr 1900 an die Spitze seiner Liste der wichtigsten offenen Probleme. Auch heute noch wird die Antwort auf diese Frage häufig missverstanden.

- Heute wissen wir dank der gemeinsamen Arbeit von Kurt Gödel aus den 1940er Jahren und Paul Cohen aus den 1960er Jahren, dass diese Frage unmöglich zu beantworten ist. (man sagt dass CH "unabhängig von dem ZFC-Axiomensystem ist").
- Der Grund dafür ist, ganz informell gesprochen, dass es trotz der genauen mathematischen Definition der reellen Linie verschiedene Modelle der reellen Linie und ihrer Teilmengen gibt, in denen die Antwort auf die Kontinuumshypothese entweder wahr oder falsch ist.
- Es besteht die entfernte Möglichkeit (so gennante "Dream Solution"), dass es bessere mathematische Definitionen gibt, die genau beschreiben, woran (alle? die meisten?) Mathematiker denken, wenn sie an die reelle Linie und ihre Teilmengen denken. Dies scheint eine Überzeugung zu sein, die Kurt Gödel manchmal äußerte. In der Zwischenzeit fragen sich Mathematiker manchmal halb spaßhaft, ob sie "an die Kontinuumshypothese glauben".



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski

Mathematisches Institut

grabowski@math.uni-leipzig.de



UNIVERSITÄT
LEIPZIG

Vorlesung 9 - Mächtigkeit von Mengen

Diskrete Strukturen (WS 2023-24)

Łukasz Grabowski

Mathematisches Institut

1. Wiederholung
2. Weitere Beispiele zur Mächtigkeit
3. Fixpunkte
4. Der zweite Beweis vom Satz von Cantor-Schröder-Bernstein
5. Verbände
6. Charakterisierung von Verbänden durch \vee und \wedge

- Zwei Mengen M und N sind **gleichmächtig**, kurz $|M| = |N|$, gdw. eine bijektive Funktion $f: M \rightarrow N$ existiert.
 - ▶ Z.B. $|\mathbb{Z}| = |\mathbb{N}|$
 - ▶ $|\mathbb{N}| \neq |\mathbb{R}|$, $|\mathcal{P}(X)| \neq |\mathcal{X}|$ Andere Notation: $\mathcal{P}(X) = 2^X$.
- Sei \mathcal{U} ein Universum von Mengen. Dann die Gleichmächtigkeit ist eine Äquivalenzrelation auf \mathcal{U} .
- Die Äquivalenzklassen heißen **Kardinalitäten**.
- (Cantor -Schröder-Bernstein) Seien $f: A \rightarrow B$ und $g: B \rightarrow A$ injektive Funktionen. Dann existiert eine bijektive Funktion $h: A \rightarrow B$.
 - ▶ Wir definieren $|M| \leq |N|$ genau dann wenn es gibt eine Injektion $f: M \rightarrow N$. Das ist eine Ordnungsrelation.

1. Wiederholung
2. Weitere Beispiele zur Mächtigkeit
3. Fixpunkte
4. Der zweite Beweis vom Satz von Cantor-Schröder-Bernstein
5. Verbände
6. Charakterisierung von Verbänden durch \vee und \wedge

- $|\mathbb{N}^2| = |\mathbb{N}|$.
 - ▶ Nach CBS, wir brauchen Injektionen $f: \mathbb{N} \rightarrow \mathbb{N}^2$ und $g: \mathbb{N}^2 \rightarrow \mathbb{N}$ zu konstruieren.
 - ▶ $f: \mathbb{N} \rightarrow \mathbb{N}^2$; Z.B. $f(x) := (x, 0)$,
 - ▶ $g: \mathbb{N}^2 \rightarrow \mathbb{N}$: $g(n, m) := 1n_km_kn_{k-1}m_{k-1}\dots n_0m_0$, wobei $k + 1$ ist das Maximum der Längen der Dezimaldarstellungen von n und m , und $n = \sum_{i=0}^k n_i \cdot 10^i$ und $m = \sum_{i=0}^k m_i \cdot 10^i$ mit $n_i, m_i \in \{0, \dots, 9\}$ für alle $i \in \{0, \dots, k\}$.

- $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.
 - ▶ $|\mathbb{R}| = |(0, 1)|$. Nach CBS reicht die Injektionen $f: (0, 1) \rightarrow \mathcal{P}(\mathbb{N})$ und $g: \mathcal{P}(\mathbb{N}) \rightarrow (0, 1)$ zu konstruieren.
 - ▶ Jede reelle Zahl $x \in (0, 1)$ lässt sich eindeutig als $x = [0, d_1d_2d_3d_4 \dots]_{10}$ darstellen, mit den Ziffern $d_1, d_2, \dots \in \{0, 1, \dots, 9\}$, so dass kein $n \in \mathbb{N}$ existiert mit $d_i = 9$ für alle $i \in \mathbb{N}$ mit $i \geq n$.
 - ▶ Dann sei $g: \mathbb{R} \rightarrow \mathcal{P}((0, 1)) \rightarrow \mathbb{R}$ so definiert:
$$f(x) := \{[d_1]_{10}, [d_1d_2]_{10}, [d_1d_2d_3]_{10}, \dots\}$$

. Diese Funktion f ist injektiv.

► Sei $X \subseteq \mathbb{N}$. Wir definieren die reelle Zahl $g(X) := [0,1b_0b_1b_2\cdots]_{10}$ mit $b_i \in \{0,5\}$, so dass $b_i = 5$ gdw. $i \in X$ für alle $i \in \mathbb{N}$. Offenbar ist auch diese Funktion g injektiv.

- $|\mathbb{Q}| = |\mathbb{Z}|$
- Wir wissen $|\mathbb{Q}| \geq |\mathbb{Z}|$, also es reicht zu zeigen dass $|\mathbb{Q}| \leq |\mathbb{Z}|$.
- Wir wissen auch $|\mathbb{Z}| = |\mathbb{N}| = |\mathbb{N}^2|$, also es reicht zu zeigen dass $|\mathbb{Q}| \leq |\mathbb{N}^2|$.
- Die positiven rationalen Zahlen entsprechen den nicht weiter kürzbaren Brüchen $\frac{m}{n}$ mit $m, n \in \mathbb{N}_+$. Also wir haben eine Injektion $f: \mathbb{Q}_+ \rightarrow \mathbb{N}_+ \times \mathbb{N}_+$, mit $f(\frac{m}{n}) = (m, n)$.
- Jetzt bauen wir die Injektion $g: \mathbb{Q} \rightarrow \mathbb{N} \times \mathbb{N}$.
 - ▶ $g(\frac{m}{n}) := (m, n)$ wenn $\text{ggt}(m, n) = 1$, $m, n > 0$,
 - ▶ $g(\frac{-m}{n}) := (-m, n)$ $\text{ggt}(m, n) = 1$, $m, n > 0$
 - ▶ $g(0) := (0, 0)$.

Satz

Seien A_1, A_2, \dots abzählbar. Dann $\bigcup_{i=1}^{\infty} A_i$ ist auch abzählbar.

Beweis.

- Wir müssen eine Injektion $\bigcup_i A_i \rightarrow \mathbb{N}$ definieren.
- Erst, wir finden disjunkte Teilmenge $B_1, B_2, \dots \subset \mathbb{N}$ mit $|B_i| = |\mathbb{N}|$ und $\bigcup_i B_i = \mathbb{N}$.
 - ▶ 1, 1, 2, 1, 2, 3, 1, 2, 3, 4, 1, 2, 3, 4, 5, ...
- Wir haben Bijektionen $\beta_i: \mathbb{N} \rightarrow B_i$. Wir haben auch Injektionen $\alpha_i: A_i \rightarrow \mathbb{N}$.
- Wir definieren $s: \bigcup_{i=1}^{\infty} A_i \rightarrow \mathbb{N}$, so dass $s(x)$ ist die kleinste i mit $x \in A_i$.
- Schließlich können wir die Injektion $F: \bigcup_{i=1}^{\infty} A_i \rightarrow \mathbb{N}$ definieren, wie folgt:
$$F(x) := \beta_{s(x)}(\alpha_{s(x)}(x)).$$
 - ▶ Falls $F(x) = F(y)$, dann $s(x) = s(y)$, weil die Bilde von verschiedenen β_i 's disjunkt sind. Dann die Injektivität folgt da $\alpha_{s(x)}$ and $\beta_{s(x)}$ sind beide injektiv.

□

Sei X eine Menge. Dann definieren wir $\mathcal{P}_{<\infty}(X) := \{A \subset X : |A| < \infty\}$.

Satz

$\mathcal{P}_{<\infty}(\mathbb{N})$ ist abzählbar.

Beweis.

- Es reicht zu zeigen dass $\forall k \in \mathbb{N}$ gilt dass $\mathcal{P}_k(\mathbb{N})$ ist abzählbar.
- Wir haben eine Surjektion $\mathbb{N}^k \rightarrow \mathcal{P}_k(\mathbb{N})$: $(a_1, a_2, \dots, a_k) \mapsto \{a_1, \dots, a_k\}$. Also es reicht zu zeigen, dass \mathbb{N}^k ist abzählbar.
- Wir beweisen mit Induktion $|\mathbb{N}^k| = |\mathbb{N}|$.
 - ▶ IA: $k = 2$ Wir wissen $|\mathbb{N}^2| = |\mathbb{N}|$.
 - ▶ IH: $|\mathbb{N}^k| = |\mathbb{N}|$ wenn $k \geq 1$.
 - ▶ IB: zu zeigen ist $|\mathbb{N}^{k+1}| = |\mathbb{N}|$. Es gilt $|\mathbb{N}^{k+1}| = |\mathbb{N} \times \mathbb{N}^k|$. Aus dem Übungsblatt und aus IH folgt $|\mathbb{N} \times \mathbb{N}^k| = |\mathbb{N} \times \mathbb{N}|$. Also auch $|\mathbb{N}^{k+1}| = |\mathbb{N}|$. □

1. Wiederholung
2. Weitere Beispiele zur Mächtigkeit
3. Fixpunkte
4. Der zweite Beweis vom Satz von Cantor-Schröder-Bernstein
5. Verbände
6. Charakterisierung von Verbänden durch \vee und \wedge

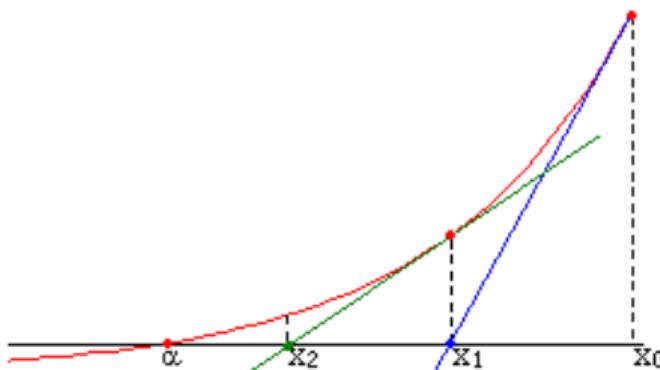
Die Iteration ist ein wesentliches Prinzip in Rainer Mathematik und in der Programmierung. Ein wichtiger Aspekt der Iteration sind die sogenannte **Fixpunkte**. Sei $f: M \rightarrow M$ eine Funktion auf einer Menge M . Ein **Fixpunkt** von f ist ein Element $m \in M$, so dass $f(m) = m$.

Beispiele

- Die Funktion $f: \mathbb{N} \rightarrow \mathbb{N}$ mit $f(x) := x + 1$ hat keine Fixpunkte.
- Die Funktion $f: \mathbb{N} \rightarrow \mathbb{N}$ mit $n \mapsto \lceil \sqrt{n} \rceil$ hat die Fixpunkte 0, 1 und 2.

Beispiel - Die Methode von Newton

- Gegeben: eine differenzierbare Funktion $f: \mathbb{R} \rightarrow \mathbb{R}$
- Ziel: $x \in \mathbb{R}$ zu finden, mit $f(x) = 0$.
- Algorithmus von Newton: wir nehmen $x_0 \in \mathbb{R}$, dann definieren wir $x_1 := x_0 - \frac{f(x_0)}{f'(x_0)}$ und allgemein $x_k := x_{k-1} - \frac{f(x_{k-1})}{f'(x_{k-1})}$
 - ▶ Fixpunkte sind die gesuchten Lösungen. Sehr häufig konvergieren Iterationen zu einem Fixpunkt.



- Wir möchten Fixpunkte benutzen, um einen alternativen Beweis von CBS zu geben
Wir beginnen mit der Erinnerung an das folgende Lemma.

Lemma. Sei M eine Menge. Wir betrachten die teilweise geordnete Menge $(\mathcal{P}(M), \subseteq)$.
Sei $\mathcal{X} \subseteq \mathcal{P}(M)$. Dann $\bigcup \mathcal{X}$ ist die kleinste obere Schranke von \mathcal{X} . D.h.

$$\bigcup \mathcal{X} \subseteq U$$

für alle $U \in \uparrow \mathcal{X}$

Satz. (Lemma von Knaster-Tarski) Sei $f: \mathcal{P}(M) \rightarrow \mathcal{P}(M)$ mit $f(X) \subseteq f(Y)$ für alle $X \subseteq Y \subseteq M$. Dann hat f einen Fixpunkt.

Beweis. Seien

$$\mathcal{Q} := \{X \in \mathcal{P}(M) \mid X \subseteq f(X)\}$$

und $N := \bigcup \mathcal{Q}$.

- Wir zeigen jetzt dass $f(N) = N$, d.h. N ist ein Fixpunkt von f .
- Für jede Menge $X \in \mathcal{Q}$ gilt $X \subseteq N$. Deswegen gilt $X \subseteq f(X) \subseteq f(N)$.
- Es folgt dass $f(N)$ ist eine obere Schranke von \mathcal{Q} . Deswegen $N = \bigcup \mathcal{Q} \subseteq f(N)$.
- Auch gilt: $f(N) \subseteq f(f(N))$, wodurch $f(N) \in \mathcal{Q}$. Es folgt also $f(N) \subseteq \bigcup \mathcal{Q} = N$, und deswegen auch $N = f(N)$,

□

Beispiele

- Sei $f: \mathbb{N} \rightarrow \mathbb{N}$ mit $f(x) := x + 1$. Wir betrachten jetzt f als eine Funktion auf $\mathcal{P}(\mathbb{N})$.
- Für welche Teilmengen $X \subseteq \mathbb{N}$ gilt $f(X) = X$? Für $X = \emptyset$
- Sei $g: \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ wie folgt definiert:

$$g(X) := X \cup f(X).$$

Fixpunkte: $\emptyset, \mathbb{N}, X_k := \{n \in \mathbb{N} \mid n \geq k\}$ mit $k \in \mathbb{N}$.

1. Wiederholung
2. Weitere Beispiele zur Mächtigkeit
3. Fixpunkte
4. Der zweite Beweis vom Satz von Cantor-Schröder-Bernstein
5. Verbände
6. Charakterisierung von Verbänden durch \vee und \wedge

Satz. (Cantor-Schröder-Bernstein) Seien $f: M \rightarrow N$ und $g: N \rightarrow M$ injektive Funktionen. Dann existiert eine bijektive Funktion $B: M \rightarrow N$.

Beweis.

- Wir definieren die Funktion $h: \mathcal{P}(M) \rightarrow \mathcal{P}(M)$:

$$h(X) := M \setminus g(N \setminus f(X)) .$$

- Für alle $X \subseteq Y \subseteq M$ gilt $f(X) \subseteq f(Y)$ also auch $N \setminus f(Y) \subseteq N \setminus f(X)$, und deswegen auch

$$g(N \setminus f(Y)) \subseteq g(N \setminus f(X)).$$

D.h. $h(X) \subseteq h(Y)$.

- Nach dem Lemma von Knaster-Tarski existiert also ein Fixpunkt $F \subseteq M$ für h . Es gilt

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

- Wir definieren eine Funktion $B: M \rightarrow N$ durch

$$B(m) := f(m) \text{ wenn } m \in F$$

$$B(m) := g^{-1}(m) \text{ wenn } m \in M \setminus F$$

Wir möchten zeigen dass B ist bijektiv.

- **Surjektivität:** 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 ist $n \in N \setminus f(F)$ und damit

$$g(n) \in g(N \setminus f(F)) = M \setminus F.$$

Also $B(g(n)) = n$.

Injektivität: Seien $x, y \in M$ mit $B(x) = B(y)$.

- Sei $B(x) \in f(F)$. Erst zeigen wir dass $x, y \in F$. Sonst wenn z.b. $x \in M \setminus F$, dann deswegen dass $M \setminus F = g(N \setminus f(F))$, würden wir $B(x) = g^{-1}(x) \in N \setminus f(F)$ haben, was jedoch $B(x) \in f(F)$ widerspricht. Also gilt $x, y \in F$. Damit gilt auch $x = y$, da f injektiv ist.
- Sei $B(x) \notin f(F)$. Dann gilt $x, y \in M \setminus F$, also $x = g(B(x)) = g(B(y)) = y$. □

1. Wiederholung
2. Weitere Beispiele zur Mächtigkeit
3. Fixpunkte
4. Der zweite Beweis vom Satz von Cantor-Schröder-Bernstein
5. Verbände
6. Charakterisierung von Verbänden durch \vee und \wedge

- Sei (M, \preceq) eine teilweise geordnete Menge und $X \subseteq M$.
- Das **Supremum** $\sup X$ von X ist das kleinste Element von $\uparrow X$, also die kleinste obere Schranke für X .
- Das **Infimum** $\inf X$ von X ist das größte Element von $\downarrow X$, also die größte untere Schranke für X .
- Suprema/Infima existieren nicht immer. Als Beispiel betrachten wir \mathbb{R} mit üblicher Ordnungsrelation. Dann \mathbb{R} selbst hat kein Supremum und kein Infimum.
- Noch ein Beispiel: Die Menge M von allen endlichen Teilmengen von \mathbb{N} , mit der Teilmengerelation \subseteq . Dann hat M kein Supremum.
- Sei M eine Menge, und sei $X \subset \mathcal{P}(M)$. Dann \mathcal{M} hat Supremum und Infimum in \mathcal{P} , und es gilt $\sup X = \bigcup X$, $\inf X = \bigcap X$.
- Dieser Satz motiviert folgende Notation: Sei (M, \subseteq) eine geordnete Menge, und $x, y \in M$. Dann schreiben wir $x \vee y := \sup(\{x, y\})$, $x \wedge y := \inf(\{x, y\})$.

- (M, \subseteq) heißt **Verband** gdw. für alle $x, y \in M$ wir haben dass $x \vee y$ und $x \wedge y$ existieren.
- (M, \subseteq) heißt **vollständiger Verband** gdw. für alle $X \subseteq M$ wir habe dass $\sup X$ und $\inf X$ existieren.

Beispiele

- (\mathbb{N}, \leq) , (\mathbb{Z}, \leq) , (\mathbb{Q}, \leq) und (\mathbb{R}, \leq) sind alle Verbände. Sie sind alle nicht vollständig.
- Wir haben gesehen dass für jede Menge M gilt dass $(\mathcal{P}(M), \subseteq)$ ist ein vollständiger Verband.
- Sei $\mathcal{Q} \subset \mathcal{P}(M)$ die Menge von allen endlichen Mengen. Dann \mathcal{Q} ist ein Verband. \mathcal{Q} ist vollständig gdw. M ist eine endliche Menge.
- Jeder vollständiger Verband \mathcal{M} hat das kleinste und das grosse Element. Sie sind, bzw., $\inf \mathcal{M}$ und $\sup \mathcal{M}$.

Satz. Jeder endliche Verband ist vollständig.

Beweis. Sei (M, \preceq) ein Verband. Wir beweisen durch Induktion über $n = |X|$: Für jede endliche nicht-leere Teilmenge $X \subseteq M$ existiert $\sup X$. (Der Beweis bezüglich $\inf X$ ist ähnlich.)

- **Induktionsanfang:** Sei $n = 1 = |X|$ und $x \in X$. Dann ist $x \preceq x$ und für alle oberen Schranken z von X gilt offenbar $x \preceq z$. Also ist $x = \sup X$.
- Sei $n \in \mathbb{N}_+$ beliebig.
 - ▶ **Induktionshypothese:** Für jedes $X \subseteq M$ mit $|X| = n$ existiert $\sup X$.
 - ▶ **Induktionsbehauptung:** Für jedes $X \subseteq M$ mit $|X| = n + 1$ existiert $\sup X$.

Satz. Jeder endliche Verband ist vollständig.

Beweis. (Fortsetzung)

- Sei $X \subseteq M$ mit $|X| = n + 1$ und $z \in X$. Gemäß Induktionshypothese existiert ein $y = \sup(X \setminus \{z\})$. Wir zeigen, dass $z \vee y = \sup X$.
- Es gilt $x \preceq z \vee y$ für alle $x \in X$. Sei $m \in M$, so dass $x \preceq m$ für alle $x \in X$. Also auch $z \preceq m$ und $y \preceq m$. Damit allerdings auch $z \vee y \preceq m$.

□

1. Wiederholung
2. Weitere Beispiele zur Mächtigkeit
3. Fixpunkte
4. Der zweite Beweis vom Satz von Cantor-Schröder-Bernstein
5. Verbände
6. Charakterisierung von Verbänden durch \vee und \wedge

Satz. Für jeden Verband (M, \preceq) und alle $x, y, z \in M$ gelten

- $x \vee y = y \vee x$ und $x \wedge y = y \wedge x$ Kommutativität
- $x \vee (y \vee z) = (x \vee y) \vee z$ und $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ Assoziativität
- $x \vee (x \wedge y) = x$ und $x \wedge (x \vee y) = x$ Absorption

Beweis. Z.B. beweisen wir dass $x \wedge (y \wedge z) = (x \wedge y) \wedge z$.

$x \wedge (y \wedge z) \geq x$ und $x \wedge (y \wedge z) \geq y \wedge z$. Also $x \wedge (y \wedge z) \geq x$ und $x \wedge (y \wedge z) \geq y$ und $x \wedge (y \wedge z) \geq z$.

Damit sehen wir $x \wedge (y \wedge z) \geq x \wedge y$, und deswegen

$$x \wedge (y \wedge z) \geq (x \wedge y) \wedge z.$$

Ähnlich zeigen wir $(x \wedge y) \wedge z \geq x \wedge (y \wedge z)$, also $(x \wedge y) \wedge z = x \wedge (y \wedge z)$,



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski

Mathematisches Institut

grabowski@math.uni-leipzig.de



UNIVERSITÄT
LEIPZIG

Vorlesung 10 - Verbände

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

Wo sind wir im Modul?

- Gemacht:
 - ▶ Logik
 - ▶ Mengenlehre
 - ▶ Insbesondere: Relationen, Äquivalenzrelationen, Funktionen, Ordnungsrelationen, Kardinalität
- Ab jetzt: Verschiedene Strukturen die in Anwendungen in Mathematik und Informatik wichtig sind.

1. Verbände

2. Charakterisierung von Verbänden durch die Operationen \vee und \wedge

- Sei (M, \preceq) eine teilweise geordnete Menge und $X \subseteq M$.
- Das **Supremum** $\sup X$ von X ist die kleinste obere Schranke für X , also das kleinste Element von $\uparrow X$.
- Das **Infimum** $\inf X$ von X ist die größte untere Schranke für X , also das größte Element von $\downarrow X$.
- Suprema/Infima existieren nicht immer. Als Beispiel betrachten wir \mathbb{R} mit der üblichen Ordnungsrelation. Dann \mathbb{R} selbst hat kein Supremum und kein Infimum.
- Noch ein Beispiel: Die Menge M von allen endlichen Teilmengen von \mathbb{N} , mit der Teilmengerelation \subseteq . Dann hat M kein Supremum in M .
- Sei M eine Menge, und sei $X \subset \mathcal{P}(M)$. Dann X hat Supremum und Infimum in $\mathcal{P}(M)$, und es gilt $\sup X = \bigcup X$, $\inf X = \bigcap X$.
- Dieser Satz motiviert die folgende Notation: Sei (M, \subseteq) eine geordnete Menge, und $x, y \in M$. Dann schreiben wir $x \vee y := \sup(\{x, y\})$, $x \wedge y := \inf(\{x, y\})$.

- (M, \subseteq) heißt **Verband** gdw. für alle $x, y \in M$ gilt dass $x \vee y$ und $x \wedge y$ existieren.
- (M, \subseteq) heißt **vollständiger Verband** gdw. für alle $X \subseteq M$ gilt dass $\sup X$ und $\inf X$ existieren.

Beispiele

- $(\mathbb{N}, \leq), (\mathbb{Z}, \leq), (\mathbb{Q}, \leq)$ und (\mathbb{R}, \leq) sind alle Verbände. Sie sind alle nicht vollständig.
- Für jede Menge M gilt dass $(\mathcal{P}(M), \subseteq)$ ist ein vollständiger Verband.
- Sei $\mathcal{Q} \subset \mathcal{P}(M)$ die Menge von allen endlichen Mengen. Dann \mathcal{Q} ist ein Verband. \mathcal{Q} ist vollständig gdw. M ist eine endliche Menge.
- Jeder vollständiger Verband M hat das kleinste und das grosse Element. Sie sind jeweils $\inf M$ und $\sup M$.

Satz. Jeder endliche Verband ist vollständig.

Beweis.

- Sei (M, \preceq) ein Verband. Wir beweisen durch Induktion über $n = |X|$: Für jede endliche nicht-leere Teilmenge $X \subseteq M$ existiert $\sup X$.
- (Ähnlich mit $\inf X$).
- **Induktionsanfang:** Sei $n = 1 = |X|$ und $x \in X$. Dann ist $x \preceq x$ und für alle oberen Schranken z von X gilt $x \preceq z$. Deswegen ist x die kleinste obere Schranke, also $x = \sup X$.
- Sei $n \in \mathbb{N}_+$ beliebig.
 - ▶ **Induktionshypothese:** Für jedes $X \subseteq M$ mit $|X| = n$ existiert $\sup X$.
 - ▶ **Induktionsbehauptung:** Für jedes $X \subseteq M$ mit $|X| = n + 1$ existiert $\sup X$.

Satz. Jeder endliche Verband ist vollständig.

Beweis. (Fortsetzung)

- Sei $X \subseteq M$ mit $|X| = n + 1$ und $z \in X$.
- Gemäß Induktionshypothese existiert ein $y = \sup(X \setminus \{z\})$.
- Wir zeigen jetzt, dass $z \vee y = \sup X$.
 - ▶ Für alle $x \in X$ gilt $x \preceq z \vee y$. Deswegen ist $z \vee y$ eine obere Schranke für X .
 - ▶ Sei $m \in M$ eine obere Schranke für X , so dass für alle $x \in X$ gilt $x \preceq m$. Also auch $z \preceq m$ und $y \preceq m$. Damit folgt auch $z \vee y \preceq m$, also ist $z \vee y$ die kleinste obere Schranke.
 - ▶ Dies zeigt dass $z \vee y = \sup X$.

□

1. Verbände

2. Charakterisierung von Verbänden durch die Operationen \vee und \wedge

Satz. Für jeden Verband (M, \geq) und alle $x, y, z \in M$ gelten die folgende Eigenschaften.

- $x \vee y = y \vee x$ und $x \wedge y = y \wedge x$ Kommutativität
- $x \vee (y \vee z) = (x \vee y) \vee z$ und $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ Assoziativität
- $x \vee (x \wedge y) = x$ und $x \wedge (x \vee y) = x$ Absorption

Beweis. Als Beispiel, beweisen wir dass $x \wedge (y \wedge z) = (x \wedge y) \wedge z$.

- $x \wedge (y \wedge z) \geq x$ und $x \wedge (y \wedge z) \geq y \wedge z$. Also $x \wedge (y \wedge z) \geq x$ und $x \wedge (y \wedge z) \geq y$ und $x \wedge (y \wedge z) \geq z$.
- Damit sehen wir $x \wedge (y \wedge z) \geq x \wedge y$, und deswegen

$$x \wedge (y \wedge z) \geq (x \wedge y) \wedge z.$$

- Ähnlich zeigen wir $(x \wedge y) \wedge z \geq x \wedge (y \wedge z)$. Deswegen $(x \wedge y) \wedge z = x \wedge (y \wedge z)$,

Ein Verband (M, \subseteq) ist **distributiv** gdw. für alle $x, y, z \in M$ gilt

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

und

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

Satz. Jede total geordnete Menge (M, \preceq) ist ein distributiver Verband.

Beweis.

- Wir müssen zeigen dass \vee und \wedge existieren, und dass die Distributivität gilt
- **Supremum:** Für alle $x, y \in M$ gilt $x \preceq y$ oder $y \preceq x$.
- Ohne Beschränkung der Allgemeinheit (oBdA) sei $x \preceq y$. Dann ist y eine obere Schranke für $\{x, y\}$. Sei z eine beliebige obere Schranke für $\{x, y\}$. Dann gilt $y \preceq z$ und damit ist y die kleinste obere Schranke für $\{x, y\}$. D.h. $y = x \vee y$.
- **Infimum:** Ähnlich.

Satz. Jede total geordnete Menge (M, \preceq) ist ein distributiver Verband.

Beweis. (Fortsetzung.)

- **Distributivitat:** Seien $x, y, z \in M$. Wir zeigen z.B. dass $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.

Ordnung	$x \wedge (y \vee z)$	$(x \wedge y) \vee (x \wedge z)$
$x \preceq y \preceq z$	x	x
$x \preceq z \preceq y$	x	x
$y \preceq x \preceq z$	x	x
$y \preceq z \preceq x$	z	z
$z \preceq x \preceq y$	x	x
$z \preceq y \preceq x$	y	y

□

- Wir betrachten jetzt die folgende Frage: Inwieweit erlauben die Operationen \vee und \wedge die Wiederherstellung der Ordnungsrelation?
- Wir betrachten also eine Menge M zusammen mit zwei Funktionen $\vee, \wedge: M \times M \rightarrow M$.
- Der nächste Satz sagt, dass, wenn wir annehmen, dass diese Operationen sind kommutativ, assoziativ und abssorptiv, dann stammen sie aus einer Ordnungsrelation stammen.

Satz. Sei (M, \sqcup, \sqcap) eine Menge zusammen mit zwei Funktionen $\sqcup, \sqcap: M \times M \rightarrow M$. Wir nehmen an, dass für alle $x, y, z \in M$ das Folgende gilt:

- $x \sqcup y = y \sqcup x$ und $x \sqcap y = y \sqcap x$ (Kommutativität)
- $x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$ und $x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z$ (Assoziativität)
- $x \sqcup (x \sqcap y) = x$ und $x \sqcap (x \sqcup y) = x$ (Absorption)

Dann ist (M, \preceq) ein Verband, wobei

$$\preceq = \{(x, y) \in M \times M \mid x = x \sqcap y\} .$$

Beweis. Für alle $x, y \in M$ definieren wir $x \preceq y$ gdw. $x = x \sqcap y$. Wir beweisen zunächst die Eigenschaften einer Ordnungsrelation.

- **Reflexivität:** Für jedes $x \in M$ gilt nach zweimaligem Anwenden der Absorption

$$x = x \sqcap (x \sqcup (x \sqcap x)) = x \sqcap x ,$$

also $x \preceq x$.

- **Antisymmetrie:** Seien $x \preceq y$ und $y \preceq x$. Es gelten $x = x \sqcap y$ und $y = y \sqcap x$.
Mit Hilfe der Kommutativität gilt dann

$$x = x \sqcap y = y \sqcap x = y .$$

Beweis. (Fortsetzung)

- **Transitivität:** Seien $x \preceq y$ und $y \preceq z$. Es gelten $x = x \sqcap y$ und $y = y \sqcap z$. Unter Nutzung der Assoziativität erhalten wir

$$x = x \sqcap y = x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z = x \sqcap z$$

und damit $x \preceq z$.

Wir beweisen nun noch die Existenz der Suprema (Infima ähnlich). Seien $x, y \in M$. Wir zeigen, dass $x \sqcup y$ das Supremum von $\{x, y\}$ ist.

- **Obere Schranke:** Es gilt $x = x \sqcap (x \sqcup y)$ und damit $x \preceq x \sqcup y$. Ebenso gilt $y = y \sqcap (y \sqcup x)$ und damit $y \preceq x \sqcup y$,

Beweis. (Fortsetzung)

- **Kleinste obere Schranke:** Sei $z \in M$ mit $x \preceq z$ und $y \preceq z$, also $x = x \sqcap z$ und $y = y \sqcap z$. Wir folgern zunächst mit Absorption und Kommutativität

$$\begin{aligned}x \sqcup z &= (x \sqcap z) \sqcup z = z \quad \text{und} \\y \sqcup z &= (y \sqcap z) \sqcup z = z .\end{aligned}$$

Damit ergibt sich nun

$$\begin{aligned}(x \sqcup y) \sqcap z &= (x \sqcup y) \sqcap (x \sqcup z) \\&= (x \sqcup y) \sqcap (x \sqcup (y \sqcup z)) \\&= (x \sqcup y) \sqcap ((x \sqcup y) \sqcup z) = (x \sqcup y)\end{aligned}$$

und damit $(x \sqcup y) \preceq z$.

□



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski

Mathematisches Institut

grabowski@math.uni-leipzig.de



UNIVERSITÄT
LEIPZIG

Vorlesung 11 - Distributive Verbände, allgemeine algebraische
Strukturen, Boolesche Algebren

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

1. Wiederholung

2. Unterverbände und isomorphismen

3. Allgemeine algebraische Strukturen

4. Boolesche Algebren - Definition

- eine geordnete Menge (M, \leq) heißt **Verband** gdw. für alle $x, y \in M$ wir haben dass $x \vee y$ (infimum) und $x \wedge y$ (supremum) existieren. Z.B. $(P(X), \subseteq)$ ist ein Verband.
- Verband (M, \leq) gibt uns eine Menge mit zwei Operationen (M, \vee, \wedge) , die kommutativ, assoziativ, und absorbtiv sind. Umgekehrt jede solche Menge (M, \vee, \wedge) gibt uns ein Verband (M, \leq) . D.H. es gibt zwei äquivalente Wege wie mein ein Verband definieren/betrachten kann.

- Distributive Verbände sind solche wo für alle $x, y, z \in M$ gilt

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

und

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

- Total geordnete Mengen, $(P(X), \subseteq)$ sind distributive Verbände.

1. Wiederholung

2. Unterverbände und isomorphismen

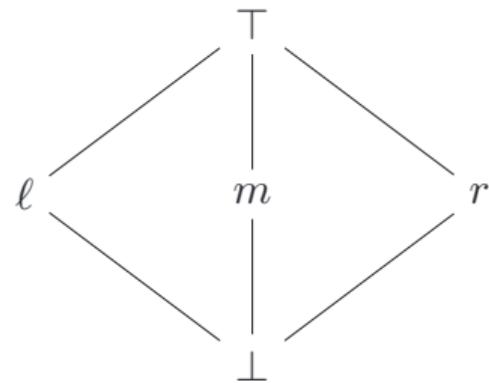
3. Allgemeine algebraische Strukturen

4. Boolesche Algebren - Definition

- Sei (V, \vee, \wedge) ein Verband. Ein **Unterverband** ist eine Menge $W \subset V$ mit der Eigenschaft dass für alle $x, y \in W$ haben wir $x \vee y \in W$ und $x \wedge y \in W$.
- Ein Unterverband von $(P(X), \cap, \cup)$ heißt Mengenverband. Mengenverbände sind distributiv.
- VORSICHT: Jede Menge $Q \subset P(X)$ hat eine Ordnungsrelation die sie zu einer geordneten Mengen macht. Manchmal ist so eine Menge (Q, \subseteq) ein Verband, aber kein Unterverband. Z.B. $Q := \{\emptyset, \{1\}, \{1, 2\}, \{3\}, \{1, 2, 3\}\}$.
 - ▶ Es geht darum dass die Operationen \vee und \wedge müssen in einem Unterverband gleich sein als im ursprünglichen Verband.
 - ▶ Also Q ist zwar ein Verband aber kein Unterverband von $P(\{1, 2, 3\})$.

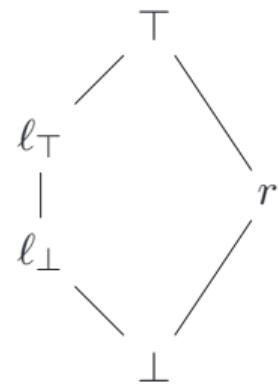
- Wir sagen dass zwei Verbände (V, \vee, \wedge) und (V', \vee', \wedge') sind **isomorph** gdw. es gibt eine bijektion $\varphi: V \rightarrow V'$ mit der Eigenschaft dass für alle $x, y \in V$ haben wir $\varphi(x \vee y) = \varphi(x) \vee' \varphi(y)$ und $\varphi(x \wedge y) = \varphi(x) \wedge' \varphi(y)$.
- Äquivalent gesagt, zwei Verbände (V, \geq) und (V', \geq') sind isomorph gdw. es gibt eine bijektion $\varphi: V \rightarrow V'$ mit der Eigenschaft dass für alle $x, y \in V$ haben wir $x \leq y \iff \varphi(x) \leq' \varphi(y)$.
- Noch anders, äquivalent, gesagt, zwei Verbände sind isomorph, wenn sie “gleiche” Hasse-diagramme haben, wobei “gleiche” bedeutet dass der einzige mögliche Unterschied sind die Namen von Knoten.

- nicht-distributiver Verband M_3 :



- $\ell \vee (m \wedge r) = \ell$ und $(\ell \vee m) \wedge (\ell \vee r) = \top$.

- nicht-distributiver Verband N_5 :



- $\ell_{\top} \wedge (\ell_{\perp} \vee r) = \ell_{\top}$ und $(\ell_{\top} \wedge \ell_{\perp}) \vee (\ell_{\top} \wedge r) = \ell_{\perp}$.

Satz. Sei $\mathcal{V} = (V, \vee, \wedge)$ ein Verband. Dann ist \mathcal{V} distributiv gdw. kein Unterverband von \mathcal{V} isomorph zu den Verbänden M_3 oder N_5 ist.

Beweis.

- Wir zeigen in der Vorlesung nur eine, die “einfache”, Richtung. D.h. wir nehmen an, dass es gibt ein Unterverband von \mathcal{V} , der entweder zu M_3 oder zu N_5 isomorph ist.
- Für die andere Richtung, sehe Skript.
- Sei $U \subseteq V$ eine Teilmenge, die ein Unterverband von V ist, und der isomorph zu M_3 ist.
- Sei $\varphi: V \rightarrow M_3$ ein Isomorphismus. Seien $x := \varphi^{-1}(\ell)$, $y := \varphi^{-1}(m)$, $z := \varphi^{-1}(r)$.
- Wir sehen jetzt dass

$$x \vee (y \wedge z) \neq (x \vee y) \wedge (x \vee z).$$

Satz. Sei $\mathcal{V} = (V, \vee, \wedge)$ ein Verband. Dann ist \mathcal{V} distributiv gdw. kein Unterverband von \mathcal{V} isomorph zu den Verbänden M_3 oder N_5 ist.

Beweis. (Fortsetzung) In der Tat,

$$\varphi(x \vee (y \wedge z)) = \ell \vee (m \wedge r) = \ell$$

und

$$\varphi((x \vee y) \wedge (x \vee z)) = (\ell \vee m) \wedge (\ell \vee r) = \top.$$

- Ähnlich beweisen wir dass wenn U isomorph zu N_5 ist dann auch \mathcal{V} nicht distributiv ist.

1. Wiederholung

2. Unterverbände und Isomorphismen

3. Allgemeine algebraische Strukturen

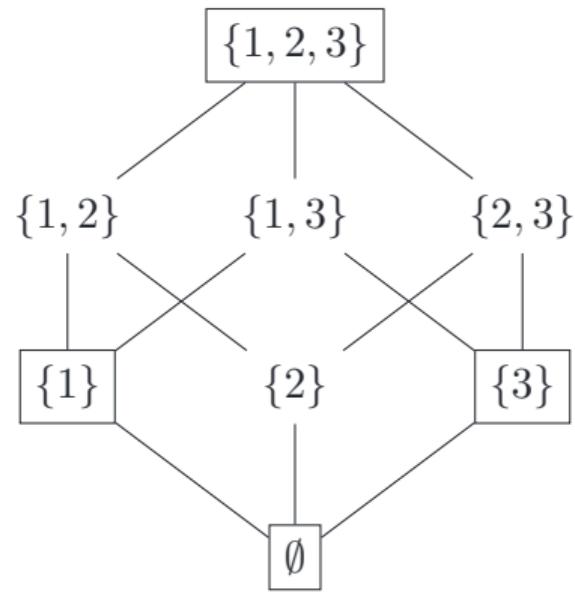
4. Boolesche Algebren - Definition

- Motivation: (U, \leq) , (U, \vee, \wedge) , $(U, \equiv), \dots$
- In allgemeinen, wenn wir eine algebraische Struktur definieren, benutzen wir
 - ▶ $R_1, \dots, R_k \subseteq U \times U$ 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 .
- Wir können so eine **algebraische Struktur** schreiben als $(U, \langle R_1, \dots, R_k \rangle, \langle f_1, \dots, f_\ell \rangle, \langle g_1, \dots, g_m \rangle, \langle c_1, \dots, c_n \rangle)$. Wir sagen dass sie des Typs (k, l, m, n) ist.

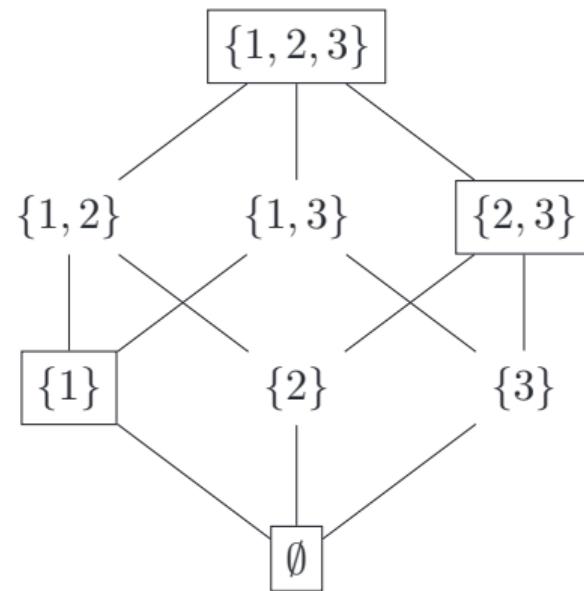
- Jede Äquivalenzrelation \equiv auf M liefert eine algebraische Struktur $(M, \equiv) = (M, \langle \equiv \rangle, \langle \rangle, \langle \rangle, \langle \rangle)$ des Typs (1, 0, 0, 0).
- Jede teilweise geordnete Menge (M, \preceq) mit einer Relation $\preceq \subseteq M \times M$ ist eine algebraische Struktur des Typs (1, 0, 0, 0).
- 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).
- Man kann jetzt definieren Isomorphismum von Strukturen, und Unterstrukturen ganz generell (siehe Skript). Diese allgemeine Definitionen sind für die Klausur nicht erforderlich. Isomorphismen und Unterstrukturen müssen jedoch in allen von uns untersuchten Sonderfällen verstanden werden.

Wir betrachten den Verband $\mathcal{O} = (\mathcal{P}(\{1, 2, 3\}), \cup, \cap)$.

- keine Unterstruktur:



- Unterstruktur:



1. Wiederholung

2. Unterverbände und Isomorphismen

3. Allgemeine algebraische Strukturen

4. Boolesche Algebren - Definition

- Sei (M, \preceq) ein Verband mit kleinstem Element \perp und größtem Element \top und sei $x \in M$.
- Ein Element $y \in M$ heißt **Komplement** von x gdw. $x \wedge y = \perp$ und $x \vee y = \top$.
- Der Verband (M, \preceq) heißt **komplementiert** gdw. für jedes $x \in M$ ein Komplement $y \in M$ von x existiert.
- Ein Verband (M, \preceq) heißt **Boolesche Algebra** gdw. er distributiv und komplementiert ist, und zusätzlich $\perp \neq \top$.
- Beispiel: $(P(X), \subseteq)$, $X \neq \emptyset$.
- Die Komplemente sind im Allgemeinen in Verbänden nicht eindeutig. Z.B. das Element ℓ im Verband M_3 hat die Komplemente m und r .

Satz. Sei (M, \preceq) ein distributiver Verband mit kleinstem Element \perp und größtem Element \top . Für jedes $x \in M$ existiert höchstens ein Komplement von x .

Beweis. Sei $x \in M$ und seien $y, z \in M$ Komplemente von x .

- Wir zeigen erst $y = y \wedge z$:

$$y = \top \wedge y = (x \vee z) \wedge y = (x \wedge y) \vee (z \wedge y) = \perp \vee (z \wedge y) = y \wedge z$$

- Aber auch $z = y \wedge z$:

$$z = \top \wedge z = (x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z) = \perp \vee (y \wedge z) = y \wedge z$$

- Also $y = y \wedge z = z$.

□

Boolesche Algebren sind als Modelle der Aussagenlogik entstanden (Komplement ist die Abstraktion der Negation).

- Als Beispiel betrachten wir der Verband der Wahrheitswerte (isomorph zu $\mathcal{P}(\{1\})$):
 $(\{0, 1\}, \{(0, 0), (0, 1), (1, 1)\})$



Satz. Sei (M, \preceq) eine Boolesche Algebra mit kleinstem Element \perp und größtem Element \top . Dann gelten

- $(x^c)^c = x$ für alle $x \in M$, und
- (Morganische Gesetze) $(x \wedge y)^c = x^c \vee y^c$ und $(x \vee y)^c = x^c \wedge y^c$ für alle $x, y \in M$.

Beweis.

- Per Definition ist $(x^c)^c$ das Komplement von x^c . Also $(x^c)^c \wedge x^c = \top$ und $(x^c)^c \vee x^c = \perp$. Durch Eindeutigkeit des Komplements es folgt $(x^c)^c = x$.

- Wir zeigen z.B. das Gesetz $(x \vee y)^c = x^c \wedge y^c$.
- Wir zeigen, dass $(x \vee y) \wedge (x^c \wedge y^c) = \perp$ und $(x \vee y) \vee (x^c \wedge y^c) = \top$. Aufgrund der Eindeutigkeit des Komplements ist dann $(x \vee y)^c = x^c \wedge y^c$ bewiesen.
- Es gilt

$$(x \vee y) \wedge (x^c \wedge y^c) = (x \wedge x^c \wedge y^c) \vee (y \wedge x^c \wedge y^c)$$

$$= (\perp \wedge y^c) \vee (\perp \wedge x^c) = \perp \vee \perp = \perp$$

- Es gilt auch

$$(x \vee y) \vee (x^c \wedge y^c) = (x \vee y \vee x^c) \wedge (x \vee y \vee y^c)$$

$$= (\top \vee y) \vee (\top \vee x) = \top \vee \top = \top$$

□

Wie Verbände, lassen sich auch Boolesche Algebren operationell charakterisieren.

Satz. Sei $(M, \sqcap, \sqcup, \cdot^*, \perp, \top)$ eine algebraische Struktur des Typs $(0, 2, 1, 2)$, so dass

- \sqcap und \sqcup assoziativ, kommutativ, distributiv und absorptiv sind, und
- Die operation \cdot^* jedes Element $x \in M$ auf sein Komplement abbildet, d.H.

$$x \sqcap x^* = \perp \quad \text{und} \quad x \sqcup x^* = \top .$$

Dann ist (M, \preceq) , mit $x \preceq y$ gdw. $x = x \sqcap y$, eine Boolesche Algebra.

Beweis. Folgt aus der Charakterisierung von Verbänden.

□



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski

Mathematisches Institut

grabowski@math.uni-leipzig.de



UNIVERSITÄT
LEIPZIG

Vorlesung 12 - Boolesche Algebren, Kommutative Gruppen

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

1. Wiederholung

2. Boolesche Algebren - Isomorphiesatz von Stone

3. Kommutative Gruppen

- Ein Verband (M, \preceq) heißt **Boolesche Algebra** gdw. er distributiv und komplementiert ist, und zusätzlich $\perp \neq \top$.
- Beispiel: $(P(X), \subseteq)$, $X \neq \emptyset$.

Satz. Sei $(M, \sqcap, \sqcup, \cdot^*, \perp, \top)$ eine algebraische Struktur des Typs $(0, 2, 1, 2)$, so dass

- \sqcap und \sqcup assoziativ, kommutativ, distributiv und absorptiv sind, und
- Die operation \cdot^* jedes Element $x \in M$ auf sein Komplement abbildet, d.H.

$$x \sqcap x^* = \perp \quad \text{und} \quad x \sqcup x^* = \top .$$

Dann ist (M, \preceq) , mit $x \preceq y$ gdw. $x = x \sqcap y$, eine Boolesche Algebra.

1. Wiederholung

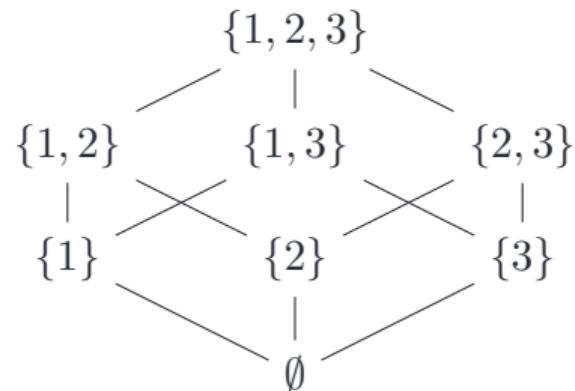
2. Boolesche Algebren - Isomorphiesatz von Stone

3. Kommutative Gruppen

- Wir wenden uns nun zu dem wichtigsten Ergebnis über endliche Boolesche Algebren:
Jede endliche Boolesche Algebra ist isomorph zu $\mathcal{P}(A)$, wo A ist eine endliche Menge.
- Ein Element $x \in M \setminus \{\perp\}$ ist ein **Atom** gdw. für alle $y \in M$ mit $y \preceq x$ gilt $y \in \{\perp, x\}$
- Atome sind also die direkten Nachbarn des kleinsten Elements \perp im Hasse-Diagramm, und die minimalen Elemente in $M \setminus \{\perp\}$.
- Beispiel. Die Boolesche Algebra der Wahrheitswerte hat nur das Atom 1.



- Beispiel. Die Potenzmenge von $M = \{1, 2, 3\}$ hat die Atome $\{1\}$, $\{2\}$ und $\{3\}$.



Satz. Sei (M, \preceq) eine endliche Boolesche Algebra.

- Für jedes $m \in M$ und jedes Atom $a \in M$, gilt $a \wedge m \in \{\perp, a\}$
- Für alle Atome $a, b \in M$ mit $a \neq b$, gilt $a \wedge b = \perp$
- Für jedes $m \in M \setminus \{\perp\}$ existiert ein Atom $a \in M$ mit $a \preceq m$.

Beweis.

- Wir haben $a \wedge m \preceq a$. Da a Atom ist, gilt $a \wedge m \in \{\perp, a\}$.
- Wenn a und b Atome sind, dann folgt $a \wedge b \preceq a$ und $a \wedge b \preceq b$.
Also $a \wedge b \in \{\perp, a\}$ und $a \wedge b \in \{\perp, b\}$. Wegen $a \neq b$ gilt $a \wedge b = \perp$.

Noch zu beweisen:

- Für jedes $m \in M \setminus \{\perp\}$ existiert ein Atom $a \in M$ mit $a \preceq m$.
- Da M ist endlich, finden wir eine Kette

$$m = m_0 > m_1 > m_2 > m_3 > \dots$$

mit der Eigenschaft dass die einzige Elemente $x \in M$ mit $m_i \geq x \geq m_{i+1}$ sind m_i und m_{i+1} .

Da M ist endlich, die Kette muss mit \perp terminieren, und das letzte Element anders als \perp ist ein Atom mit der gewünschten Eigenschaft. □

Satz. (Isomorphiesatz von Stone) Sei (M, \leq) eine endliche Boolesche Algebra und sei A die Menge von Atomen von M . Dann sind (M, \leq) und $(\mathcal{P}(A), \subseteq)$ isomorph. Der Isomorphismus schickt $m \in M$ auf die Menge $A_m \subset A$ von Atomen a mit $a \leq m$.

Beweis.

- Wir müssen zeigen, dass die Abbildung $m \mapsto A_m$ eine ordnungserhaltende Bijektion ist.
 - ▶ Die Ordnungserhaltung ist klar: wenn $m \leq n$, dann liegen alle Atome, die unter m liegen, auch unter n , also $A_m \subseteq A_n$.
- Für die Injektivität reicht es zu zeigen, dass $m = \sup A_m$. Wir zeigen dies zunächst für $m := \top$. Offensichtlich ist A_{\top} die Menge aller Atome.
 - ▶ Sei $s := \sup A_{\top}$. Wenn $s \neq \top$ dann $s^c \neq \perp$, also es existiert ein Atom $a \leq s^c$. Aber dann $a \leq s \wedge s^c$, was ein Widerspruch ist.

- Zeigen wir jetzt für beliebige m , dass $m = \sup A_m$.
 - Seien a_1, \dots, a_k alle Atome von M . Wir haben

$$m = \top \wedge m = (a_1 \vee \dots \vee a_k) \wedge m = (a_1 \wedge m) \vee \dots \vee (a_k \wedge m).$$
 - Jedes Element $a_i \wedge m$ ist entweder \perp (wenn a_i ist nicht unten m), oder a_i (wenn a_i ist unten m).
 - Also $(a_1 \wedge m) \vee \dots \vee (a_k \wedge m)$ ist genau gleich dem Infimum der Atome, die unter m liegen.
- Für die Surjektivität reicht es zu zeigen, dass, wenn X eine Menge von Atomen ist, dann für $m := \sup X$ gilt $A_m = X$.
 - Offensichtlich gilt $X \subseteq A_m$. Nehmen wir an, dass es existiert $a \in A_m \setminus X$. Wir haben $m = \sup X = \sup A_m$. Insbesondere $\sup X \geq a$.
 - Es folgt $a = \sup X \wedge a = (x_1 \wedge a) \vee (x_2 \wedge a) \vee \dots \vee (x_l \wedge a)$. Aber $x_i \wedge a \in \{\perp, x_i\}$. Da $a \notin X$, es folgt $x_i \wedge a = \perp$, und deswegen $a = \perp$. Das ist ein Widerspruch.



Satz. (Isomorphiesatz von Stone) Sei (M, \leq) eine endliche Boolesche Algebra und sei A die Menge von Atomen von M . Dann sind (M, \leq) und $(\mathcal{P}(A), \subseteq)$ isomorph.

- Gilt dieser Satz für unendliche Boolsche Algebren?
- Nein. Sei $M \neq \emptyset$ eine unendliche Menge und

$$E := \{X \in \mathcal{P}(M) \mid X \text{ endlich}\} \cup \{X \in \mathcal{P}(M) \mid M \setminus X \text{ endlich}\}$$

- ▶ E ist eine Boole'sche unter-Algebra von $\mathcal{P}(M)$, da die Operationen \vee , \wedge , und Komplement die Elemente von E erhalten.
- ▶ Wenn M abzählbar ist, dann ist auch E abzählbar.
- ▶ Aber $\mathcal{P}(X)$ kann nicht abzählbar sein. Es folgt dass E kann nicht isomorph zu $\mathcal{P}(X)$ sein.

Satz. (Isomorphiesatz von Stone) Sei (M, \leq) eine endliche Boolesche Algebra und sei A die Menge von Atomen von M . Dann sind (M, \leq) und $(\mathcal{P}(A), \subseteq)$ isomorph.

- Dieser Satz vermittelt uns ein gutes konzeptionelles Verständnis der Aussagenlogik.
- Er motiviert auch die grundlegenden Definitionen der Wahrscheinlichkeitstheorie: In der Wahrscheinlichkeitstheorie beginnen wir mit einer Menge X von atomaren Ereignissen und jedes der Ereignisse x hat eine Wahrscheinlichkeit p_x .

1. Wiederholung

2. Boolesche Algebren - Isomorphiesatz von Stone

3. Kommutative Gruppen

- Kommutative Gruppen sind eine Abstraktion von $(\mathbb{Z}, +)$.
 - ▶ Wir haben ein spezielles Element 0 mit der Eigenschaft $x + 0 = x$ für alle $x \in \mathbb{Z}$.
 - ▶ Für jedes $x \in \mathbb{Z}$ können wir ein Element y finden, so dass $x + y = 0$ (“additive Inverse von x ”),
 - ▶ Für alle x, y haben wir $x + y = y + x$.
- Eine algebraische Struktur (M, \oplus, \cdot^*, e) des Typs $(0, 1, 1, 1)$ ist eine **kommutative** oder auch **Abelsche Gruppe** gdw. für alle $x, y, z \in M$ gilt:
 - ▶ $x \oplus (y \oplus z) = (x \oplus y) \oplus z$, (Assoziativität)
 - ▶ $x \oplus y = y \oplus x$, (Kommutativität)
 - ▶ $e \oplus x = x$, (neutrales Element)
 - ▶ $x \oplus x^* = e$. (inverse Elemente)

Beispiele von kommutativen Gruppen.

- $(\mathbb{Z}, +, (-\cdot), 0)$,
 - ▶ Auch $(\mathbb{Q}, +, (-\cdot), 0)$, $(\mathbb{R}, +, (-\cdot), 0)$,
- $(\mathbb{Q} \setminus \{0\}, \cdot, \cdot^{-1}, 1)$
 - ▶ Auch $(\mathbb{R} \setminus \{0\}, \cdot, \cdot^{-1}, 1)$
- $(\mathbb{N}, +, (-\cdot), 0)$ ist keine kommutative Gruppe, denn es gibt kein $n \in \mathbb{N}$, so dass $1 + n = 0$).
 - ▶ $(\mathbb{Q}, \cdot, \cdot^{-1}, 1)$ ist auch keine kommutative Gruppe, denn es gibt kein $q \in \mathbb{Q}$, so dass $0 \cdot q = 1$).

Wir schreiben am meistens $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, etc. da die inverse Operation und 0 sind eindeutig bestimmt.

- D.H. wir können die kommutative Gruppen auch wie folgt definieren. $(M, +)$ ist eine kommutative Gruppe, gdw.
 - ▶ für alle $x, y, z \in M$ gilt $(x + y) + z = x + (y + z)$
 - ▶ für alle $x, y \in M$ gilt $x + y = y + x$
 - ▶ es gibt $0 \in M$, so dass für alle $x \in M$ gilt $x + 0 = x$
 - ▶ für alle $x \in M$ gibt es y so dass $x + y = 0$.
- Kein Problem mit der Wohldefiniertheit im vierten Punkt: Die ersten drei implizieren, dass 0 eindeutig ist: $0 = 0 + 0' = 0'$.
- Die inverse ist auch eindeutig: Wenn $0 = x + y = x + z$ dann
 $z = 0 + z = (y + x) + z = y + (x + z) = y$.

Wir werden häufig das folgende Lemma verwenden.

Lemma. Sei $(M, +)$ eine kommutative Gruppe und $x, y \in M$. Dann existiert genau ein $z \in M$, so dass $x + z = y$.

Beweis. Wir definieren $z := (-x) + y$. Dann

$$x + z = x + ((-x) + y) = (x + (-x)) + y = 0 + y = y.$$

Für Eindeutigkeit, wenn $x + z = x + z'$ dann auch $(-x) + (x + z) = (-x) + (x + z')$, aber mit Assoziativität es folgt $z = z'$. □

- Im Beweiss haben wir auch die folgende Eigenschaft gesehen: in jeder kommutativen Gruppe wenn wir Elemente $m, x, y \in M$ mit $m + x = m + y$ haben, dann gilt $x = y$.
Wir werden häufig die Notation $x - y$ für $x + (-y)$ benutzen.
- Üblicherweise wird die Kardinalität einer Gruppe als **Ordnung der Gruppe** bezeichnet.

Wenn wir zwei Gruppen $(A, +_A)$ und $(B, +_B)$ haben, können wir auch das kartesische Produkt $A \times B$ als eine Gruppe betrachten. Die Operation ist $(a_1, b_1) + (a_2, b_2) := (a_1 +_A a_2, b_1 +_B b_2)$.

- Beispiele: $(\mathbb{R}^2, +)$, $(\mathbb{R}^n, +)$, $(\mathbb{R} \text{ times } \mathbb{Z}, +)$

Die Gruppen der Residuen modulo n

- Die Gruppe der Residuen Modulo n ist die Gruppe \mathbb{Z}/n mit Elementen $\{0, 1, 2, \dots, n - 1\}$. Die operation ist “Addition modulon n ”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \pmod{5}$.
- Jede endliche okmmutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.
 - ▶ Z.B. $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.
 - ▶ Dies ist ein sehr wichtiger Satz, der normalerweise in einem Kurs über lineare Algebra bewiesen wird. Wir werden ihn in diesem Kurs nicht beweisen.

Isomorphismen und Homomoprismen

- Ein Isomorphismus von Gruppen $(M, +)$ und $(N, +)$ ist eine Bijektion $\varphi: M \rightarrow N$, so dass $\varphi(a + b) = \varphi(a) + \varphi(b)$ für alle $a, b \in M$ gilt.
 - ▶ Daraus folgt, dass $\varphi(0_M) = 0_N$, $\varphi(-x) = -\varphi(x)$ für alle $x \in M$.
- Führen wir nun einen weiteren nützlichen Begriff ein: Gruppenhomomoprismus: Ein Homomorphismus von $(M, +)$ zu $(N, +)$ ist eine Funktion $\varphi: M \rightarrow N$, so dass für alle $a, b \in M$ gilt $\varphi(a + b) = \varphi(a) + \varphi(b)$ und außerdem $\varphi(0_M) = 0_N$ und $\varphi(-x) = -\varphi(x)$ für alle $x \in M$.
- Die Eigenschaften $\varphi(0_M) = 0_N$ und $\varphi(-x) = -\varphi(x)$ müssen wir nicht verlangen, sie folgen automatisch aus $\varphi(a + b) = \varphi(a) + \varphi(b)$.



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski

Mathematisches Institut

grabowski@math.uni-leipzig.de



UNIVERSITÄT
LEIPZIG

Vorlesung 13 - Kommutative Gruppen

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

1. Wiederholung

2. Untergruppen

3. Mehr über \mathbb{Z}/n

4. Ringe und Körper

Kommutative Gruppen - zwei äquivalente Definitionen. Die die wir am meisten nutzen:
 $(M, +)$ ist eine kommutative Gruppe, gdw.

- ▶ für alle $x, y, z \in M$ gilt $(x + y) + z = x + (y + z)$
- ▶ für alle $x, y \in M$ gilt $x + y = y + x$
- ▶ es gibt $0 \in M$, so dass für alle $x \in M$ gilt $x + 0 = x$
- ▶ für alle $x \in M$ gibt es y so dass $x + y = 0$.

- Die Gruppe der Residuen Modulo n ist die Gruppe \mathbb{Z}/n mit Elementen $\{0, 1, 2, \dots, n - 1\}$. Die operation ist “Addition modulon n ”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \pmod{5}$.
- Jede endliche kommutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.
 - ▶ Z.B. $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.
- Ein Homomorphismus von $(M, +)$ zu $(N, +)$ ist eine Funktion $\varphi: M \rightarrow N$, so dass für alle $a, b \in M$ gilt $\varphi(a + b) = \varphi(a) + \varphi(b)$ und außerdem $\varphi(0_M) = 0_N$ und für alle $x \in M$ gilt $\varphi(-x) = -\varphi(x)$

- Beispiele von Gruppenhomomorphismen:

- ▶ $f: \mathbb{Z} \rightarrow \mathbb{Z}/n$, $f(x) := x \pmod n$.
- ▶ $f: \mathbb{Z}/m \rightarrow \mathbb{Z}/n$, wenn $n \mid m$. $f(x) := x \pmod n$.
- ▶ $n \mid m$ ist nötig um einen Homomorphismus zu haben. Z.B. $f: \mathbb{Z}/5\mathbb{Z} \rightarrow \mathbb{Z}/3$ mit $f(x) := x \pmod 3$ ist kein Homomorphismus: $f(3 + 3) = f(6) = f(1) = 1$, aber $f(3) + f(3) = 0 + 0 = 0$.
- ▶

1. Wiederholung

2. Untergruppen

3. Mehr über \mathbb{Z}/n

4. Ringe und Körper

Sei $(M, +)$ eine kommutative Gruppe. $N \subset M$ ist eine Untergruppe, wenn $0 \in N$, und für alle $x, y \in N$ gilt $x + y \in N$, und für alle $x \in N$ gilt $-x \in N$.

Beispiele

- $\{0_M\}$ ist die “triviale Untergruppe” von M .
- $\mathbb{Z} \subset \mathbb{Q}$ ist eine Untergruppe
- $\mathbb{N} \subset \mathbb{Q}$ ist keine Untergruppe
- $n\mathbb{Z} \subset \mathbb{Z}$ ist eine Untergruppe, wobei $n\mathbb{Z} := \{nx: x \in \mathbb{Z}\}$.
- \mathbb{Z} ist isomorph zu vielen verschiedenen Untergruppen von \mathbb{Z}^2 , zum Beispiel $\{(x, 0): x \in \mathbb{Z}\}, \{(x, x): x \in \mathbb{Z}\}, \{(5x, 7x): x \in \mathbb{Z}\}$.
- Sei $k, n \in \mathbb{N}$ mit $k \mid n$. Dann $\{0, k, 2k, \dots, n - k\}$ ist eine Untergruppe von $\mathbb{Z}/n := \{0, 1, 2, \dots, n\}$. Diese Untergruppe ist isomorph zu $\mathbb{Z}/\frac{n}{k}$.

1. Wiederholung

2. Untergruppen

3. Mehr über \mathbb{Z}/n

4. Ringe und Körper

- Wir haben \mathbb{Z}/n als $\{0, 1, 2, \dots, n - 1\}$ definiert, mit addition modulo n .
- Etwas abstraktere Perspektive:
 - ▶ wir haben eine Äquivalenzrelation auf \mathbb{Z} , gegeben als $x \equiv y$ gdw. $n \mid x - y$.
- Die Klassen dieser Äquivalenzrelation sind $\{\dots, -n, 0, n, 2n, \dots\}$, $\{\dots, 1, n + 1, \dots\}, \dots, \{\dots - 1, n - 1, \dots\}$
- Wir können alternativ \mathbb{Z}/n als die Menge allen Äquivalenzklassen definieren. Also $\mathbb{Z}/n := \mathbb{Z}/\equiv$.
 - ▶ Die Addition ist dann definiert als $[x] + [y] := [x + y]$.
 - ▶ Der Homomorphismus $\mathbb{Z} \rightarrow \mathbb{Z}/n$ ist dann definiert als $f(x) := [x]$.

- Sei nun p eine Primzahl. Wir können die folgende Gruppe betrachten:
 $\mathbb{Z}/p^* := \{1, 2, \dots, p - 1\}$ aber mit Multiplikation, d.h. die Operation ist $x \oplus y := x \cdot \text{mod } p$.
 - ▶ In $\mathbb{Z}/7^*$ haben wir zum Beispiel $3 \cdot 4 \equiv 5$.
- Warum ist es eine Gruppe?
 - ▶ Assoziativitat, Kommutativitat - klar
 - ▶ Neutrales Element: 1. $1 \cdot x \equiv x \pmod{p}$.
 - ▶ Inversen: hier verwenden wir, dass p eine Primzahl ist: die Aufgabe ist folgende: fur ein gegebenes $a \in \mathbb{Z}/p^*$ mussen wir $b \in \mathbb{Z}/p^*$ finden, so dass $xy \equiv 1 \pmod{p}$.
 - ▶ Betrachten wir die Funktion $f: \mathbb{Z}/p^* \rightarrow \mathbb{Z}/p^*$, die als $f(x) := ax$ definiert ist.
 - ▶ Diese Funktion ist injektiv: Wenn $ax \equiv ay$ dann $a(x - y) \equiv 0 \pmod{p}$, d.h. $p \mid a(x - y)$. Also entweder $p \mid a$ oder $p \mid (x - y)$, aber das ist nicht moglich.
 - ▶ Somit ist f auch surjektiv, und somit $ab \equiv 1$ fur irgendein b .

- In Anwendungen ist es äußerst wichtig, diese “multiplikative Inversen modulo p ” zu berechnen.
- Der Beweis, den wir gegeben haben, liefert keinen effektiven Algorithmus.
 - Wenn p 1000 Ziffern hat und wir ein Element $a \in \mathbb{Z}/p^*$ invertieren wollen, dann müssten wir ungefähr $p \approx 10^{1000}$ verschiedene Elemente von \mathbb{Z}/p^* überprüfen, um die Inverse zu finden.
- Aus diesem Grund geben wir einen anderen, etwas komplizierteren Beweis, dass multiplikative Inverse modulo p existieren, der einen effektiven Algorithmus liefert.

- Wir führen den euklidischen Algorithmus durch, mit p und a , das wir invertieren wollen.
 - ▶ $p = q_1a + r_1$
 - ▶ $a = q_2r_1 + r_2$
 - ▶ $r_1 = q_3r_2 + r_3$
 - ▶ \dots
 - ▶ $r_{k-2} = q_kr_{k-1} + r_k$
 - ▶ $r_{k-1} = q_{k+1}r_k.$
- Dann ist r_k gleich zu $\text{ggt}(p, a)$, also 1.
- Wenn wir nach oben gehen, erhalten wir die *Bezout-Identität*: $xp + ya = r_k = 1$ für einige x, y . Jetzt ist y die multiplikative Inverse von a .
- Die Anzahl der Zeilen im euklidischen Algorithmus ist vergleichbar mit $\log(p)$.

- Wenn $n \mid m$, dann haben wir einen surjektiven Homomorphismus $\varphi: \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, gegeben durch $\varphi(a) := a \pmod{n}$.
- Der folgende Satz ist als “Chinesischer Restsatz” bekannt.

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

- Dieser Satz ist extrem häufig benutzt. Anders gesagt: Gegeben sind $k, l \in \mathbb{Z}$. Wir wollen die Gleichungs-system $x \equiv k \pmod{a}, x \equiv l \pmod{b}$ lösen.

Satz. Seien a, b positive teilerfremde ganze Zahlen und $n := ab$. Dann sind die Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ isomorph.

Beweis. Wir betrachten den Homomorphismus $\varphi: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, der als $\varphi(x) := (x \bmod a, x \bmod b)$ definiert ist. Wir müssen zeigen, dass φ bijektiv ist.

- Da die Mengen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ die gleiche Kardinalität haben, genügt es zu prüfen, dass φ injektiv ist.
- Dazu nehmen wir an, dass $x, y \in \{0, \dots, n-1\}$ so sind, dass $\varphi(x) = \varphi(y)$ und nehmen wir widerspruchshalber $x < y$ an.
- Dann $a \mid y - x$ und $b \mid y - x$. Da aber a und b teilfremd sind, bedeutet dies, dass $n \mid y - x$. Widerspruch zu der Tatsache, dass $0 < y - x < n$.

□

- Was für eine Gruppe ist \mathbb{Z}/p^* ? Ist sie zu $\mathbb{Z}/(n - 1)$ isomorph?

1. Wiederholung

2. Untergruppen

3. Mehr über \mathbb{Z}/n

4. Ringe und Körper

- Natürlich gibt es für Zahlenmengen wie \mathbb{Z} oder \mathbb{Q} zwei Operationen, nämlich Addition und Multiplikation. Dies führt uns zum Begriff des *Rings* (oder “kommutativen Rings mit Eins”).
- Ein Ring ist eine algebraische Struktur $(M, +, \cdot)$, so dass
 - ▶ $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
 - ▶ \cdot ist assoziativ und kommutativ
 - ▶ es gibt $1_M \in M$ so dass für alle $m \in M$ gilt $1_M \cdot m = m$ (daraus folgt, dass 1_M eindeutig ist).
 - ▶ für alle $a, b, c \in M$ gilt $a \cdot (b + c) = a \cdot b + a \cdot c$.

- Wie bei Gruppen könnten wir Ringe als $(M, +, \cdot, 0_M, \cdot, \cdot^{-1}, 1_M)$ mit geeigneten Axiomen definieren.
- $(\mathbb{Z}, +, \cdot)$ ist ein Ring, $(\mathbb{Q}, +, \cdot)$ ist ein Ring
- In einem Ring $(M, +, \cdot)$ haben wir $0 \cdot x = 0$ für alle x .
 - ▶ Tatsächlich: $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, und da $(M, +)$ eine kommutative Gruppe ist, folgt $0 \cdot x = 0$.

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
- In einem Körper $(M, +, \cdot)$ gilt, dass $xy = 0$ impliziert, dass $x = 0$ oder $y = 0$.
 - In der Tat, wenn $x \neq 0$ dann können wir schreiben $y = x^{-1}xy = x^{-1}0 = 0$.
- Wenn A und B Ringe sind, dann ist $A \times B$ ebenfalls ein Ring. Wenn A und B jedoch Körper sind, dann ist $A \times B$ kein Körper: wir haben $(1_A, 0_B) \cdot (0_A, 1_B) = (0_A, 0_B)$

Beispiel

$\mathbb{Z}/m\mathbb{Z}$ ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$ mit $[a], [b] \neq [0]$ so finden, dass $[a][b] = 0$. Wenn also m nicht prim ist, dann ist \mathbb{Z}/m kein Körper.

Lemma. $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper gdw. p eine Primzahl ist.

Beweis.

- Wir haben im obigen Beispiel gesehen, dass, wenn p keine Primzahl ist, $\mathbb{Z}/p\mathbb{Z}$ kein Körper ist.
- Wir haben auch gesehen dass wenn p eine Primzahl, dann die multiplikative Inversen existieren, also \mathbb{Z}/p ist ein Körper. □

Der Körper \mathbb{Q} und die Körper $\mathbb{Z}/p\mathbb{Z}$ werden als **Primkörper** bezeichnet. Jeder Körper enthält ein Primkörper.



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski

Mathematisches Institut

grabowski@math.uni-leipzig.de



UNIVERSITÄT
LEIPZIG

Vorlesung 14 - Ringe, Körper, Polynome

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

Übersicht

1. Wiederholung
2. Polynome
3. Abstrakter Sichtpunkt - Ideale und Faktorringe

1. Wiederholung

2. Polynome

3. Abstrakter Sichtpunkt - Ideale und Faktorringe

- Ein Ring ist eine algebraische Struktur $(M, +, \cdot)$, so dass
 - ▶ $(M, +)$ ist eine kommutative Gruppe (genannt additive Gruppe des Rings)
 - ▶ \cdot ist assoziativ und kommutativ
 - ▶ es gibt $1_M \in M$ so dass für alle $m \in M$ gilt $1_M \cdot m = m$ (daraus folgt, dass 1_M eindeutig ist).
 - ▶ für alle $a, b, c \in M$ gilt $a \cdot (b + c) = a \cdot b + a \cdot c$.

- Körper - ein Ring $(M, +, \cdot)$ so dass für jedes $x \in M$ mit $x \neq 0_M$ existiert $y \in M$ mit $xy = 1_M$.
- Äquivalent: $(M, +, \cdot)$ ist ein Körper, wenn $(M \setminus \{0_M\}, \cdot)$ eine Gruppe ist.
- Beispiele für Körper: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
- In einem Körper $(M, +, \cdot)$ gilt, dass $xy = 0$ impliziert, dass $x = 0$ oder $y = 0$.
 - In der Tat, wenn $x \neq 0$ dann können wir schreiben $y = x^{-1}xy = x^{-1}0 = 0$.
- Wenn A und B Ringe sind, dann ist $A \times B$ ebenfalls ein Ring. Wenn A und B jedoch Körper sind, dann ist $A \times B$ kein Körper: wir haben $(1_A, 0_B) \cdot (0_A, 1_B) = (0_A, 0_B)$

Beispiel

\mathbb{Z}/m ist ein Ring. Wenn m nicht prim ist, kann man $[a], [b] \in \mathbb{Z}/m$ mit $[a], [b] \neq [0]$ so finden, dass $[a][b] = [0]$. Wenn also m nicht prim ist, dann ist \mathbb{Z}/m kein Körper.

Lemma. \mathbb{Z}/p ist ein Körper gdw. p ist eine Primzahl.

- Der Körper \mathbb{Q} und die Körper \mathbb{Z}/p werden als **Primkörper** bezeichnet. Jeder Körper enthält ein Primkörper.
- Gibt's andere als \mathbb{Z}/p endliche Körper?

1. Wiederholung

2. Polynome

3. Abstrakter Sichtpunkt - Ideale und Faktorringe

- Sei $(M, +, \cdot)$ ein Ring, und sei $a_0, \dots, a_n \in M$ mit $a_n \neq 0$. Wir assoziieren mit dieser endlichen Folge ein Polynom:

$$p = a_0 + a_1 X + \dots + a_n X^n.$$

- Dieses Polynom p definiert eine Funktion $p: M \rightarrow M$. Für alle $x \in M$:

$$p(x) = a_0 + a_1 x + \dots + a_n x^n \in M.$$

- Wir schreiben auch $\text{grad}(p) = n$. Das **Nullpolynom** p mit $p = 0$ hat kein Grad oder Grad $-\infty$. Ein Element $x \in M$ ist **Nullstelle** von p gdw. $p(x) = 0$.
- Die Menge von allen Polynomen mit Koeffizienten aus M wird mit $M[X]$ bezeichnet.

- Im Körper $\mathbb{Z}/5$ betrachten wir das Polynom $X^2 + 4X + 2$. Es gilt

$$p(2) \equiv 2 + (4 \cdot 2) + (2 \cdot 2) \equiv 2 + 3 + 4 \equiv 4$$

- Für die Bestimmung der Nullstellen von p berechnen wir:

- ▶ $p(0) \equiv 2$,
- ▶ $p(1) \equiv 2 + 4 + 1 \equiv 2$,
- ▶ $p(2) \equiv 4$,
- ▶ $p(3) \equiv 2 + 2 + 4 \equiv 3$ und
- ▶ $p(4) \equiv 2 + 1 + 1 \equiv 4$.

Offenbar hat p keine Nullstellen.

- Wie schnell kann man $p(a)$ berechnen?
 - ▶ Wie viele Operationen $+$ und \cdot werden gebraucht? .
 - ▶ Nicht mehr als: $(n + 1)$ (für $a_n a^n$) $+ n$ (für $a_{n-1} a^{n-1}$...
 - ▶ Also nicht mehr als $\frac{(n+1)(n+2)}{2} + n$. D.h. Cn^2 .
 - ▶ kann man einen besseren Algorithmus finden?

Lemma. [Horner-Schema] Sei $(M, +, \cdot)$ ein Ring und sei $p = a_0 + a_1 X + \dots + a_n X$ ein Polynom von einem Grad $n \geq 0$. Dann gilt für alle $x \in M$

$$p(x) = a_0 + x \cdot (a_1 + x \cdot (a_2 + \dots + x a_n))$$

- Mit Induktion beweisen wir dass mit Horner-Schema brauchen wir nur $2n$ Operationen. Also $C_1 \cdot n$. Deutlich besser als $C \cdot n^2$.

Satz. (Polynomdivision) Sei $(M, +, \cdot)$ ein Körper. Seien p und q Polynome mit $\text{grad}(q) \geq 0$. Dann existieren Polynome t und r mit

$$p(X) = t(X) \cdot q(X) + r(X)$$

und $\text{grad}(r) < \text{grad}(q)$.

- Die Polynome t und r erhält man per Polynomdivision.

$$\begin{array}{r} & x^3 & -x-2 \\ \hline x^2+1) & \overline{x^5 & -2x^2+4x+7} \\ & \underline{-x^5-x^3} \\ & -x^3-2x^2+4x \\ & \underline{x^3 & +x} \\ & -2x^2+5x+7 \\ & \underline{2x^2 & +2} \\ & 5x+9 \end{array}$$

- $x^5 - 2x^2 + 4x + 7 = (x^3 - x - 2)(x^2 + 1) + (5x + 9)$

$$\begin{array}{r}
 \frac{\frac{1}{2}x^3}{2x^2 + 1} \\
 -\frac{1}{4}x - 1 \\
 \hline
 -x^5 - 2x^2 + 4x + 7 \\
 \hline
 -x^5 - \frac{1}{2}x^3 \\
 -\frac{1}{2}x^3 - 2x^2 + 4x \\
 \hline
 \frac{1}{2}x^3 + \frac{1}{4}x \\
 -2x^2 + \frac{17}{4}x + 7 \\
 \hline
 2x^2 + 1 \\
 \hline
 \frac{17}{4}x + 8
 \end{array}$$

- In \mathbb{Q} : $x^5 - 2x^2 + 4x + 7 = (\frac{1}{2}x^3 - \frac{1}{4}x - 1)(2x^2 + 1) + (\frac{17}{4}x + 8)$
- In $\mathbb{Z}/5$: $x^5 - 2x^2 + 4x + 2 \equiv (3x^3 + x - 1)(2x^2 + 1) + (3x + 3)$

- Folgerung: Wenn M ist ein Körper, dann $M[X]$ hat Euklidischer Algorithmus.
 - ▶ Wenn $p, q \in M[X]$ und $\text{ggt}(p, q) = 1$, dann existieren polynome a, b mit $ap + bq = 1$. ($\text{ggt}(p, q)$ ist nur bis zur Multiplikation mit einer Konstante nicht gleich Null definiert!)
 - ▶ Z.B.
 - ▶ $p = x^4 - 2x^2 - 3x - 2$ $q = x^3 + 4x^2 + 4x + 1$
 - ▶ Euklidischer Algorithmus: $\text{ggt}(p, q) = x + 1$
 - ▶ Bezout-identität:

$$x + 1(5x^2/22 - 3x/11 - 3/11)p + (-5x/22 - 7/11)q$$

- Wir sagen, dass ein Polynom f irreduzibel ist, wenn es mindestens den Grad 1 hat, und seine einzigen Teiler von der Form Cf , C sind, wobei $C \in M$.
- Folgerung: “Unreduzierbare Polynome sind prim”
 - ▶ Das heißt, wenn $f \in M[X]$ irreduzibel ist, dann hat f die folgende Eigenschaft. Wenn $f \mid ab$ und $f \nmid a$, dann $f \mid b$.
 - ▶ Beweis. Wir schreiben $sf + ta = 1$, dann erhalten wir $sfb + tab = b$, und wir erhalten, dass f die linke Seite teilt, und deshalb teilt es auch die rechte Seite.
 - ▶ Zum Beispiel: in $\mathbb{Z}/5$ das Polynom $p = X^2 + 4X + 2$ ist irreduzibel.

- Folgerung: (“Eindeutigkeit der Faktorisierung”) Wenn $f \in M[X]$, dann kann f als Produkt irreduzibler Polynome $p_1 \cdot \dots \cdot p_k$ geschrieben werden. Die Polynome p_1, \dots, p_k sind bis zur Multiplikation mit einer Konstanten eindeutig.
 - ▶ Beweis. Nehmen wir an, wir haben zwei Faktorisierungen $p_1 \cdot \dots \cdot p_k = r_1 \dots r_l$. Dann teilt p_1 das Produkt $r_1 \dots r_l$, und da p_1 irreduzibel ist, teilt p_1 also einen der Faktoren r_i . Dann können wir Induktion benutzen um die Eindeutigkeit zu zeigen.
- Folgerung: Wenn $f \in M[X]$ und $a \in M$, dann sind die folgenden äquivalent: a ist eine Wurzel von f gdw $(X - a) \mid f$.
 - ▶ In der Tat: Wir schreiben $f = q(X - a) + r$, mit $\deg r < 1$.

- Folgerung: Ein Polynom f in $M[X]$ vom Grad n hat höchstens n Wurzeln.
 - ▶ Die Polynome $(X - a)$ sind irreduzibel, wenn also a eine Wurzel von f ist, dann erscheint $(X - a)$ in der irreduziblen Faktorisierung von f . Die Behauptung folgt aus dem Vergleich der Grade.
- Für Ringe, die keine Körper sind, gilt dies nicht.
 - ▶ In $\mathbb{Z}/8$ hat das Polynom x^3 die Wurzeln 0, 2, 4, 6.

- Wir können nun Körper mit p^k Elementen konstruieren.
- Wir beginnen mit einem irreduziblen Polynom F vom Grad k . Um z.B. ein Körper mit 25 Elementen zu konstruieren, können wir mit $x^2 + x + 2$ beginnen.
- Als Elemente nehmen wir die Menge $\mathbb{Z}/5[X]/(x^2 + x + 2)$, die aus allen Polynomen vom Grad höchstens $k - 1$ besteht. In unserem Beispiel also $ux + v$, mit $u, v \in \mathbb{Z}/5$.
- Um Elemente zu multiplizieren, reduzieren wir modulo F . Zum Beispiel $(x + 3)(x + 2) \equiv x^2 + 1 \equiv -x - 3$.
 - ▶ Die Irreduzibilität von F wird benutzt, um zu zeigen, dass alle Elemente ungleich Null Inverse haben.
 - ▶ In der Tat: Wenn $g \in M[X]/(x^2 + x + 2)$, dann können wir mitte Bezout-Identität $ag + bF = 1$ für einige Polynome a, b schreiben. Dann ist a die multiplikative Inverse von g modulo F .

Satz. [Moore]

- Sei $(M, +, \cdot)$ ein endlicher Körper (auch Galois-Körper genannt). Dann existieren $n, p \in \mathbb{N}$ mit p prim, so dass $|M| = p^n$.
- Seien \mathcal{K} und \mathcal{N} endliche Körper mit gleich vielen Elementen. Dann sind \mathcal{K} und \mathcal{N} isomorph.
- Insbesondere: kein Körper mit 6 Elementen.

1. Wiederholung

2. Polynome

3. Abstrakter Sichtpunkt - Ideale und Faktorringe

- Sei $(M, +, \cdot)$ ein Ring. Wir sagen, dass $I \subset M$ ein **Ideal** ist, wenn
 - ▶ I eine Untergruppe von $(M, +)$ ist und
 - ▶ für alle $m \in M$ gilt $mI \subset I$

Beispiele

- M ist ein Ideal von M . Jedes andere Ideal heißt **echt**. Ein Ideal ist echt, wenn es 1_M nicht als Element enthält.
- $\{0\} \subset M$ ist ein Ideal.
- $n\mathbb{Z} \subset \mathbb{Z}$ ist ein Ideal für jede natürliche Zahl n .
- $fM[X] \subset M[X]$ ist ein Ideal für jedes Polynom f .

- Ist $I \subset M$ ein Ideal, so nehmen wir eine Äquivalenzrelation auf M so definiert: $a \equiv b$ gdw $a - b \in I$.
- Die Menge der Äquivalenzklassen nennen wir M/I .

Lemma. $(M/I, +, \cdot)$ wird zu einem Ring, mit $[m] \cdot [n] := [mn]$, und $[m+n] := [m+n]$.

Beweis.

- Wir überprüfen z.B., dass die Multiplikation wohldefiniert ist.
- Nehmen wir also $[m] = [m']$ und $[n] = [n']$ an, so haben wir $m - m', n - n' \in I$. Da I ein Ideal ist, haben wir auch $n(m - m'), m(n - n') \in I$. Daraus folgt, dass $n'(m - m') + m(n - n') = mn - n'm' \in I$ und somit tatsächlich $[mn] = [m'n']$. □
- Spezieller Fall: $\mathbb{Z}/5[X]/(x^2 + x + 2)$.



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski

Mathematisches Institut

grabowski@math.uni-leipzig.de