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)

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 Geschlechtstriebs, 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 befördet frische Milch", ...
- Aussagenkombination:
  - "L befördet frische Milch" oder "L befördet frisches Fleich"
  - Wenn "Es ist Sonntag" und ("L befördet frische Milch" oder "L befördet frisches Fleich") 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 = wahr und 0 = 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	$\neg A$	$A \wedge B$	$A \vee B$	$A \to B$	$A \leftrightarrow B$
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 $A \to B$ 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 $A_1, \ldots, A_n$
- Auflistung aller 2^n Wahrheitswertbelegungen für $A_1, \ldots, A_n$

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: $(A \wedge B) \to A$ eine Tautologie? (d.H. wir zeigen dass diese Formel gilt immer, unabhänging davon was A and B sind)

A	B	$A \wedge B$	$(A \wedge B) \to A$
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 $(A \to B) \to C$ und $A \to (B \to C)$ sind nicht äquivalent.

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

Die Aussagen $A \to B$ and $\neg A \vee B$ sind äquivalent. Man nennt diese Äquivalenz "Elimination von $\to$". Die Wahrheitstabelle für die Aussage $A \to B$ 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. überprúfen 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 "$\rightarrow$": $(A \rightarrow B) \rightarrow C$ and $A \rightarrow (B \rightarrow C)$ 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 $\vee$
$A \to B$	$\neg A \vee B$	Elimination von $\to$
$A \leftrightarrow B$	$(A \to B) \wedge (B \to A)$	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 $A, B, C, \ldots$ 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. $(A \wedge B) \to A$.

- 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 $A \to B$ 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 verschieden 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 Formelm 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

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

- Gemäß der Eliminationsregel sind die Formeln $A \iff B$ und $A \to B \wedge B \to A$ 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 $A \to B$ und $B \to A$.

- 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 $(A \to B) \wedge (B \to A)$ 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.

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

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

Beweis.

- $A \to B$ ist äquivalent zu $\neg A \vee B$ (Elimination $\to$)
- $\neg A \vee B$ 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 $\neg B \to \neg A$ (Elimination $\to$)

> ***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. $\square$

Satz (Modus Ponens). *Die Formel* $(A \wedge (A \to B)) \to B$ *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 $F = \cdots \to B$ wahr.
- Falls B falsch ist, dann ist entweder
  - (i) A wahr, womit $A \wedge (A \to B)$ falsch ist oder
  - (ii)A falsch, womit $A \wedge (A \to B)$ auch falsch ist. In beiden Unterällen ist also $F' = A \wedge (A \to B)$ falsch und damit $F = F' \to B$ 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 jdem 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: $((A \to C) \land (B \to C) \land (A \lor B)) \to C$.

Satz (Kettenschluss). *Die Formel* $((A \to B) \land (B \to C)) \to (A \to C)$ *ist eine Tautologie.*

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

Fallunterscheidung:

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

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

$$((\neg A \to B) \land (\neg A \to \neg B)) \to A$$

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

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

  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. $\square$
- 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 $\neg A \to B$ und $\neg A \to \neg B$ 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

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 tatsätzlich N die Negation von P ist.

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

- Quantoren (oder Qunatifikatoren) 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

$$\forall n\Big(\text{QuadratGerade}(n) \to \text{Gerade}(n)\Big),$$

wenn wir explizit den Bereich der ganzen Zahlen betrachten.

- Oder wir könnten auch schreiben

$$\forall n\Big(\text{GanzeZahl}(n) \to (\text{QuadratGerade}(n) \to \text{Gerade}(n))\Big),$$

wobei 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

$$\neg\exists x\big(\mathit{Rat}(x) \wedge \mathit{QuadratGleich2}(x)\big),$$

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

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

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

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 $\exists n P(n)$, 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:

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

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 $m > n$. $\square$

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 $A \to B$ kann ein Beweis für die Aussage $\neg B \to \neg A$ 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.
- $e = 1 + \frac{1}{2!} + \ldots$ 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 $\alpha := N!(1 + \frac{1}{2!} + \ldots + \frac{1}{N!})$. Dies ist eine natürliche Zahl.
  - ▶ Wir können es aber auch schreiben als $\alpha = N!(e - \frac{1}{(N+1)!} - \frac{1}{(N+2)!} - \ldots) = N!(\frac{a}{b} - \frac{1}{(N+1)!} - \frac{1}{(N+2)!} - \ldots)$
  - ▶ Nun ist $N! \cdot \frac{a}{b}$ eine ganze Zahl, und $N!(\frac{1}{(N+1)!} + \ldots) = \frac{1}{(N+1)} + \frac{1}{(N+1)(N+2)} + \ldots < \frac{1}{N+1} + \frac{1}{(N+1)^2} + \ldots = \frac{1}{1-\frac{1}{N+1}} - 1 = \frac{1}{N} < 1$.
  - ▶ 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 $2 = p_1,\ 3 = p_2,\ \ldots,\ p = p_n$.
  - Betrachten wir die Zahl $N := p_1 \cdot p_2 \cdot \ldots p_n + 1$.
  - 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 Behautung 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:

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

- **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 $m > n$. $\square$

- 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 Mangelehre” 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. $\{0, 1, 2, \ldots\}$ 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 is 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

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

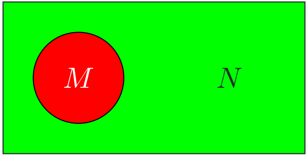
?

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

$$M \subseteq N \iff \forall m \left((m \in M) \to (m \in N)\right).$$

$$M = N \iff \forall m\left((m \in M) \to (m \in N)\right) \wedge \forall n \left((n \in N) \to (n \in M)\right),$$



- 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:* $M = N \iff M \subseteq N$ *und* $N \subseteq M$.

Beweis. Durch Einsetzen der Definitionen:

$$M = N$$

ist äq. zu

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

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. GanzeZahl(x), Gerade(x), Rat(x))
- Wir können die Objekte, für die $P(x)$ wahr ist, in eine Menge zusammenfassen.
- Beispiele
  - ▶ $\{L \in$ Lkw $|$ hatFisch$(L)\}$ oder $\{L \in$ Lkw : hatFisch$(L)\}$

    Die Menge enthält genau die Elemente L von Lkw, für die hatFisch(L) wahr ist.
  - ▶ $\{n \in \mathbb{N} \mid$ Gerade$(n)\} = \{n \in \mathbb{N} \mid n$ durch 2 teilbar$\} = \{n \in \mathbb{N} \mid \exists h(h \in \mathbb{N} \wedge n = 2h)\}$.
  - ▶ Wir haben auch $\{n \in \mathbb{N} \mid$ Gerade$(n)\} \subseteq \{n \in \mathbb{N} \mid n$ ist durch 2 teilbar$\}$,
  - ▶ $\{n \in \mathbb{N} \mid n$ ist durch 4 teilbar$\} \subseteq \{n \in \mathbb{N} \mid$ 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.

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

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

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

Seien M und N Mengen.

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

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

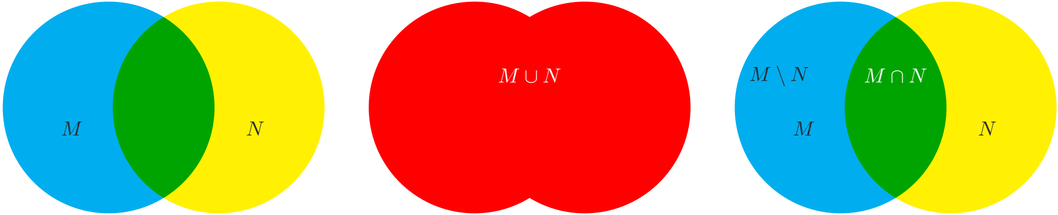
- Der Schnitt von M und N besteht aus den Elementen, die Element von M **und** von N sind:

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

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

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

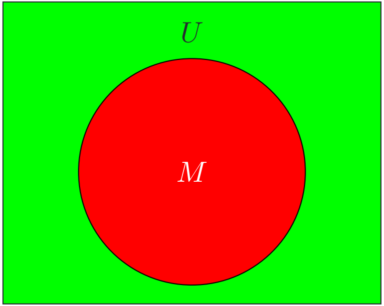
Venn-Diagramme illustrieren diese Definitionen.

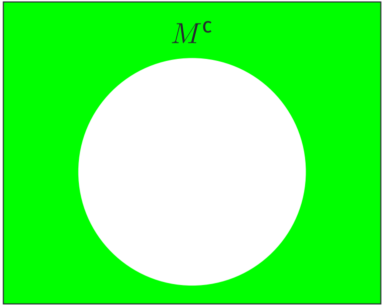


Im Kontext von Mengenoperationen gehen wir oft von einer Grundmenge U aus, in der alle betrachteten Mengen enthalten sind.

- 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:

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


U
M


M^{c}

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 $\cup$
$(A^\mathsf{c})^\mathsf{c}$	A	Involution $\cdot^\mathsf{c}$
$(A \cap B)^\mathsf{c}$	$A^\mathsf{c} \cup B^\mathsf{c}$	De-Morgan-Gesetz für $\cap$
$(A \cup B)^\mathsf{c}$	$A^\mathsf{c} \cap B^\mathsf{c}$	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 (Distributivität) Durch Anwendung der Definitionen erhalten wir:

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

$$= \{x \mid (x \in M) \lor (x \in \{y \mid (y \in N) \land (y \in P)\})\}$$

$$= \{x \mid \underbrace{(x \in M)}_{A} \lor (\underbrace{(x \in N)}_{B} \land \underbrace{(x \in P)}_{C})\}$$

$$= \{x \mid (\underbrace{(x \in M)}_{A} \lor \underbrace{(x \in N)}_{B}) \land (\underbrace{(x \in M)}_{A} \lor \underbrace{(x \in P)}_{C})\}$$

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

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

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

Beweis.

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

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

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

□

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

Eigenschaft	Bezeichnung
$A \cup A^{\mathsf{c}} = U$	Ausgeschlossenes Drittes
$((A \subseteq B) \wedge (B \subseteq C)) \to (A \subseteq C)$	Transitivität von $\subseteq$
$(A \subseteq B) \iff (B^{\mathsf{c}} \subseteq A^{\mathsf{c}})$	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

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

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

- 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 $x \in (M' \cup N')$. $\square$

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

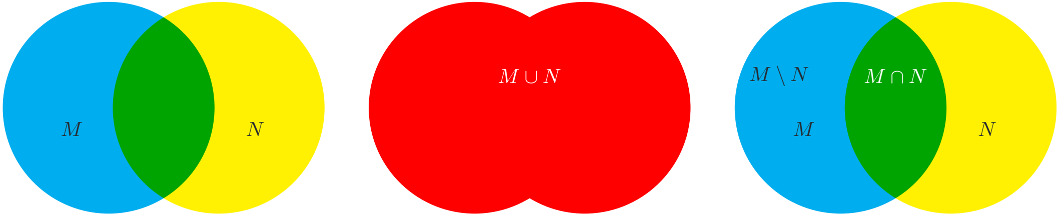
3. Kardinalität von endlichen Mengen, Potenzmenge

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 is 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 $\forall x\ x \in M \to x \in N$.
- Für alle Mengen M und N gilt: $M = N \iff M \subseteq N$ 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 eirgenwelches Universum U fixieren)

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

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

- Zuerst nehmen wir an, dass $x \in (A \cap B)^{\mathsf{c}}$, 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 $(A \cap B)^c = A^c \cup B^c$. $\square$

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) $\to$ (2), (2) $\to$ (3), und (3) $\to$ (1).
- (1) $\to$ (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) $\to$ (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 $M \subset N$. $\square$

- 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

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

und

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

- 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 Interval $[u,o]$ für $u,o \in \mathbb{R}$ mit $u \leq o$ ist definiert durch
$$[u,o] := \{r \in \mathbb{R}\colon\ u \leq r \leq o\}.$$
- 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. $\square$

- Wichtige Notationsvarianten. Für $I = \{u, u+1, \ldots, o\} \subseteq \mathbb{N}$ 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 "Distributivität von $\cap$": $M \cap \left(\bigcup_{i \in I} M_i\right) = \bigcup_{i \in I}(M \cap M_i)$
- Beweis:
  - Sei $x \in M \cap \left(\bigcup_{i \in I} M_i\right)$. Also $x \in M$ und $x \in \left(\bigcup_{i \in I} M_i\right)$. 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 $x \in \left(\bigcup_{i \in I} M_i\right)$, und es folgt $x \in M \cap \left(\bigcup_{i \in I} M_i\right)$. $\square$

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.

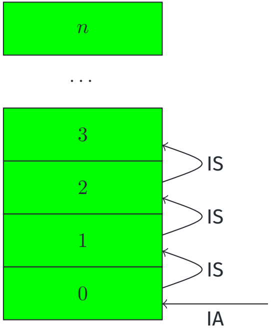
  Da es $2^{|M|}$ solche Auswahlmöglichkeiten gibt, ist dies auch die Anzahl der Teilmengen von M.
- Um solche Argumente präzis schreiben zu können, benötigen wir eine neue Beweistechnik "Induktion".

- 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*
- $F(n) \to F(n+1)$ *für alle* $n \in \mathbb{N}$,

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


n
$\dots$
3
2
1
0
IS
IS
IS
IA

- 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

$$\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + (n+1) \overset{\text{IH}}{=} \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2}$$

$$= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

Nach dem Prinzip der vollständigen Induktion folgt die Behauptung. $\square$

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

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

$$\forall n \Big(\forall M \; (|M| = n \to |\mathcal{P}(M)| = 2^n). \Big)$$

- 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

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

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

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 $(n+1)^2 = n^2 + 2n + 1 \overset{\text{IH}}{>} n + 5 + 2n + 1 > (n+1) + 5$. 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 $4! = 24 > 16 = 2^4$
  - Induktionshypotose: Sei $n \in \mathbb{N}, n \geq 4$ mit $n! > 2^n$.
  - Induktionsbehauptung: Zu zeigen ist, dass $(n+1)! > 2^{n+1}$.

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

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

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 Bahauptung fúr 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.

- 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 Webbrowser 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

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

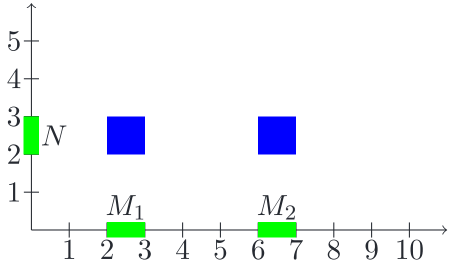
- $M \times N$ ist die Menge aller geordneten Paare von einem Element m aus M gefolgt von einem Element n aus N.
- Wir betonen dass wenn $M \neq N$ dann auch $M \times N \neq N \times M$.

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

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

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

$(M_1 \cup M_2) \times N =$



- 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:

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

- 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 $\mathcal{P}(M)$.

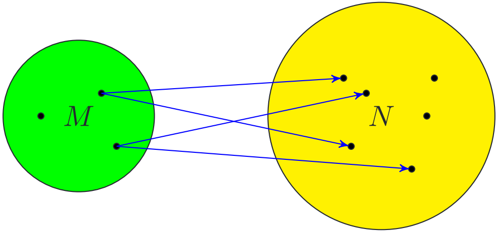
- Die Freund-Relation auf der Menge F der Facebook-Nutzer

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

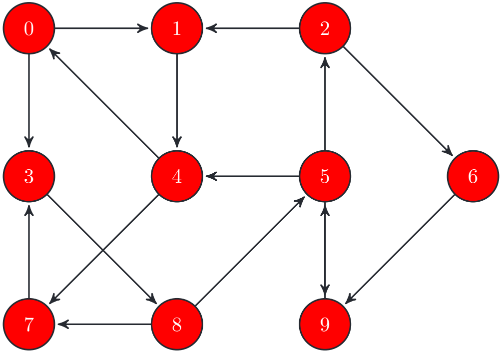
  ist eine Relation.

- Für jede Menge M ist die Identität $\mathrm{id}_M = \{(m, m) \mid m \in M\}$ eine Relation auf M. Gewöhnlich schreibt man $x = y$ statt $x \sim_{\mathrm{id}_M} y$.

Relation von M nach N

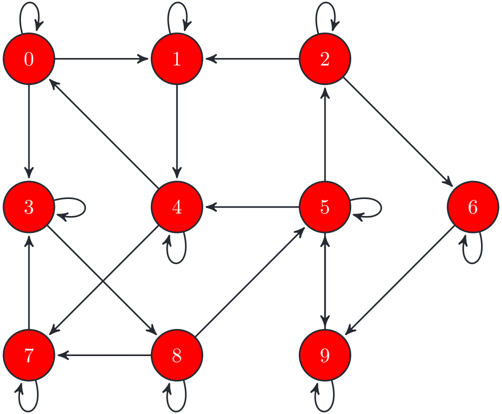


Relation auf $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$



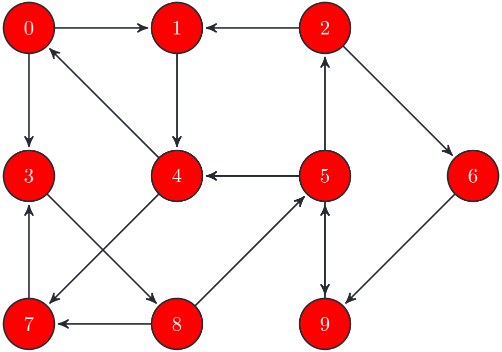
Sei $R \subseteq M \times M$ ein Relation auf M. R heißt

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



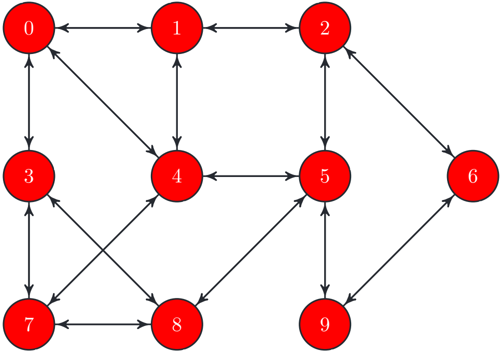
- Reflexivität: Alle Elemente haben Schleifen. z. B. $=$ ist reflexiv, $<$ ist nicht reflexiv, $\subseteq$ ist reflexiv,

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



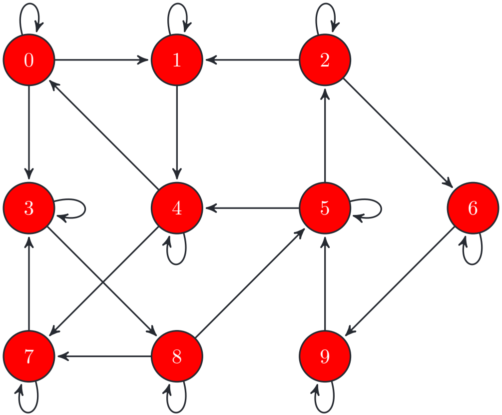
- Irreflexivität: Kein Element hat Schleifen.
- z.B. $<$ is irreflexiv

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



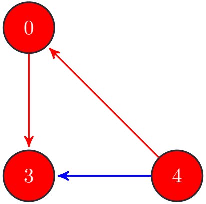
- Symmetrie: Jeder Pfeil ist beidseitig. Z.B. $=$ is symmetrisch, Facebook-frenschaft ist symmetrisch.

- antisymmetrisch, falls wenn $x \sim y$ und $y \sim x$ dann $x = y$.
  $\forall x, y\Big(\big((x,y) \in R \land (y,x) \in R\big) \to x = y\Big)$,



- 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 $x \sim z$.
  $\forall x, y, z\Big(\big((x,y) \in R \wedge (y,z) \in R\big) \to (x,z) \in R\Big)$.



- 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, $<$ is nicht vollständig.

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

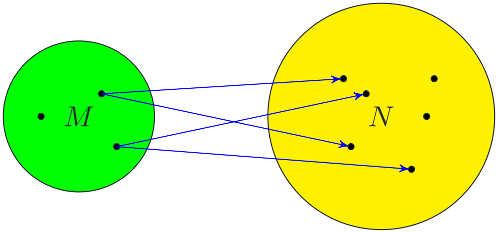
$$R^{-1} := \{(n, m) \in N \times M \mid (m, n) \in R\}.$$

- 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

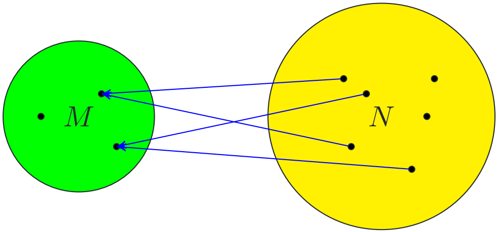
$$R^{-1} = \{(1, 1), (3, 1), (2, 2), (4, 2), (2, 3)\}.$$

- 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 $R \mathbin{;} R'$:

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

- Beispiel. Seien

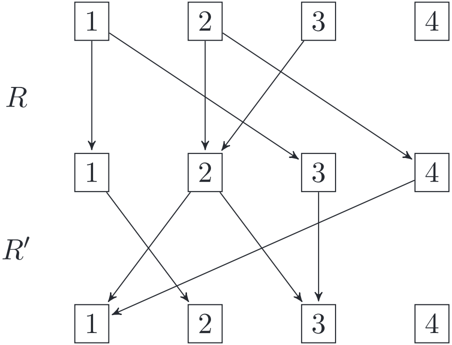
$$R := \{(1,1),\ (1,3),\ (2,2),\ (2,4),\ (3,2)\}$$

  und

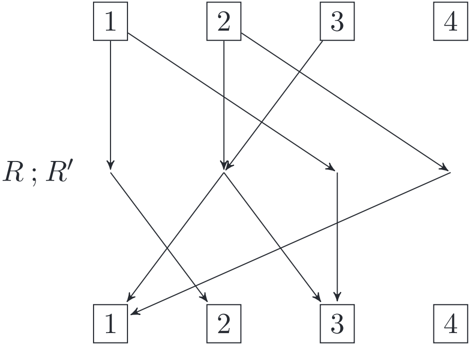
$$R' := \{(1,2),\ (2,1),\ (2,3),\ (3,3),\ (4,1)\}.$$

  Dann ist

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



1 2 3 4
R
1 2 3 4
R′
1 2 3 4



1 2 3 4
R ; R′
1 2 3 4

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

  Beweis.

- Reflexivität: Für alle $x \in \mathbb{N} \quad 2 \mid x - x = 0$, 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 $(y, x) \in R_2$.

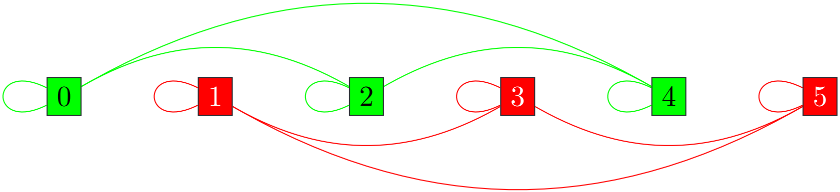
- Transitivität: Seien $x, y, z \in \mathbb{N}$, so dass $(x, y) \in R_2$ und $(y, z) \in R_2$. Daher $2 \mid x - y$, und $2 \mid y - z$. Dann $2 \mid (x - y) + (y - z) = x - z$. D.h. $2 \mid x - z$, womit auch $(x, z) \in R_2$. $\square$

- Äquivalenzklassen von R_2:

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

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

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



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

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

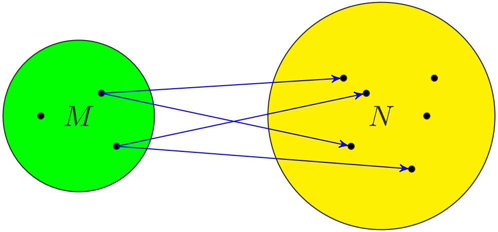
Mathematisches Institut

- 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

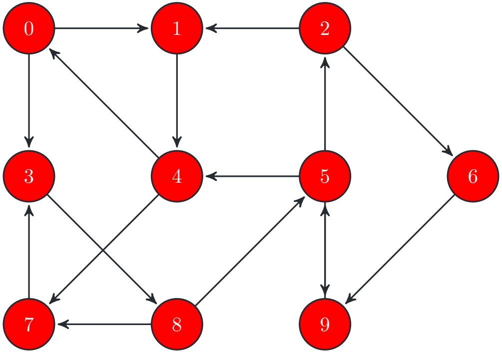
$$\{(x, y) \in F \times F \mid x \text{ ist Facebook-Freund von } y\}$$

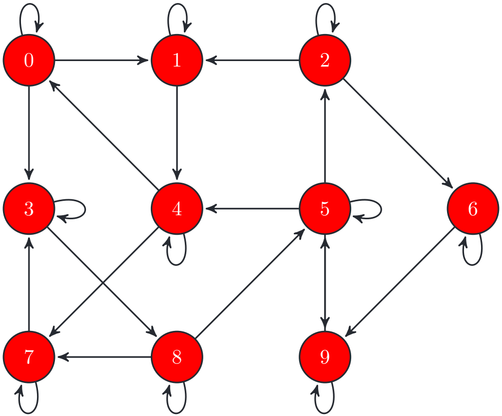
  ist eine Relation.

Relation von M nach N

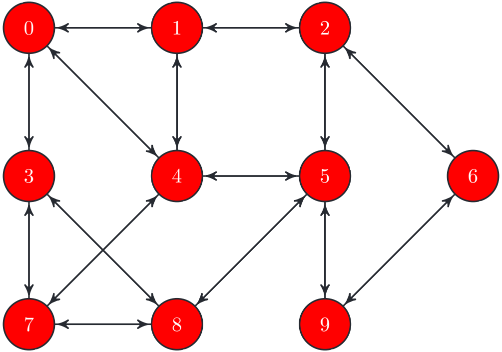


Relation auf $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

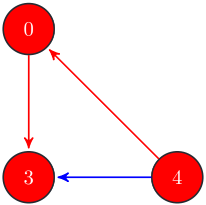




Reflexivität: Alle Elemente haben Schleifen.

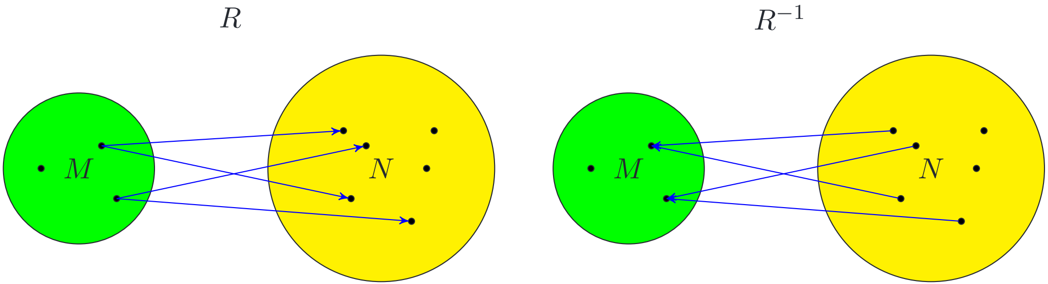


Symmetrie: Jeder Pfeil ist beidseitig.

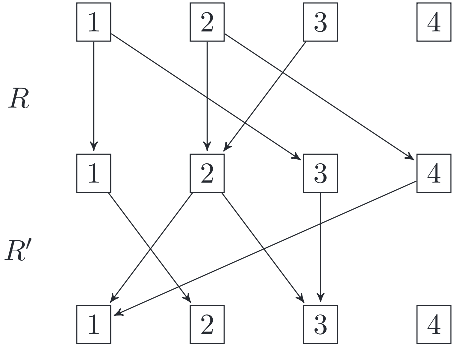


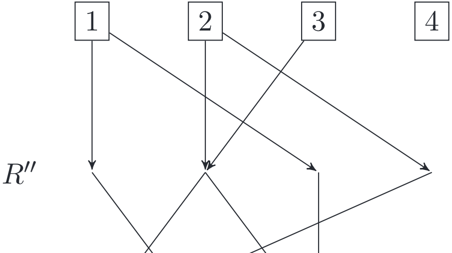
Transitivität: Für jeden Weg existiert auch der direkte Weg.

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



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





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

- 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:

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

Anders geschrieben:

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

Theorem

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

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

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

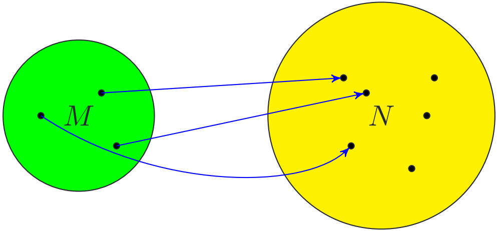
- Reflexivität: Sei $x \in M$. Da $M = \bigcup \mathcal{K}$ gibt es eine Menge $N \in \mathcal{N}$ mit $x \in N$. Also $x \equiv x$.
- Symmetrie: Sei $x \equiv y$. Dann existiert $N \in \mathcal{K}$ mit $\{x, y\} \subseteq N$. Folglich auch $y \equiv x$.
- Transitivität: Seien $x \equiv y$ und $y \equiv z$. 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 $x \equiv z$. $\square$

- 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:

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



M
N

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 $f\colon M \to N$.
- Für $(m, n) \in f$ schreiben wir entweder $n = f(m)$ oder $m \overset{f}{\mapsto} n$.
  - 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 $\mathrm{id}_M \colon M \to M$. Diese Funktion könnte man auch so definieren:

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

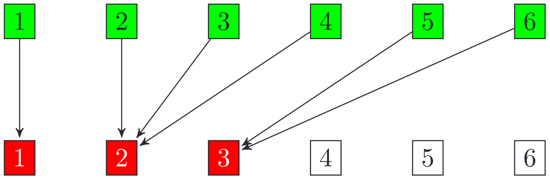
Für alle $M' \subseteq M$ gilt $\mathrm{id}_M(M') = M'$ und $\mathrm{id}_M^{-1}(M') = M'$

- Sei verdoppeln$\colon \mathbb{N} \to \mathbb{N}$ die Funktion

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

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

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



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

- $f\colon M \to N$ heißt injektiv gdw. alle verschiedenen Elemente von M auch verschiedene Bilder unter f haben.
$$\forall x, y \in M\colon\ x \neq y \to f(x) \neq f(y)$$
Manchmal schreibt man $f\colon M \hookrightarrow N$.
- f heißt surjektiv gdw. $f(M) = N$. (Jedes Element von N ist ein Bild eines Elements von M).
$$\forall n \in N \exists m \in M\colon\ f(m) = n$$
Manchman schreibt man $f\colon M \twoheadrightarrow N$.

- 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:
  - $\mathrm{id}_M : M \to M$ ist eine Bijektion.
  - Die Funktion verdoppeln$: \mathbb{N} \to \mathbb{N}$ ist injektiv, aber nicht surjektiv.
  - Die Funktion $f : \mathbb{N} \to \mathbb{N}$ mit $f(n) = \lceil \sqrt{n} \rceil$ ist surjektiv, aber nicht injektiv, denn es gilt $f(2) = f(3)$.
  - Die Funktion $q : \mathbb{R} \to \mathbb{R}$, mit $q(x) := x^2$ definiert, ist weder injektiv noch surjektiv.

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 $f\colon M \to N$ und $g\colon N \to P$.

- 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 $f\colon M \to N$, $g\colon N \to P$ und $h\colon P \to Q$ 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 folgf $(b,y) \in g;h$, und deswegen auch $(x,y) \in f;(g;h)$. $\square$

Theorem

Seien $f\colon M \to N$ und $g\colon N \to P$.

- *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 Punkte. $\square$

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 $f\colon M \to N$ ist invertierbar gdw. eine Funktion $g\colon N \to M$ existiert, so dass

$$f \mathbin{;} g = \mathrm{id}_M$$

und

$$g \mathbin{;} f = \mathrm{id}_N.$$

- 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. $\mathrm{id}_M ; \mathrm{id}_M = \mathrm{id}_M$.
- 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

- 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. Nähmlich, $f \subset M \times N$ ist eine Funktion gdw für jedes $m \in M$ existiert genau ein Element $n \in M$ so dass $(m, n) \in f$. Wir schreiben $f(m) = n$, oder $m \mapsto n$.
- $f: M \to N$ ist injektiv gdw $\forall x, y \in M: \; x \neq y \to f(x) \neq f(y)$
- $f: M \to N$ ist surjektiv gdw $\forall b \in N \exists a \in M \mid f(a) = b$
- $f: M \to N$ 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 $f\colon M \to N, g\colon N \to P$ sind zwei Funktionen dann $f;g\colon M \to P$ 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.

- Eine Funktion $f\colon M \to N$ ist invertierbar gdw. eine Funktion $g\colon N \to M$ existiert, so dass
$$f \mathbin{;} g = \mathrm{id}_M$$
und
$$g \mathbin{;} f = \mathrm{id}_N.$$
- 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 $f\colon M \to N$ eine Funktion. Für alle $m \in M$ und $n \in N$ gelten
>
> - $(m, m) \in f; f^{-1}$
> - $(f^{-1}; f \subset \mathrm{id}_N$. Wenn f surjektiv ist, dann $(f^{-1}; f = \mathrm{id}_N$.

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 $f^{-1}; f \subset \mathrm{id}_N$.

  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 $\mathrm{id}_N \subset f^{-1}; f$.

Satz. Eine Funktion $f\colon M \to N$ ist invertierbar gdw. sie bijektiv ist.

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

- 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 $f\colon M \to N$ ist invertierbar gdw. sie bijektiv ist.

$\leftarrow$ 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 $f^{-1}; f = \mathrm{id}_N$, und $\mathrm{id}_N \subset f; f^{-1}$. Da $f; f^{-1}$ ist eine Funktion, folgt aus der Eindeutigkeit $\mathrm{id}_N = f; f^{-1}$.

$\square$

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

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

und

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

Dann gilt $g = g'$.

Beweis. Wegen der Assoziativität der Komposition gilt

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

$\square$

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 $f\colon M \to N$ existiert eine Funktion $g\colon N \to M$, so dass $f;g = \mathrm{id}_M$.

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 $g\colon N \to M$ 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 $g(f(m)) = f^{-1}(f(m)) = m$. $\square$

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

Satz. Für jede surjektive Funktion $f\colon M \to N$ existiert eine Funktion $g\colon N \to M$, so dass $g\,;f = \mathrm{id}_N$.

- 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 $f\colon M \to N$ existiert eine Funktion $g\colon N \to M$, so dass $g \,;\, f = \mathrm{id}_N$.

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 $g\colon N \to M$ durch $g(n) := m_n$.

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

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

$\square$

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 $f : \mathbb{N} \to \mathbb{N}$ haben. In diesem Fall könnten wir die einseitige Inverse $g : \mathbb{N} \to \mathbb{N}$ 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 $c \colon \mathcal{X} \to \bigcup \mathcal{X}$ mit $c(M) \in M$ für alle $M \in \mathcal{X}$.

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

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 $\mid\, = \{(n, n') \in \mathbb{N}_+ \times \mathbb{N}_+ \mid n \text{ teilt } n'\}$ ist eine Ordnungsrelation.
  - **Reflexivität:** Für alle $x \in \mathbb{N}_+$ teilt x sich selbst, also $x \mid x$.
  - **Antisymmetrie:** Seien $x \mid y$ und $y \mid x$. Dann gelten $x \leq y$ und $y \leq x$, womit $x = y$.
  - **Transitivität:** Seien $x \mid y$ und $y \mid z$. 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 $x \mid z$ gilt.

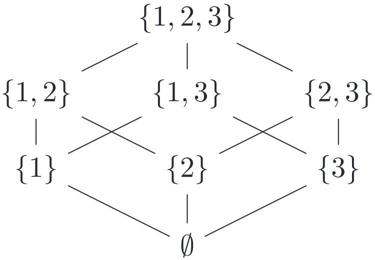
Teilweise geordnete Mengen lassen sich durch Hasse-Diagramme visualisieren.

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

$$\begin{tikzcd}
\vdots \arrow[d, dash, dotted] \\
3 \arrow[d, dash] \\
2 \arrow[d, dash] \\
1 \arrow[d, dash] \\
0
\end{tikzcd}$$

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

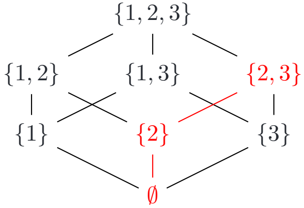
Hasse-Digramm für $(\mathcal{P}(\{1,2,3\}), \subseteq)$:



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 $x, y \in X$.

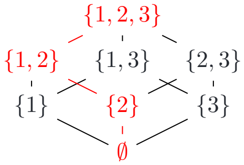
Beispiele

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

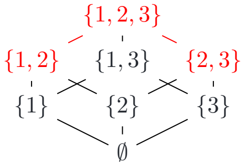


Beispiele

- 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 <u>keine</u> Teilkette von $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$.



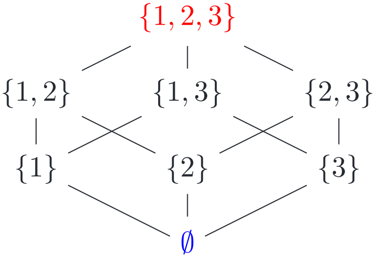
- Wir dürfen jedoch die geordnete Menge $(\{\{1, 2\}, \{1, 2, 3\}, \{2, 3\}\}, \subseteq)$ betrachten.

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

- maximal gdw. $x \npreceq m$ für alle $m \in M$ mit $m \neq x$; d. h. es gibt keine echt größeren Elemente,
- minimal gdw. $m \npreceq x$ für alle $m \in M$ mit $m \neq x$; d. h. es gibt keine echt kleineren Elemente.

Beispiele

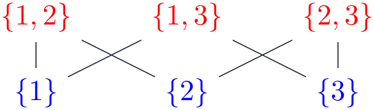
- In $(\mathbb{N}, \leq)$ haben wir 0 als einziges minimales Element und keine maximalen Elemente.
- $(\mathcal{P}(\{1,\ 2,\ 3\}), \subseteq)$



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 $m \preceq m$. 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 $\{1\}, \{2\}$.

- 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 $X \subset \mathcal{P}(\mathcal{M})$. 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 irgenwelche andere obere Schranke. Dann für jede $Y \in X$ gilt $Y \subset S$, wobei auch $\bigcup X \subset X$. □

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

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

$$f \mathbin{;} g = \mathrm{id}_M$$

und

$$g \mathbin{;} f = \mathrm{id}_N .$$

- 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 $f\colon M \to N$ ist invertierbar gdw. f ist bijektiv.

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

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

und

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

Dann gilt $g = g'$.

Satz. Für jede injektive Funktion $f\colon M \to N$ existiert eine Funktion $g\colon N \to M$, so dass $f; g = \mathrm{id}_M$.

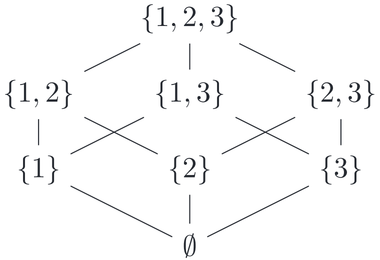
Satz. Für jede surjektive Funktion $f\colon M \to N$ existiert eine Funktion $g\colon N \to M$, so dass $g \,;\, f = \mathrm{id}_N$.

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



Satz. Sei M eine endliche Menge und sei $f\colon M \to M$ 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. $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(x) = 2x$ ist zwar injektiv, aber nicht surjektiv.
  - $f\colon \mathbb{N} \to \mathbb{N}$ 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 $f: M \to N$ 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 $f: \mathbb{Z} \to \mathbb{N}$ mit

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

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

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

  Die Äquivalenzklassen heißen Kardinalitäten.

- Biespiel: die Kardinalität von $\{6, 9, 11\}$ heißt "drei".

- Sind alle unendliche Mengen gleichmächtig? Andersgesagt: gibt es nur eine unendliche Kardinalität?
- Bevor wie diese Frage betantworten, 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.

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

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

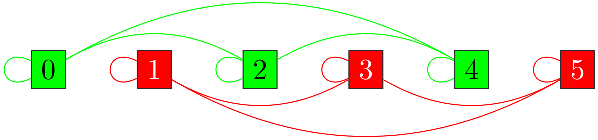
$$
\begin{array}{rccccccccc}
b(0) = & a_0 & , & d_{00} & d_{01} & d_{02} & \cdots & d_{0n} & \cdots \\
b(1) = & a_1 & , & d_{10} & d_{11} & d_{12} & \cdots & d_{1n} & \cdots \\
b(2) = & a_2 & , & d_{20} & d_{21} & d_{22} & \cdots & d_{2n} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots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

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

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. $\square$

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

- Wir definieren $|M| \leq |N|$ genau dann wenn es gibt eine Injektion $f\colon M \to N$. 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 $f\colon M \to N$ gdw. es existiert eine injektive Funktion $g\colon X \to Y$.

Beweis.

- ($\to$) Sei $f\colon M \to N$ injektiv. Aufgrund der Annahme $|M| = |X|$ und $|N| = |Y|$. existieren Bijektionen $b\colon X \to M$ und $c\colon N \to Y$.

  Dann ist die Funktion $(b\,;f\,;c\colon X \to Y$ injektiv.

- ($\leftarrow$) Durch die Symmetrie der Aussage $\square$

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 $f\colon M \to N$.

- Für endliche Kardinalitäten erhalten wir die normale Ordnungsrelation $|\{1, 2\}| \leq |\{2, 3, 4\}|$
- $|\mathbb{N}| \leq |\mathbb{Z}|$ vermittels $\iota\colon \mathbb{N} \to \mathbb{Z}$ 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 $\iota\colon M \to N$, mit $\iota(m) = m$, ist injektiv.
- Sei $f\colon M \to N$ surjektiv. Dann $|N| \leq |M|$. In der Tat, sei $g\colon N \to M$ mit $g; f = \mathrm{id}_M$. 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?
  - Reflexivität: $\mathrm{id}_M : M \to M$ ist injektiv, also $|M| \leq |M|$
  - Transitivität: $f : A \to B$, $g : B \to C$ - Injektionen, dann $f;g : A \to C$ auch Injektion. Also $|A| \leq |B|$ und $|B| \leq |C|$ impliziert $|A| \leq |C|$.
  - Antisymmetrie: $f : A \to B$ Injektion, $g : B \to A$ Injektion (also $|A| \leq |B|$ und $|B| \leq |A|$). Gibt es eine Bijektion $A \to B$? Das ist nicht klar.

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

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

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

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

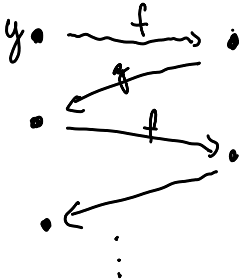
- Wenn dass nicht der Fall ist, dann betrachten wir die Mengen $M' := \{(m,0)\colon m \in M\}$, $N' := \{(n,0)\colon n \in N\}$. Wir haben Bijektionen $M' \to M$, $N' \to N$, also eine Bijektion zwischen M und N existiert gdw eine Bijektion zwischen M' und N' existiert.

- 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 $b_K\colon K \cup M \to K \cup N$ zu konstruieren. In der Tat, falls wir das schaffen, dann definieren wir $b\colon M \to N$ durch $b(x) := b_K(x)$ wenn $x \in K$. Weil $\{K \cap M\colon K \in M \cup N/V\}$ eine Zerlegung von M ist, schließen wir, dass b eine Bijektion ist.

Sei K eine Äquivalenzklasse von V.

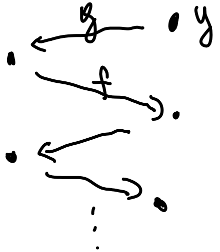
- In K : gibt's $y \in M$ mit $y \notin g(N)$.



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

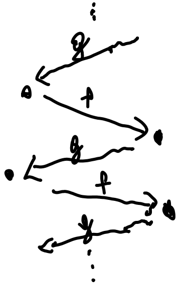
- b_K is eine Bijektion: Tatsätzlich, $K = \{y, f(y), gf(y), fgf(y), \ldots\}$. Alle diese Elemente sind unterschiedlich.
- Erst beweisen wir $y, gf(y), (gf)^2(y), \ldots$ sind unterschiedlich.
  - Induktionsbeweis: IA: $y, gf(y)$ sind unterschiedlich, da $y \notin g(N)$.
  - IH: $y, gf(y), \ldots (gf)^k(y)$ sind unterschiedlich.
  - IB: Zu zeigen ist, dass $y, gf(y), \ldots (gf)^k(y)$ 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 ist injektiv, folgt $(gf)^k(y) = gf^{l-1}(y)$. Widerpsruch mit IA.
- Da g eine Injektion ist, sehen wir, dass $y, f(y), gf(y), fgf(y), \ldots$ sind unterschiedliche Elemente. Es folgt dass b eine Bijetion 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 $b_K(z) := f(z)$. $\square$

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 $f: M \to N$ und $g: N \to M$. Dann existiert auch eine bijektive Funktion $h: M \to N$ nach CSB und damit $|M| = |N|$. $\square$

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

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 $f\colon M \to \mathcal{P}(M)$, 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 $g\colon M \to \mathcal{P}(M)$.

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. $\square$

Es gibt also unendlich viele unendliche Kardinalitäten:

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

- Die Kardinalität $|\mathbb{R}|$ nennt man auch Kontinuum und bezeichnet man sie mit dem Symbol $\mathfrak{c}$.
- Gibt es Kardinalitäten zwischen $\aleph_0 = |\mathbb{N}|$ und $\mathfrak{c} = |\mathbb{R}|$? 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 zwie Injektionen zu konstruieren.

- Jede reelle Zahl $x \in (0, 1)$ lässt sich eindeutig als $x = [0, d_1 d_2 d_3 d_4 \cdots]_{10}$ mit den Ziffern $d_1, d_2, \ldots \in \{0, 1, \ldots, 9\}$ 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 $f(x) := \{[d_1]_{10}, [d_1 d_2]_{10}, [d_1 d_2 d_3]_{10}, \ldots\}$. Diese Funktion f ist injektiv.
- Sei $X \subseteq \mathbb{N}$. Wir konstruieren die reelle Zahl $g(X) := [0, 1 b_0 b_1 b_2 \cdots]_{10}$ 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. $\square$

- 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 R, oder die gleiche Anzahl von Elementen hat wie die natürlichen Zahlen 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