UNIVERSITÄT
LEIPZIG

Vorlesung 3 - Naive Mengenlehre

Diskrete Strukturen (WS 2023-24)

Łukasz Grabowski

Mathematisches Institut

Diskrete Strukturen

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:

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

- **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

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

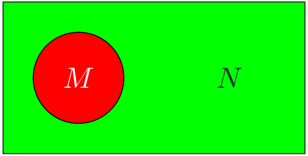
?

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

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

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



- 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

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

ist äq. zu

$$(M \subseteq N) \;\wedge\; (N \subseteq M) \qquad \square$$

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
  - $\{L \in \text{Lkw} \mid \text{hatFisch}(L)\}$ oder $\{L \in \text{Lkw} : \text{hatFisch}(L)\}$

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

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

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

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

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

Seien M und N Mengen.

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

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

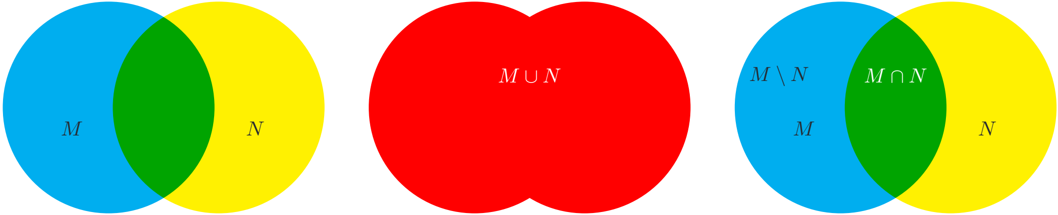
- Der Schnitt von M und N besteht aus den Elementen, die Element von M **und** von N sind:

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

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

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

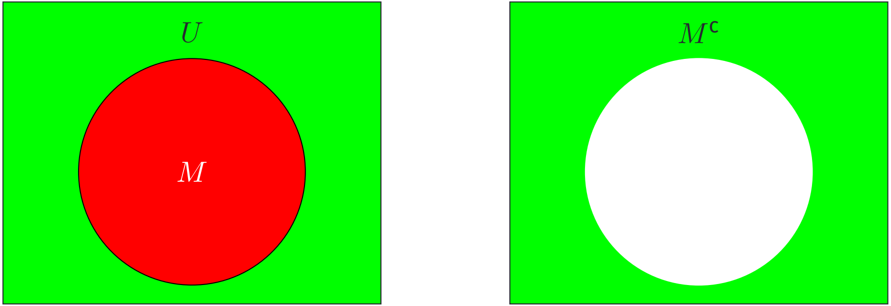
Venn-Diagramme illustrieren diese Definitionen.



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:

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

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

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

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

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

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

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

Beweis.

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

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

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

$\square$

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