Vorlesung Lineare Algebra I

WiSe'19/'20 hhu
K. Halupczok

§1: Mathematische Grundbegriffe

L3: Elementare Mengenlehre und Beweise

Stichworte: Menge, Element, $\emptyset$, Mengenverknüpfungen $\cap\,\cup\,\setminus$, Mengenbeziehung $\subseteq$, Formulieren von Sätzen/Beweisen, Beweise von Aussagen mit Quantoren

---

Wir haben hier noch nicht erklärt, woher oder was die "Geltungsbereiche" für die Variablen sind. Wir wollen hierfür Mengen nehmen und werden deswegen als nächstes die Mengenlehre behandeln. Die gesamte Mathematik beruht hierauf:

3.1. Die Fundamente der modernen Mathematik: Zu Beginn des 20. Jhd. hat man die Mathematik auf diese beiden Tragpfeiler gesetzt:

1. Jede mathematische Struktur wird mit Hilfe der Mengenlehre beschrieben und besteht aus Mengen. Selbst Abbildungen und Relationen können als Mengen aufgefasst werden (wir werden noch sehen, wie).
2. Axiome, Aussagen und Beweise werden in der Sprache der Prädikatenlogik aufgeschrieben ("formuliert").

Was wir als "abstrakten Formalismus" bezeichnen, setzt sich also im Detail alles aus Begriffen der Mengenlehre und Prädikatenlogik zusammen. Jede Formel bzw. Aussage lässt sich im Prinzip immer in kleinste "Bausteine" zerlegen.

3.2. Idee: Eine Menge ist eine Zusammenfassung von verschiedenen Objekten (die auch Mengen sind). Diese Objekte heißen Elemente der Menge.

Ist x ein Element der Menge M, schreibt man $x \in M$.

Wenn x kein Element der Menge M ist, schreibt man $x \notin M$, d.h. $x \notin M \Leftrightarrow \neg(x \in M)$.

Bsp: G sei die Menge der geraden natürlichen Zahlen. Dann gilt $2 \in G$, $5 \notin G$.

3.3. Durch folgende Regeln können Mengen beschrieben oder definiert werden:

(a) durch explizite Aufzählung ihrer Elemente, z.B. ("..." ok, falls klar ist, was hier gemeint ist)

$\{1,3,7\}$, $\{2,17,4,3\}$, $\{1,\dots,10\}$,

wobei die Reihenfolge/Mehrfachnennung keine Rolle spielt: $\{1,2\} = \{2,1\} = \{1,2,1,1\}$.

L3

-2-

(b) durch Aussondern: Ist A eine Menge und P eine Bedingung an die Elemente von A (genauer: P ist Prädikat in x und A der Wertebereich für x), so ist auch $\{x \in A \mid P(x) \text{ ist wahr}\}$ eine Menge. Kürzer: $\{x \in A \mid P(x)\}$,

lies "Menge der $x \in A$, für die $P(x)$ wahr ist",

man sagt auch "so dass" bzw. "für die gilt"

für den vertikalen Strich "|" darin kann auch ":" oder ";" geschrieben werden.

Bsp: Wird die Menge der natürlichen Zahlen $1, 2, 3, \ldots$ mit $\mathbb{N}$ bezeichnet, so ist $\{x \in \mathbb{N} \mid \underbrace{x \text{ ist gerade}}_{\text{ist ein Prädikat } P(x)}\} = \{2, 4, 6, 8, \ldots\}$ die Menge der geraden Zahlen.

Kommas stehen für "und", wie fast immer

3.4. Bem.: Eine wichtige Menge ist die leere Menge, welche per Definition die Menge ohne Elemente ist. Sie wird mit $\emptyset$ und manchmal auch mit $\{\}$ bezeichnet. Durch Aussondern ist sie z.B. als $\emptyset = \{x \in \mathbb{N} \mid x \neq x\}$ beschreibbar.

3.5. Bem.: Die Bezeichnungen für Zahlbereiche sind $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, \ldots\}$ (die Menge der ganzen Zahlen), $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z} \wedge b \neq 0\}$, und $\mathbb{R}$ für die Menge der reellen Zahlen, $\mathbb{N} = \{1, 2, 3, \ldots\}$ für die Menge der natürlichen Zahlen.

Vom Definieren und der sinnvollen Wahl von Notationen:

3.6. Aussagen hatten wir stellvertretend mit $A, B, C, \ldots$ bezeichnet und gesehen, dass man auch längere Teile mit einem neuen Namen/Buchstaben abkürzen will. Dafür definiert bzw. setzt man die Aussage auf die neue Bezeichnung mit dem Zeichen $:\Leftrightarrow$, also z.B. $C :\Leftrightarrow A \vee \neg B$, so dass man anstelle $(A \vee \neg B) \wedge D$ danach einfacher $C \wedge D$ schreiben kann, falls das nützlicher ist. Generell bemüht man sich um sinnvolle Bezeichnungen/Notationen und sagt immer dazu, was für ein Objekt ein Buchstabe bezeichnen soll, z.B. "C sei die Aussage $C :\Leftrightarrow A \vee \neg B$". Der Doppelpunkt steht immer bei der neuen Bezeichnung, daher ginge auch z.B. $A \vee \neg B \Leftrightarrow: C$.

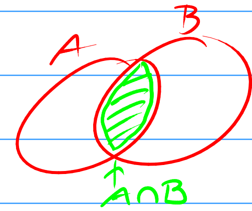
Jetzt in der Mengenlehre sollen Großbuchstaben $A, B, C, \ldots, M, N, \ldots$ auch Mengen bezeichnen. Wir wollen zum Definieren von Mengen ebenso vorgehen und z.B. $M := \{2, 4, -1\}$ schreiben.

3.7. Solche Bezeichnungen bleiben dann solange gültig, wie man über sie spricht.
Die universellen Bezeichnungen
$\emptyset, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ gelten immer wie hier angegeben.
Für Variablen hatten wir bereits Kleinbuchstaben $x, y, z, t, d, \ldots$ benutzt.
Prädikate kann man mit $P(x) :\Leftrightarrow$ (Formel/Aussage in x) definieren,
z.B. $P(x) :\Leftrightarrow x > 0$.

Mengenverknüpfungen $\cap, \cup, \setminus$

3.8. Ein Spezialfall des Aussonderns ist die Durchschnittsbildung:
Sind A und B Mengen, so setzt man

$$A \cap B := \{x \in A \mid x \in B\} = \{x \in B \mid x \in A\}.$$



Die Menge $A \cap B$ heißt (Durch-)Schnitt von A und B.
Die Elemente von $A \cap B$ sind genau die Elemente von A und von B, d.h. $x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$.

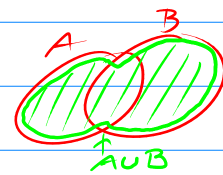
Bsp.: $A = \{2, 3, 4, 7, 11\}$, $B = \{3, 4, 11, 17, 19\}$, dann ist
$A \cap B = \{3, 4, 11\}$.

Bem.: Für jede Menge A gilt $A \cap \emptyset = \emptyset$, $A \cap A = A$.

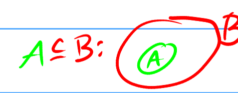
3.9. Die Vereinigung zweier Mengen A und B ist die Menge, die aus allen Elementen aus A oder B besteht und wird mit $A \cup B$ bezeichnet:

$$A \cup B := \{x \mid x \in A \vee x \in B\}.$$

Bsp.: $A = \{2, 3, 4, 7, 11\}$, $B = \{3, 4, 11, 17, 19\}$, dann ist
$A \cup B = \{2, 3, 4, 7, 11, 17, 19\}$.



Bem.: Für jede Menge A gilt $A \cup \emptyset = A$, $A \cup A = A$.



Teilmengen

3.10. Zwei Mengen sind gleich genau dann, wenn sie die gleichen Elemente enthalten, also $A = B :\Leftrightarrow (\forall x \in A : x \in B) \wedge (\forall x \in B : x \in A)$. Gilt $A = B$, so kann in einer Formel mit B dann auch A eingesetzt werden und umgekehrt.

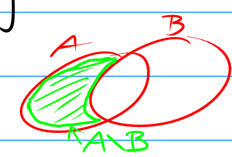
3.11. Def.: Sind A, B Mengen, so ist A Teilmenge von B (in Zeichen: $A \subseteq B$), falls $\forall x \in A : x \in B$. D.h.: $A \subseteq B :\Leftrightarrow \forall x \in A : x \in B$.

3.12. Bem.: Statt $A \subseteq B$ kann man auch $B \supseteq A$ schreiben und sagt manchmal, B ist Obermenge von A. Weiter gilt immer $\emptyset \subseteq A$, $A \subseteq A$. Damit lässt sich $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$ schreiben.
Der Strich $\subseteq$ am Teilmengenzeichen lässt man manchmal weg, wir wollen ihn der Deutlichkeit halber schreiben. Er bedeutet, dass bei "$A \subseteq B$" auch "$A = B$" möglich ist. Will man das ausschließen, schreibt man

$$A \subsetneq B :\Leftrightarrow A \subseteq B \wedge A \neq B$$

Im Gegensatz dazu ist $A \nsubseteq B :\Leftrightarrow \neg(A \subseteq B)$ eine andere Aussage, nämlich $\neg(A \subseteq B) \Leftrightarrow \neg(\forall x \in A : x \in B) \Leftrightarrow \exists x \in A : x \notin B$.
Bsp: Es gilt $\{1,2\} \nsubseteq \{2\}$, $\{1\} \subsetneq \{1,5\}$, $\{1\} \subseteq \{1,5\}$.
Ü Gilt eine Implikation zwischen $A \subsetneq B$ und $A \nsubseteq B$?

3.13. Sind A und B Mengen, so heißt $A \setminus B := \{x \in A \mid x \notin B\}$ die Differenzmenge. Lies "A ohne B".



Gelegentlich schreibt man $A - B$ ("A minus B"), eher selten.
Ist $B \subseteq A$, so heißt $A \setminus B$ auch das Komplement von B in A.
Bsp: $\{3,2,4,5\} \setminus \{1,2,4,6\} = \{3,5\}$.

3.14 Bem.: Somit gilt: $\neg(A \subseteq B) \Leftrightarrow \exists x \in A \setminus B$.
Sind $A, B \subseteq C$, dann gilt: $A \subseteq B \Leftrightarrow \forall x \in A : x \in B \Leftrightarrow \forall x \in C : x \in A \Rightarrow x \in B$.
Ein wichtiger Schritt ist nun, dass auch "Mengen von Mengen" untersucht werden können, z.B. $A := \{\emptyset, \{1,2\}, \{3\}, \{4,1\}\}$, so dass $\emptyset \in A$, $\{3\} \in A$, $\{1,4\} \in A$ wahr ist. Später soll z.B. eine Gerade eine gewisse Menge von Punkten sein, und auch Mengen von Geraden sollen betrachtet werden etc.

3.15. Damit sind interessante Konstruktionen möglich: $A = \{1,2,3\}$, dann ist $B := \{\{x,y\} \mid x,y \in A\} = \{\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\}\}$.
Und $\{C \mid C \subseteq A\} = \{\emptyset\} \cup B \cup \{A\}$ ist die Menge aller Teilmengen von A, die für jede Menge A interessant ist:

3.16. Ist A eine Menge, dann heißt die Menge aller Teilmengen von A die Potenzmenge von A, in Zeichen: $\mathcal{P}(A) := \{B \mid B \subseteq A\}$.

Bsp.: $\mathcal{P}(\emptyset) = \{\emptyset\}$, beachten Sie, dass $\{\emptyset\} \neq \emptyset$, da ja $\emptyset \in \{\emptyset\}$.

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

Hat A insgesamt n Elemente, so hat $\mathcal{P}(A)$ dann 2^n viele Elemente.

3.17. Quantoren und Mengen: Die Quantoren "$\forall, \exists$" stehen oft in der Form "$\forall x \in A$" bzw. "$\exists x \in A$" für eine Menge A da, wie schon oben 3.10, 3.11, 3.14 gesehen, mit der Bedeutung "Für alle Elemente x von A gilt..." bzw. "Es gibt ein Element x von A mit...".

3.18. Beweise von Sätzen mit Quantoren:

Mathematische Sätze in der Form "Satz: $\underbrace{A}_{\text{Voraussetzung}} \Rightarrow \underbrace{B}_{\text{Behauptung}}$" benutzen fast immer Quantoren, was wir hier in Anwendungsbeispielen studieren möchten:

3.19. Bsp.: Beweis eines Satzes mit dem Existenzquantor $\exists$: Satz: $\underbrace{A}_{\text{Vor}} \Rightarrow \overbrace{\exists x \in M : P(x)}^{\text{Beh. } B \text{ mit } "\exists"}$

Durch (ev. konstruktive) Angabe eines Elements x, für das $P(x)$ gezeigt werden kann, ist der Beweis geführt.

$\exists k$: $2^{2^k}+1$ nicht prim

6. Bsp.: Satz: Beh.: Es gibt eine Zahl der Form $2^{2^k}+1$, $k \in \mathbb{N}$, die keine Primzahl ist (d.h. aus zwei Faktoren >1 zusammenges. ist).

Bew.: Für $k=5$ ist die Zahl $2^{2^5}+1 = 641 \cdot 6700417$ zusammengesetzt. $\square$

3.20. Bsp.: Beweis eines Satzes mit dem Allquantor $\forall$: Satz: $\underbrace{A}_{\text{Vor}} \Rightarrow \overbrace{\forall x \in M : P(x)}^{\text{Beh. } B \text{ mit } "\forall"}$

Durch Nachweis von $P(x)$ für jedes Element x ist der Beweis geführt.

a) Dies kann durch expliziten Beweis für jedes El. x der Reihe nach erbracht werden, falls es nicht zuviele Elemente sind.

b) Man führt den Beweis von $P(x)$ für jedes beliebige, aber fest gewählte x, auf abstraktem Wege (mit dem Namen "x" für das untersuchte Element).

c) Man teilt M auf in separate Teilmengen $M = M_1 \cup M_2 \cup \ldots \cup M_n$ und beweist $P(x)$ für jedes $x \in M_i$, $i \in \{1,\ldots,n\}$, separat. Man sagt, man macht eine Fallunterscheidung (mit n vielen "Unterbeweisen", wo wieder a), b) oder c) benutzt werden können).

Wir zeigen dieses Vorgehen anhand von Beispielen:

3.21. Bsp. für a): Satz: Für alle natürlichen Zahlen $k \le 4$ ist $2^{2^k}+1$ eine Primzahl.
Beweis: Die Zahl $2^{2^1}+1=5$ ist prim, $2^{2^2}+1=17$ ist prim, $2^{2^3}+1=257$ ist prim (da keine Primzahl $<\sqrt{257}\approx 16$ Teiler ist), $2^{2^4}+1=65537$ ist prim (da keine Primzahl $<\sqrt{65537}\approx 256$ Teiler ist). □

Man kann hier die einzelnen Elemente in einer "Liste" abarbeiten.

3.22. Bsp. für b): Satz: Für alle reellen Zahlen x,y gilt $4xy \le (x+y)^2 \le 2(x^2+y^2)$.
Bew.: Zur 1. Beh. $4xy \le (x+y)^2$: Es gilt $(x-y)^2 \ge 0 \Leftrightarrow x^2-2xy+y^2 \ge 0 \Leftrightarrow x^2+2xy+y^2 \ge 4xy$
$\Leftrightarrow (x+y)^2 \ge 4xy$.

Zur 2. Beh. $(x+y)^2 \le 2(x^2+y^2)$: Es gilt $(x-y)^2 \ge 0 \Leftrightarrow x^2-2xy+y^2 \ge 0 \Leftrightarrow 2xy \le x^2+y^2$
$\Leftrightarrow x^2+2xy+y^2 \le 2x^2+2y^2 \Leftrightarrow (x+y)^2 \le 2(x^2+y^2)$. □

Für beide Teile der Behauptung wurde der Beweis abstrakt geführt mit den Rechenregeln reeller Zahlen und der Tatsache, dass $u^2 \ge 0$ ist für jede reelle Zahl u.

3.23. Bsp., für c): Satz: Jede Quadratzahl lässt bei Division durch 8 den Rest 0, 1 oder 4.
Beweis: 1. Fall: n gerade: Wenn n gerade ist, ist $n=2k$ mit $k \in \mathbb{N}$ und $n^2=4k^2$.

zwei Unterfälle
- Falls k gerade, etwa $k=2l$ mit $l \in \mathbb{N}$, ist $n^2=4\cdot(2l)^2$ durch 8 teilbar, lässt also Rest 0.
- Falls k ungerade, etwa $k=2l+1$ mit $l \in \mathbb{N}$, lässt $n^2=4(2l+1)^2=16l^2+16l+4$ den Rest 4.

2. Fall: n ungerade: Wenn n ungerade ist, ist $n=2k+1$ mit $k \in \mathbb{N}_0$, und $n^2=4k(k+1)+1$ lässt den Rest 1, weil $k(k+1)$ stets gerade und daher $4k(k+1)$ durch 8 teilbar ist. □

Bem.: Für diese Fallunterscheidung wurde die Menge $Q=\{n^2;\ n\in\mathbb{N}\}$ der Quadratzahlen aufgeteilt in $Q=\underbrace{\{(4l)^2;\ l\in\mathbb{N}\}}_{\text{"}M_1\text{"}} \cup \underbrace{\{(4l+2)^2;\ l\in\mathbb{N}_0\}}_{\text{"}M_2\text{"}} \cup \underbrace{\{(2k+1)^2;\ k\in\mathbb{N}_0\}}_{\text{"}M_3\text{"}}$

3.24. Bem.: Q wurde hier in eine disjunkte Vereinigung von Mengen M_1, M_2, M_3 zerlegt: Man nennt zwei Mengen A,B disjunkt, falls $A\cap B=\emptyset$. Ansonsten sagt man, ihr (Durch)schnitt ist nichtleer. Sind $M_1, M_2, \dots, M_n$ disjunkt, so heißt das, dass sie paarweise disjunkt sind, d.h. $\forall i,j \in \{1,\dots,n\},\ i\ne j: M_i \cap M_j=\emptyset$. Anstelle $M_1\cup M_2\cup\dots\cup M_n$ schreibt man zur Verdeutlichung dann auch $M_1 \dot\cup M_2 \dot\cup \dots \dot\cup M_n$.

3.25. Nachtrag zu 3.12: Gilt $A \subsetneq B$, so heißt A eine echte Teilmenge von B.