# Inhalt der Vorlesung "Logische Grundlagen" im WiSe 2016/17, PD Dr. K. Halupczok

## LG1: Mathematische Grundbegriffe und Aussagenlogik

Stichworte: Sprache der Mathematik, Abstrakter Formalismus, Deduktion durch Einsetzen, Induktion, Axiomensysteme, Satz, Aussage, Verknüpfungen $\wedge \vee \neg$, Klammersetzungsregeln, Implikation, Äquivalenz, Logikregeln, erste Beweistheorie

## LG2: Prädikatenlogik, Quantoren, einfache Mengenlehre

Stichworte: Prädikate, Quantoren $\forall \exists \exists!$, Umgang mit Quantoren, Fundamente der Mathematik, Mengenlehre, Aussondern und Aufzählen, Verknüpfungen $\cap \cup \setminus$, Teilmengen $\subseteq \subsetneq \not\subseteq$, Potenzmengen, Russel-Antinomie

## LG3: Beweistechniken und die Praxis des Beweisens

Stichworte: Formulierung eines Satzes, mehrere Voraussetzungsteile, Formulieren eines Beweises, direkte/indirekte Beweise, Kontrapositionsbeweise, Widerspruchsbeweise, Beweise von Sätzen mit Quantoren, Schubfachprinzip, Fallunterscheidungen, effiziente Beweise (z.B. Ringschluss, Mengengl.), Heuristik

## LG4: Natürliche Zahlen und die vollständige Induktion

Stichworte: Peano-Axiome, Konstruktion der natürlichen Zahlen, Peano-Arithmetik, Rekursion/Iteration, Zeichen $\Pi$ und $\Sigma$, Grenzen der Peano-Arithmetik: Goodstein-Folgen, Prinzip der vollständigen Induktion, Beweise mit vollständiger Induktion

## LG5: Kartesische Produkte, Relationen, Ordnungen, Schranken/Supremum

Stichworte: Paare/Kuratowski und Kartesische Produkte, Relationen und namhafte Eigenschaften von Relationen, Ordnungen und totale Ordnungen, größtes/maximales Element, obere Schranke, Supremum, Zusammenhänge dieser Begriffe
[Kleinstes/minimales Element, untere Schranke, Infimum]

## LG6: Äquivalenzrelationen

Stichworte: $\sim$-Relation, $\sim$-klassen, Quotientenmengen, solche mit algebraischen Strukturen $+ \cdot$, Konstruktion der Zahlbereiche mit $\sim$-Relationen

## LG7: Abbildungen / Funktionen

**Stichworte:** Def. Abbildung als Relation, Bild einer Teilmenge, Urbild einer Teilmenge, Abbildungstypen: surjektiv/injektiv/bijektiv, Komposition und (Rechts-/Links-) inverse Abb., $\mathrm{Sym}(X)$, besondere Abb.: charakteristische Abb., Folgen, Abbildungen bei Quotientenmengen

## LG8: Endliche Mengen

**Stichworte:** endliche Menge, Kardinalität $\#X = n$, Ergebnisse über endliche Mengen, Kombinatorik, Permutationen, $\binom{n}{k}$, Binomialsatz, Multinomialsatz, Potenzreihen als kombinatorisches Hilfsmittel

## LG9: Große Zahlen und unendliche Mengen

**Stichworte:** große Zahlen, abzählbar unendlich, $\mathbb{N}, \mathbb{Z}$ und $\mathbb{Q}$ sind gleichmächtig, Lemma von Cantor, überabzählbar, $\mathcal{P}(\mathbb{N})$ und $\mathbb{R}$ sind überabzählbar, Cantorsche Diagonalverfahren, Hilberts Hotel, Wachstum divergenter Folgen

## LG10: Das Auswahlaxiom

**Stichworte:** Familien, beliebige (Durch-) Schnitte/Vereinigungen/Produkte, Auswahlaxiom, dazu äquivalente Formulierungen (surj. $\Rightarrow \exists$ Rechtsinverse, bel. Produkte nichtleerer Mengen sind $\neq \emptyset$, Lemma von Zorn, jeder VR hat eine Basis), Fixpunktsatz von Bourbaki impliziert mit dem Auswahlaxiom das Lemma von Zorn

## LG11: Die ZFC-Axiome

**Stichworte:** alle 10 ZFC-Axiome mit Besprechung, Erweiterungen von ZFC, Widerspruchsfreiheit von ZFC, Gödelsche Unvollständigkeitssätze, Kontinuumshypothese

# Vorlesung "Logische Grundlagen"

## LG1: Mathematische Grundbegriffe und Aussagenlogik

Stichworte: Sprache der Mathematik, Abstrakter Formalismus, Deduktion durch Einsetzen, Induktion, Axiomensysteme, Satz, Aussage, Verknüpfungen $\wedge \vee \neg$, Klammersetzungsregeln, Implikation, Äquivalenz, Logikregeln, erste Beweistheorie

---

## §1: Einstimmung: Zur Sprache der Mathematik

Das Wort Definition ist aus dem Lateinischen und bedeutet "Abgrenzung". In Definitionen versuchen wir, die Bedeutung von Symbolen und Begriffen so klar wie nur möglich festzulegen. In der Mathematik werden häufig Begriffe der Umgangssprache (wie z.B. Gruppe, Ring, Körper, Abbildung, ...) umgewidmet und ihnen spezielle neue Bedeutungen gegeben, so dass eine Fachsprache entsteht. Neben dem Anspruch, die Begriffe der Fachsprache sauber zu definieren, möchte man auch Aussagen über diese soweit wie möglich beweisen, d.h. mithilfe logischen Schlussfolgerns zu verifizieren. Das bedeutet, mit(Anwendung der) klarer logischer Regeln zu zeigen, dass diese wahr sind. Dabei greift man auf möglichst wenige Begriffe, Aussagen und Regeln zurück (sogenannte Axiome als Grundbausteine der Mathematik) und baut auf diesen auf. Die Axiome als solche werden dann nicht mehr hinterfragt, sondern als gegeben und wahr akzeptiert, wenn sie als klar und einleuchtend erscheinen. Diese Herangehensweise wurde im Laufe der Mathematikgeschichte immer wieder heftig diskutiert und bis heute hinterfragt, wie z.B. das sogenannte Auswahlaxiom.
Dennoch spricht in der täglichen Praxis der Mathematik nichts gegen diese Vorgehensweise: üblicherweise baut man auf dem sogenannten ZFC-Axiomensystem auf (dessen Axiome wir in dieser Vorlesung mal sehen werden) und wendet die gewöhnlichen Schlüsse der Aussagenlogik an. Wie letzteres geht, wollen wir hier als erstes erarbeiten.

## Vom Sinn der Abstraktion:

"Deduktion":
- wird einem ein abstrakter Zusammenhang genannt, so kann man ihn verstehen, indem man ihn auf Beispiele zurückführt und diese studiert.
  [Wenn man z.B. den Satz des Pythagoras erfährt, kann man ihn z.B. am rechtwinkligen Dreieck mit den Katheten der Länge 3 und 4 überprüfen.]

"Induktion":
- studiert man sehr viele Beispiele, so soll eine Abstraktion dann helfen, einen gefundenen Zusammenhang für alle machbaren Beispiele zu formulieren.
  [Nachdem er viele rechtwinklige Dreiecke und seine Seitenlängen studiert hat, wird ein denkendes Mensch irgendwann den Satz des Pythagoras formulieren.]

Das Zusammenspiel zwischen Deduktion und Induktion ist Wesen des wissenschaftlichen Denkens an sich. Die Mathematik erlaubt es, mit ihrer abstrakten Formelsprache ("Formalismus"), hier unterstützend zu wirken: Zur Deduktion braucht man nur erlaubte Objekte einsetzen, und sie ist so gemacht, dass man immer etwas einsetzen kann. Dafür dienen Variable, das sind Platzhalter, für die dazugesagt werden muss, welche Objekte eingesetzt werden dürfen, Bsp.: Ist $x$ eine gerade Quadratzahl, dann ist $x$ durch 4 teilbar. Zur Induktion würde man nach vielen Beispielen einen abstrakten Zusammenhang exakt formulieren. Dieser braucht noch lange nicht richtig sein, es wird ein Beweis zur Verifizierung erforderlich sein, dazu später mehr. Natürlich ist das Studium von Beispielen nicht der einzige Weg, Zusammenhänge zu finden, sondern auch die Regeln der Aussagenlogik sollen dafür erlaubt sein.

Wir formulieren zuerst, was ein guter abstrakter Formalismus idealerweise leisten soll:

## Ziele eines abstrakten Formalismus:

- alles soll unmissverständlich sein ["Tafelebene", "Verschiebung des Raums": ??]
- seine Spielregeln so klar, dass alles nachvollziehbar sein soll

Starke Vereinfachungen sind dabei nötig, die beschriebenen Objekte werden so auf ihre zu thematisierenden Aspekte reduziert. [Ob ein rechtwinkliges Dreieck grün ist, spielt für den Satz des Pythagoras keine Rolle.]

## Vom Sinn von Genauigkeit und sorgfältiger Sprache:

Wozu die Pedanterie im Studium mit exaktem Formalismus, mit dem z.B. die Zahlensysteme $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ erklärt werden? Kann man nicht wie in der Schule einfach darauf losrechnen? Wenn Sie einen hohen Turm aus Bierdeckeln bauen möchten, muss jeder einzelne Bierdeckel genau sitzen, sonst fällt der ganze Turm sehr leicht zusammen! In der Mathematik muss jeder Zwischenschritt stimmen, sonst kann man leicht auf falsche Aussagen wie das Ergebnis $0=1$ kommen. Z.B.: $-2 = \sqrt[3]{(-8)} = (-8)^{1/3} = (-8)^{2/6} = \sqrt[6]{(-8)^2} = \sqrt[6]{64} = 2$

also ist $0 = 2+(-2) = 2+2 = 4$, also $0=4$, also (nach Teilen durch 4) $0=1$ ???,
$\uparrow -2=2$ einsetzen

Also muss z.B. genau gesagt werden, was Wurzelausdrücke / Potenzgesetze sind. Die Begriffe und (Rechen-)regeln, die eingesetzt werden müssen unmissverständlich klar sein, d.h. u.a., dass ihr <u>Geltungsbereich</u> genau genannt wird!

Worauf wird die Mathematik nun aufgebaut? Auf einer bestimmten Liste von Axiomen, üblicherweise dem ZFC-Axiomensystem.
Nach einer Idee des Mathematikers David Hilbert zu Beginn des 20. Jahrhunderts hat man folgende Ansprüche, welche Eigenschaften ein <u>Axiomensystem</u> haben soll:
Hilberts Idee: Axiomensysteme sollten sein:

- <u>widerspruchsfrei</u>, d.h. es soll aus einem Satz nicht auch seine Negation herleitbar sein,
- <u>unabhängig</u>, d.h. jedes einzelne Axiom soll nicht aus den anderen des Systems herleitbar sein,
- <u>vollständig</u>, d.h. für jeden in der mathematischen Sprache formulierbaren Satz soll der Satz selbst oder seine Negation herleitbar sein
- <u>kategorisch</u>, d.h. alle Beispiele für ein Axiomensystem sind im Prinzip von der Struktur her gleich.

Es gibt Grenzen der Axiomatik: Kurt Gödel zeigte um 1930 den <u>Unvollständigkeitssatz</u>: In jedem mathematischen Axiomensystem existieren entweder wahre, jedoch nicht beweisbare Aussagen, oder aber das System ist widersprüchlich.

Eine mathematische wahre Aussage bezeichnen wir als (mathematischen) Satz.
Bsp.: Satz: Gerade Quadratzahlen sind durch 4 teilbar.
Dabei wird bereits vorausgesetzt, dass die Begriffe "gerade", "Quadratzahl", "teilbar", ja sogar die Zahl "4", bekannt sind und vorher sauber definiert wurden. Varianten des "Satzes" sind:

Theorem: ein besonders wichtiger Satz,
Lemma: ein Hilfssatz, welcher ein Zwischenresultat ausdrückt,
Korollar: ein Ergebnis, der ohne großem Beweisaufwand aus einem vorangehenden Satz erhältlich ist (griech. corollarium = Zugabe, Geschenk)
Proposition: ein Satz, der eher ein Hilfsergebnis ausdrückt

Def.: Eine Aussage besteht aus vollständig definierten Ausdrücken (die aus mathem. Objekten bestehen) und ist entweder wahr (w) oder falsch (f).

Von Aussagen der Umgangssprache kann der Wahrheitsgehalt nicht immer eindeutig festgestellt werden, Bsp.: Es regnet in Paris.
Wenn eine Aussage mit logischen Schlüssen als wahr erkannt wird, sprechen wir von einem Beweis. Ein Beweis ist also eine Folge von logischen Schlüssen, jeder auf den vorherigen aufbauend, an dessen Ende die zu beweisende Aussage steht.
Welche Regeln des Schlussfolgerns dabei erlaubt sind, erarbeiten wir hier.
Wir beachten: Beweise sind für Menschen gemacht, es genügt, nur so sehr ins Detail zu gehen, dass ein Mensch den Beweis versteht. Im Prinzip soll ein Beweis aber auch durch Ausführen aller Details sogar von Maschinen verifizierbar sein, ist dann aber durch vollen Formalismus gegeben. So einen Computerbeweis versteht normalerweise kein Mensch mehr und wird von Mathematikern auch nur m.E. akzeptiert.
Sobald eine Formel zu kompliziert wird, ist sie nicht mehr so leicht zu verstehen, z.B. bedeutet "$\forall t \in \mathbb{R}: (t>0 \vee t<0 \vee t=0) \wedge \neg(t>0 \wedge t<0) \wedge \neg(t>0 \wedge t=0) \wedge \neg(t<0 \wedge t=0)$", dass jede reelle Zahl positiv, negativ oder Null ist, aber keine zwei Eigenschaften gleichzeitig eintreten können.

## §2: Grundlegende Aussagenlogik

Wir möchten allgemein über Aussagen und ihre Wahrheitswerte sprechen.
Dazu nennen wir sie stellvertretend A, B, C, ... und nehmen darauf Bezug:
Ist eine Aussage A wahr, sagen wir auch kurz "A gilt", ansonsten "A gilt nicht".
Dabei sind A, B, ... gewissermaßen Variablen, in die konkrete Aussagen eingesetzt werden können, um Beispiele zu erhalten.

Bsp.: "2 ist gerade" gilt, "2 teilt 4" ist wahr, "18 ist Quadratzahl" ist falsch,
A ist eine Aussage. "A ist eine Aussage" ist eine Aussage.
↑(Im nachfolgenden Satz wurde für A etwas eingesetzt, nämlich die Aussage A selbst, beachten Sie, dass ich zur Klarstellung Gänsefüßchen gesetzt habe.)

Manche Mathematiker nennen Aussagen mit Aussagevariablen noch genauer eine Aussageform, diese haben erst nach Einsetzen einen festgelegten Wahrheitswert.

Aber: Aussagen mit Selbstbezug sollen nicht zugelassen werden.
Bsp.: "Diese Aussage ist falsch." macht keinen Sinn!

Verknüpfung von Aussagen: "und", "oder", "nicht"
in Zeichen: $A \wedge B$, $A \vee B$, $\neg A$

- per Wahrheitstafel können diese Verknüpfungen erklärt werden in Abhängigkeit der Wahrheitswerte von A und B, welche beliebige Aussagen sein können.

| A | B | $A \wedge B$ | $A \vee B$ | $\neg A$ |
|---|---|---|---|---|
| w | w | w | w | f |
| w | f | f | w | f |
| f | w | f | w | w |
| f | f | f | f | w |

Negation: - hierbei ist $\neg A$ wahr, genau dann wenn A falsch ist (lies "nicht A")
Konjunktion: - hierbei ist $A \wedge B$ genau dann wahr, wenn A und B beide wahr sind, ansonsten ist "$A \wedge B$" falsch (lies "A und B"),
Disjunktion: - hierbei ist $A \vee B$ genau dann falsch, wenn A und B beide falsch sind, ansonsten ist "$A \vee B$" wahr (lies "A oder B"). Hier ist nicht "entweder A oder B" gemeint, was falsch wäre wenn A und B beide wahr wären; es ist eine (nützliche) mathematische Konvention, "oder" immer so zu verstehen wie hier.

Bemerkung: • Die Aussagen $A \vee \neg A$ und $\neg(A \wedge \neg A)$ sind immer wahr!
• Die Reihenfolge ist unerheblich: $A \wedge B$ bedeutet $B \wedge A$, $A \vee B$ bedeutet auch $B \vee A$

Aus diesen Grundverknüpfungen lassen sich alle anderen wichtigen Aussagenverknüpfungen aufbauen. Und vielerlei Komplizierte Ausdrücke aufschreiben, wie z.B. $(A \vee B) \vee (C \wedge (\neg D))$, wobei es auf die Klammerung ankommt, welche die Reihenfolge der Verknüpfungen klarstellt.
So ist etwa $A \vee (B \vee (C \wedge (\neg D)))$ eine andere Aussage. Damit man nicht so viele Klammern schreiben muss und diese Formeln übersichtlicher schreiben kann, gibt es die folgenden Klammersetzungsregeln:

| $\neg$ bindet stärker als $\wedge$ |
| --- |
| $\wedge$ bindet stärker als $\vee$ |

Damit kann $(A \vee B) \vee (C \wedge (\neg D))$ einfacher als $A \vee B \vee C \wedge \neg D$ geschrieben werden. Zur Verdeutlichung/Klarstellung dürfen die Klammern natürlich trotzdem geschrieben werden. Weil $(A \vee B) \vee C$ dieselbe Aussage ist wie $(A \vee B) \vee C$ (überprüfen Sie das mit den Wahrheitswerten!), darf auch $A \vee B \vee C$ dafür geschrieben werden, und analog geht das ebenso mit $A \wedge B \wedge C$. (Das Wort "analog" wird immer dann benutzt, wenn ein Sachverhalt genauso richtig ist nach leichter Abänderung, hier nach Ersetzen von "$\vee$" durch "$\wedge$". Dieses Wort wird häufig benutzt, es spart Wiederholungen. Aber es sollte nur eingesetzt werden, wenn wie hier unmissverständlich klar ist, was gemeint ist.)

Die Implikation/Schlussfolgerung/Folgerung zweier Aussagen $A$ und $B$ ist die Aussage $\neg A \vee B$ und wird bezeichnet mit dem Symbol $A \Rightarrow B$, sprich "aus $A$ folgt $B$", "$A$ impliziert $B$", "wenn $A$ gilt, dann gilt $B$", "$A$ ist hinreichend für $B$", "$B$ ist notwendig für $A$", "damit $B$ gilt, ist hinreichend, dass $A$ gilt", "wenn $A$ gilt, muss $B$ notwendig auch gelten",...
und hat die Wahrheitswerte laut Tabelle:

| $A$ | $B$ | $A \Rightarrow B$ bzw. $\neg A \vee B$ |
| --- | --- | --- |
| w | w | w |
| w | f | f |
| f | w | w |
| f | f | w |

Laut Bedeutung von $\neg A \vee B$ gilt:
Ist $A$ wahr, also $\neg A$ falsch, dann muss $B$ stimmen, damit die Aussage insgesamt stimmt.
Damit wurde "wenn $A$ wahr ist, dann gilt $B$" ausgesagt, also eine Folgerung ausgedrückt. Ist $A$ falsch, ist $\neg A \vee B$ wahr, egal, was $B$ ist: "ex falso quodlibet" = "aus Falschem folgt Beliebiges".

Wir wollen "ex falso quodlibet" so zulassen: wenn wir es anders machen wollten, also z.B. "$A \Rightarrow B$" für falsch erklären, falls $A$ falsch und $B$ wahr/falsch ist hätte man andere Aussagen erklärt und nichts Neues, vgl. diese Tabelle:

| $A$ | $B$ | | $B$ | $A \wedge B$ | |
|---|---|---|---|---|---|
| w | w | w | w | w | |
| w | f | f | f | f | } alle mögl. für andere Setzung |
| f | w | f | w | f | |
| f | f | w | f | f | |
| | | ↑ | | | |
| | | $(A \wedge B) \vee (\neg A \wedge \neg B)$ | | | |

Aber auch sonst ist "ex falso quodlibet" ein nützliches Prinzip: Soll "$\Rightarrow$" Bestandteil von Formeln werden, ist es dann mit unserem Einsetzprinzip kompatibel: Die Formel "$\forall x \in \mathbb{R}: x > 3 \Rightarrow x^2 > 9$" ist richtig, egal welche reelle Zahl für $x$ eingesetzt wird, etwa

$x = 5$: $\underbrace{5 > 3}_{w} \Rightarrow \underbrace{5^2 > 9}_{w}$, $x = 2$: $\underbrace{2 > 3}_{f} \Rightarrow \underbrace{2^2 > 9}_{f}$, $x = -4$: $\underbrace{-4 > 3}_{f} \Rightarrow \underbrace{(-4)^2 > 9}_{w}$

Die Äquivalenz zweier Aussagen ist die Aussage $(A \Rightarrow B) \wedge (B \Rightarrow A)$, d.h. sie ist wahr genau dann, wenn $A$ und $B$ dieselben Wahrheitswerte besitzen. Wir schreiben $A \Leftrightarrow B$ für diese Aussage und lesen dafür "$A$ ist genau dann wahr, wenn $B$ gilt", "$A$ gilt genau dann, wenn $B$ gilt", "$A$ gdw. $B$", "$A$ ist dann und nur dann wahr, wenn $B$ wahr ist", "$A$ ist äquivalent zu $B$", "$A$ ist notwendig und hinreichend für $B$", ...

Anhand der Wahrheitstafel ist erkennbar, dass $A \Leftrightarrow B$ dieselben Wahrheitswerte wie $(A \wedge B) \vee (\neg A \wedge \neg B)$ hat; wir werden dies gleich noch auf anderem Wege sehen.

| $A$ | $B$ | $A \Leftrightarrow B$ |
|---|---|---|
| w | w | w |
| w | f | f |
| f | w | f |
| f | f | w |

Noch ein Paar Begriffe in diesem Zusammenhang: in einer Äquivalenz $A \Leftrightarrow B$ heißt $A \Rightarrow B$ die Hinrichtung, und $B \Rightarrow A$, was auch als $A \Leftarrow B$ geschrieben werden kann, die Rückrichtung. Wenn eine Implikation $A \Rightarrow B$ vorliegt, wie z.B. $x > 2 \Rightarrow x^2 > 4$, muss noch lange nicht die Rückrichtung gelten. Oft wird dies gefragt, da Äquivalenzen eine genauere Aussage ermöglichen, wie z.B. $(x > 2 \vee x < -2) \Leftrightarrow x^2 > 4$.

Zum Sparen von Klammern gibt es für $\Rightarrow, \Leftrightarrow$ folgende Klammersetzungsregeln:

- $\vee$ bindet stärker als $\Rightarrow$ bzw. $\Leftarrow$,
- $\Rightarrow$ bzw. $\Leftarrow$ bindet stärker als $\Leftrightarrow$

Weiter lassen Äquivalenzen die Formulierung zu, dass zwei Formeln in Aussagenvariablen dieselben Wahrheitswerte haben, z.B. in $(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$.

Dies nutzen wir jetzt, um wichtige Logikregeln zu formulieren und auch zu beweisen.

1. Satz: Es gelten die folgenden Logikregeln für beliebige Aussagen $A, B, C$:

(1) $A \Leftrightarrow \neg(\neg A)$

(2) $(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$ (3) $(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$

(4) $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ (5) $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$

(6) $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$ } Distributivgesetze

(7) $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$ }

Beweis: Zu (1): Ist $A$ wahr, dann ist $\neg A$ falsch, also $\neg(\neg A)$ wieder wahr.
Ist $A$ falsch, dann ist $\neg A$ wahr, also $\neg(\neg A)$ wieder falsch.
Also haben $A$ und $\neg(\neg A)$ dieselben Wahrheitswerte, egal was $A$ ist.

Zu (2) & (3): Sind ebenso klar, auch anhand der Wahrheitstafeln.

Zu (4): Sind $A, B$ beide wahr, ist $\neg(A \wedge B)$ falsch und ebenso $\neg A \vee \neg B$.
Sind $A, B$ beide falsch, ist $\neg(A \wedge B)$ wahr und ebenso $\neg A \vee \neg B$.
Haben $A, B$ verschiedene Wahrheitswerte, ist $\neg(A \wedge B)$ wahr und ebenso $\neg A \vee \neg B$.
In jedem Fall haben $\neg(A \wedge B)$ und $\neg A \vee \neg B$ dieselben Wahrheitswerte, egal was $A, B$ ist.

Zu (5): Haben $\neg(A \vee B) \overset{(1)}{\Leftrightarrow} \neg(\neg(\neg A) \vee \neg(\neg B)) \overset{(4)}{\Leftrightarrow} \neg(\neg(\neg A \wedge \neg B)) \overset{(1)}{\Leftrightarrow} \neg A \wedge \neg B$.

Zu (6): Checken der Wahrheitswerte fällt am leichtesten:

| $A$ | $B$ | $C$ | $B \vee C$ | $A \wedge (B \vee C)$ | $A \wedge B$ | $A \wedge C$ | $(A \wedge B) \vee (A \wedge C)$ |
|---|---|---|---|---|---|---|---|
| w | w | w | w | w | w | w | w |
| w | w | f | w | w | w | f | w |
| w | f | w | w | w | f | w | w |
| w | f | f | f | f | f | f | f |
| f | w | w | w | f | f | f | f |
| f | w | f | w | f | f | f | f |
| f | f | w | w | f | f | f | f |
| f | f | f | f | f | f | f | f |

Zu (7): $A \vee (B \wedge C) \overset{(1)}{\Leftrightarrow} \neg(\neg(A \vee (B \wedge C))) \overset{(5)}{\Leftrightarrow} \neg(\neg A \wedge \neg(B \wedge C)) \overset{(4)}{\Leftrightarrow} \neg(\neg A \wedge (\neg B \vee \neg C))$
$\overset{(6)}{\Leftrightarrow} \neg((\neg A \wedge \neg B) \vee (\neg A \wedge \neg C)) \overset{(5)}{\Leftrightarrow} \neg(\neg A \wedge \neg B) \wedge \neg(\neg A \wedge \neg C)$
$\overset{(4)}{\Leftrightarrow} (\neg(\neg A) \vee \neg(\neg B)) \wedge (\neg(\neg A) \vee \neg(\neg C)) \overset{(1)}{\Leftrightarrow} (A \vee B) \wedge (A \vee C)$. □

(Zeichen für ein Beweisende)

Dies war schon unser erster Beweis. Beachten Sie, dass wir für Regeln (5) und (7) im Beweis vorangehende Ergebnisse benutzt haben, was sehr elegant ist: wir müssen derart nicht mehr die Wahrheitstabellen durchgehen. Dabei ist für Sie nützlich, dass ich die verwendeten Regeln dazugenannt habe. Für (6) habe ich keinen einfacheren Beweis, der nur mit $\neg, \vee, \wedge$ auskommt, gefunden.

Nun wollen wir noch Logikregeln mit "$\Rightarrow$" und "$\Leftrightarrow$" aufstellen.
Zunächst halten wir folgende Umschreibungen fest:

- $(A \Rightarrow B) \overset{\text{Def.}}{\Leftrightarrow} \neg A \vee B \overset{(1)}{\Leftrightarrow} \neg A \vee \neg(\neg B) \overset{(4)}{\Leftrightarrow} \neg(A \wedge \neg B)$
- $(A \Leftrightarrow B) \overset{\text{Def.}}{\Leftrightarrow} (A \Rightarrow B) \wedge (B \Rightarrow A) \overset{\text{Def.}}{\Leftrightarrow} (\neg A \vee B) \wedge (\neg B \vee A)$
  $\overset{\text{Distr.}}{\Leftrightarrow} (\neg A \vee B) \wedge \neg B \vee (\neg A \vee B) \wedge A$
  $\Leftrightarrow \neg A \wedge \neg B \vee \underbrace{B \wedge \neg B}_{f} \vee \underbrace{\neg A \wedge A}_{f} \vee B \wedge A$
  $\Leftrightarrow (\neg A \wedge \neg B) \vee (A \wedge B)$.

Die letzte Zeile interpretieren wir als "A und B haben beide denselben Wahrheitswert"

2. Satz: Es gelten die Logikregeln für beliebige Aussagen $A, B, C$:

(1) $(A \Rightarrow B) \wedge A \Rightarrow B$ — modus ponens
(2) $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$ — Kontrapositionsregel
(3) $(A \Rightarrow B) \wedge \neg B \Rightarrow \neg A$ — modus tollens
(4) $(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$ — Transitivität von "$\Rightarrow$"
(5) $(A \Leftrightarrow B) \wedge (B \Leftrightarrow C) \Rightarrow (A \Leftrightarrow C)$ — Transitivität von "$\Leftrightarrow$"

Vor dem Beweis zur Bedeutung/Interpretation dieser Regeln:
Zu (1): Das ist die "Schlussfolgerung" schlechthin: Ist $A \Rightarrow B$ bewiesen, d.h. wahr unter der Annahme, dass $A$ wahr sei, und ist $A$ wahr, muss auch $B$ wahr sein. Man sollte also sagen, dass die Behauptung $B$ wahr ist unter der Voraussetzung $A$.
Zu (2): Die Begründung von "$A \Rightarrow B$" kann indirekt erfolgen, wenn ein Beweis der Richtigkeit von $\neg B \Rightarrow \neg A$ vorliegt, wie folgt: "$A \Rightarrow B$ gilt, denn wenn ansonsten $B$ falsch wäre (Achtung, Konjunktiv!), dann wäre auch schon $A$ falsch gewesen (schon wieder Konjunktiv!). Wir haben aber die Annahme $A$ für $A \Rightarrow B$ gemacht, daher kann also $B$ nicht falsch sein."
Bsp: "Wenn es regnet, dann ist die Straße nass" ist gleichbedeutend zu "Wenn die Straße trocken ist, dann regnet es nicht."
Zu (4): Die Schlusskette $(A \Rightarrow B) \wedge (B \Rightarrow C)$ zeigt $A \Rightarrow C$.
Diese schreibt man kurz als $A \Rightarrow B \Rightarrow C$.
⚠ Vorsicht: Dies ist eine andere Aussage als $(A \Rightarrow B) \Rightarrow C$ oder $A \Rightarrow (B \Rightarrow C)$!!
Zu (5): Analoges gilt für Äquivalenzketten $A \Leftrightarrow B \Leftrightarrow C$. Vgl. Beweise oben!

**Beweis des 2. Satzes:**

Zu (1): Denn in den Zeilen der Wahrheitstabelle für $A \Rightarrow B$, wo $A \Rightarrow B$ wahr ist und ebenso $A$ wahr (das ist dort nur die 1. Zeile!), ist auch $B$ wahr.

Oder so: $((A \Rightarrow B) \wedge A \Rightarrow B) \Leftrightarrow (\neg(A \Rightarrow B) \vee \neg A \vee B) \Leftrightarrow (\neg(\neg A \vee B) \vee \neg A \vee B)$

$\Leftrightarrow (A \wedge \neg B) \vee \neg A \vee B \Leftrightarrow (A \wedge \neg B) \vee \neg(A \wedge \neg B)$, ist immer wahr.

Zu (2): $(A \Rightarrow B) \Leftrightarrow (\neg A \vee B) \Leftrightarrow (B \vee \neg A) \Leftrightarrow \neg(\neg B) \vee \neg A \Leftrightarrow (\neg B \Rightarrow \neg A)$.

Zu (3): $(A \Rightarrow B) \wedge \neg B \overset{(2)}{\Leftrightarrow} (\neg B \Rightarrow \neg A) \wedge \neg B \overset{(1)}{\Rightarrow} \neg A$.

Zu (4): $((A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)) \Leftrightarrow \neg((\neg A \vee B) \wedge (\neg B \vee C)) \vee (\neg A \vee C)$

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

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

$\Leftrightarrow \neg B \vee \neg A \vee B \vee C \Leftrightarrow (B \vee \neg B) \vee (\neg A \vee C)$, ist immer wahr.

Zu (5): $(A \Leftrightarrow B) \wedge (B \Leftrightarrow C) \Rightarrow (A \Leftrightarrow C)$ gilt,

denn $(A \Rightarrow B) \wedge (B \Rightarrow A) \wedge (B \Rightarrow C) \wedge (C \Rightarrow B)$

$\Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow C) \wedge (C \Rightarrow B) \wedge (B \Rightarrow A) \overset{(4)}{\Rightarrow} (A \Rightarrow C) \wedge (C \Rightarrow A) \Leftrightarrow (A \Leftrightarrow C)$. □

Bemerkung: Haben wir hier nicht die zu zeigenden Aussagen beim Beweisen bereits verwendet? Ein berechtigter Einwand! Generell darf keine Vermischung von Objekt- und Metasprache erfolgen, um die Beweise zu führen. Dies kann hier aber noch sauberer argumentiert werden, was wir der Übersichtlichkeit halber lassen.

Kurze Lehre mathematischer Beweise: Bewiesen werden soll ein Satz, der als Implikation formuliert wurde, d.h. in der Form: "Satz: $A \Rightarrow B$"

Dabei heißt $A$ die Voraussetzung, und $B$ die Behauptung des Satzes.

Man unterscheidet die folgenden zwei Arten von Beweisen:

1. direkter Beweis: Angabe einer Schlusskette $A \Rightarrow C_1 \Rightarrow C_2 \Rightarrow \ldots \Rightarrow C_n \Rightarrow B$
2. indirekter Beweis: Hier gibt es wieder zwei Arten:
   - Kontrapositionsbeweis: direkter Beweis von $\neg B \Rightarrow \neg A$
   - Widerspruchsbeweis: direkter Beweis von $A \wedge \neg B \Rightarrow C$, wobei $C$ falsch wie z.B. $A \wedge \neg A$, $0=1$, ...
     - Dies zeigt $A \Rightarrow B$, da $(A \wedge \neg B \Rightarrow \underbrace{C}_{f}) \Leftrightarrow (\underbrace{\neg(A \wedge \neg B)}_{A \Rightarrow B} \vee \underbrace{C}_{f}) \Leftrightarrow (A \Rightarrow B)$.
     - Wenn $C = \neg A$ ist ebenso, da $(A \wedge \neg B \Rightarrow \neg A) \overset{\text{Def.}}{\Leftrightarrow} (\neg(A \wedge \neg B) \vee \neg A) \Leftrightarrow (\neg A \vee B) \overset{\text{Def.}}{\Leftrightarrow} (A \Rightarrow B)$

Gerade das indirekte Schließen in Widerspruchsbeweisen werden wir noch genauer in Beispielen behandeln, speziell auch Tipps zum Aufschreiben geben.

# Vorlesung "Logische Grundlagen"

## LG 2: Prädikatenlogik, Quantoren, einfache Mengenlehre

**Stichworte:** Prädikate, Quantoren $\forall \exists \exists!$, Umgang mit Quantoren, Fundamente der Mathematik, Mengenlehre, Aussondern und Aufzählen, Verknüpfungen $\cap \cup \setminus$, Teilmengen $\subseteq \subsetneq \not\subseteq$, Potenzmengen, Russel-Antinomie

---

## §1: Prädikatenlogik und Quantoren

Unser "Einsetzprinzip" mit Variablen soll im Folgenden in einem genaueren Rahmen erklärt werden. Wir gelangen auf diesem Wege zur Prädikatenlogik, welche diesem Prinzip entspricht und zusammen mit der Aussagenlogik eine Beschreibungsmöglichkeit mathematischer Zusammenhänge liefert.

**Def.:** Ein **Prädikat** ist ein Ausdruck mit Platzhaltern (**Variablen**) so, dass wannimmer man die Variablen durch Objekte des für die Variablen erlaubten Geltungsbereichs ersetzt (d.h. etwas EINSETZT), eine Aussage entsteht.

**Bsp.:** • "Jede gerade Quadratzahl ist durch 4 teilbar." ist eine atomare Aussage ohne Variable. Gemeint ist: 4 ist durch 4 teilbar, 16 ist durch 4 teilbar, 36 ist durch 4 teilbar...

Beispiele für Prädikate:

→ Wollen sagen: "Ist $x$ eine gerade Quadratzahl, dann ist $x$ durch 4 teilbar."
($x$: Variable, wo gerade Quadratzahlen eingesetzt werden dürfen)

• "$x - y$ ist eine Quadratzahl" ($x, y$ sind Zahlen, etwa natürliche Zahlen)

→ Bsp.: $\underset{x=3}{3} - \underset{y=5}{5}$ ist eine Quadratzahl (f), $\underset{x=29}{29} - \underset{y=4}{4}$ ist eine Quadratzahl (w).

• "$x > 2 \Rightarrow x^2 > 4$", welche wahr für alle reellen Zahlen $x$ ist

Bsp.: $3 > 2 \Rightarrow 3^2 > 4$, da $3 > 2$ w und $3^2 > 4$ w, etc.,
vgl. "ex falso quodlibet"

• "Ist $x$ gerade Zahl, mindestens 4, dann ist $x$ Summe von zwei Primzahlen", (Goldbachsche Vermutung), Wahrheitswert unbekannt.

Durch Hintanfügen von Quantoren an Prädikaten entstehen neue Aussagen:

Def.: Sei ein Prädikat $P(x)$ gegeben, wo $x$ die Variable eines bestimmten Geltungsbereichs ist.

- Der Allquantor $\forall$ bedeutet "Für alle",
  in Formeln: $\forall x : P(x)$ ist die Aussage "Für alle $x$ ist $P(x)$ richtig",
  also entsteht durch Einsetzen eines beliebigen $x$ des Geltungsbereichs die wahre Aussage $P(x)$.
- Der Existenzquantor $\exists$ bedeutet "Es existiert",
  in Formeln: $\exists x : P(x)$ ist die Aussage
  "Es gibt (mindestens) ein $x$ so, dass $P(x)$ richtig ist",
  also entsteht durch Einsetzen von mindestens einem $x$ des Geltungsbereichs
  die wahre Aussage $P(x)$.
- Der Existenzquantor $\exists!$ bedeutet "Es existiert genau ein",
  in Formeln: $\exists! x : P(x)$ ist die Aussage
  "Es gibt genau ein $x$ so, dass $P(x)$ richtig ist",
  also entsteht durch Einsetzen von ganz genau einem einzigen $x$ des Geltungsbereichs
  die wahre Aussage $P(x)$.

Den Doppelpunkt spricht man meist als "so, dass".

Bem.: 1. Ist $P(x)$ ein Prädikat von nur einer Variablen $x$, so "bindet" ein Quantor diese Variable und es entsteht eine Aussage.

2. Ist $P(x,y,z,\dots)$ ein Prädikat von mehreren Variablen $x,y,z,\dots$, so entsteht durch Quantifizierung in $x$ ein Prädikat in den Variablen $y,z,\dots$,
   (nämlich $\forall x : P(x,y,z,\dots)$, $\exists x : P(x,y,z,\dots)$, $\exists! x : P(x,y,z,\dots)$ ).

3. "Es gibt höchstens ein $x$..." kann zurückgeführt werden auf
   "Es gibt kein $x$ mit... oder es gibt genau ein $x$ mit..."
   (dies ist die Negation von "es gibt ein $x$ mit...")
   Dafür wird (meist) kein separates Quantorenzeichen benutzt

Ü Wie könnte also der Filmtitel "Highlander - es kann nur einen geben" für einen Mathematiker in seiner "Sprache" formuliert werden?

## Regeln zur Negation von Prädikaten mit Quantoren:

Es gilt:

$$\neg(\forall x: P(x)) \iff \exists x: \neg P(x)$$
$$\neg(\exists x: P(x)) \iff \forall x: \neg P(x)$$

} Bei Negation "kehren sich die Quantoren um".

1. Bsp.: "Es ist nicht so, dass jeder Tisch grün ist."
$\iff$ "Es gibt einen Tisch, der nicht grün ist."
2. Bsp.: "Es ist nicht so, dass es einen grünen Tisch gibt."
$\iff$ "Kein Tisch ist grün." $\iff$ "Alle Tische sind nicht grün."
3. Bsp.: (ü) Was ist die Verneinung von $\exists! x: P(x)$ ?

Im Bsp.: x ist Variable für Tische, $P(x)$ ist "x ist grün", dann beschreiben die Formeln im Kasten genau diese Aussagen

## Die Reihenfolge von Quantoren ist wesentlich:

Sei t eine Variable für Töpfe, d eine Variable für Deckel. Weiter sei $P(d,t)$ das Prädikat "Der Deckel d passt auf den Topf t". Dann ist:

$\forall t\ \exists d: P(t,d)$ bedeutend zu "Zu jedem Topf gibt es einen passenden Deckel."

$\exists d\ \forall t: P(t,d)$ bedeutend zu "Es gibt einen Deckel, der passt auf jeden Topf."

Das bedeutet offensichtlich etwas verschiedenes!

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:

## 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 in kleinste "Bausteine" zerlegen.

## §2: Elementare Mengenlehre

**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 $2 \in G$, $5 \notin G$.

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 keine Rolle spielt: $\{1,2\} = \{2,1\}$ usw.
(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",
für den vertikalen Strich "|" darin kann auch ":" oder ";" geschrieben werden. (man sagt auch "so dass" bzw. "für die gilt")
**Bsp:** Wird die Menge der natürlichen Zahlen $1, 2, 3, \dots$ mit $\mathbb{N}$ bezeichnet, so ist $\{x \in \mathbb{N} \mid \underbrace{x \text{ ist gerade}}_{\text{ist ein Prädikat } P(x)}\} = \{2, 4, 6, 8, \dots\}$ die Menge der geraden Zahlen. (↑ Kommas stehen für "und", wie fast immer)

- 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.
- Weitere wichtige Bezeichnungen für Zahlbereiche sind $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, \dots\}$ (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 ($\rightsquigarrow$ vgl. Analysis).

## Vom Definieren und der sinnvollen Wahl von Notationen:

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. 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.

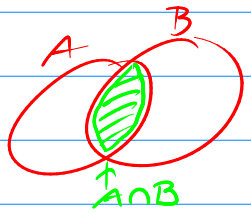
Für Variablen hatten wir bereits Kleinbuchstaben $x, y, z, t, d, \ldots$ benutzt.

Für Prädikate kann man mit $P(x) :\Leftrightarrow$ (Formel/Aussage in $x$) definieren, z.B. $P(x) :\Leftrightarrow x > 0$.

## Mengenverknüpfungen $\cap, \cup, \setminus$

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

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

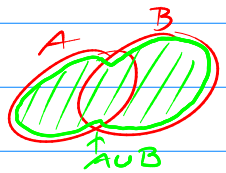



Die Menge $A \cap B$ heißt (Durch-)Schnitt von $A$ und $B$.
Die Elemente von $A \cap B$ sind genau die Elemente von $A$ und von $B$, d.h. $x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$.

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

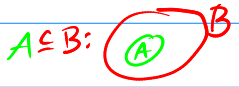
Bem.: Für jede Menge $A$ gilt $A \cap \emptyset = \emptyset$, $A \cap A = A$.

- 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

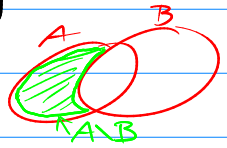



Zwei Mengen sind gleich genau dann, wenn sie die gleichen Elemente enthalten, also $A = B :\Leftrightarrow (\forall x \in A : x \in B) \wedge (\forall x \in B : x \in A)$. Gilt $A = B$, so kann in einer Formel mit $B$ dann auch $A$ eingesetzt werden und umgekehrt.

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.: $A \subseteq B :\Leftrightarrow \forall x \in A : x \in B$.

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.
Den 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 $A \not\subseteq B :\Leftrightarrow \neg(A \subseteq B)$ 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 $\{1,2\} \not\subseteq \{2\}$, $\overset{\text{Def.}}{\{1\} \subsetneq \{1,5\}}$, $\{1\} \subseteq \{1,5\}$.
(Ü) Gilt eine Implikation zwischen $A \subsetneq B$ und $A \not\subseteq B$?

- Sind $A$ und $B$ Mengen, so heißt $A \setminus B := \{x \in A \mid x \notin B\}$ das Komplement von $B$ in $A$. Lies "$A$ ohne $B$".
Gelegentlich schreibt man $A - B$ ("$A$ minus $B$"), eher selten.




Bsp: $\{3,2,4,5\} \setminus \{1,2,4,6\} = \{3,5\}$.
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.

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:

- 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.

[Noch eine ganz andere Bemerkung am Rande zum "guten Aufschreiben": warum schreibe ich hier nicht "Hat $A$ $n$ Elemente, so hat $\mathcal{P}(A)$ $2^n$ Elemente."? Weil dann im Satz Formelteile zusammentreffen, was Verwirrung stiften kann! Versuchen Sie, dies zu vermeiden durch Umformulierung, etwa wie hier. Auch sollte ein deutscher Satz nie mit einer Zahl/Formel beginnen, stellen Sie nach Möglichkeit eine Beschreibung davor wie "Die Zahl 2 ist positiv" statt "2 ist positiv". Das sehen Sie sicher ein. 3.14 am Satzanfang taugt nix.]

Es ist wichtig, mit den Mengenbegriffen sauber zu hantieren. 1901 wies Bertrand Russel darauf hin, dass allzu naive Konstruktionen mit Mengen zu Widersprüchen führen kann, bekannt als Russelsche Antinomie bzw. Russelsches Paradox: Es gibt Mengen, die sich offensichtlich nicht selbst als Element enthalten: Alle bisher betrachteten Beispiele für Mengen $A$ erfüllen $A \notin A$. Betrachte nun die Russel-Menge $R := \{A \mid A \notin A\}$. Gilt $R \in R$, muss $R \notin R$ gelten und umgekehrt! Die Auflösung dieses Paradox ist zu sagen, dass $R$ keine Menge ist.

# Vorlesung "Logische Grundlagen"

## LG3: Beweistechniken und die Praxis des Beweisens

**Stichworte:** Formulierung eines Satzes, mehrere Voraussetzungsteile, Formulieren eines Beweises, direkte/indirekte Beweise, Kontrapositionsbeweise, Widerspruchsbeweise, Beweise von Sätzen mit Quantoren, Schubfachprinzip, Fallunterscheidungen, effiziente Beweise (z.B. Ringschluss, Mengengl.), Heuristik

---

## §1: Praktische Beweistheorie

zunächst ein

**Nachtrag zu Quantoren:**

1 ist äqu. zu:
- $\forall t,\ G(t): H(t)$ "Alle Tische, die grün sind, sind 1m hoch"
- $\forall t: G(t) \Rightarrow H(t)$ "Alle Tische erfüllen: ist der Tisch grün, dann ist er 1m hoch"

⚠ Ist aber nicht äqu. zu: $\forall t: G(t) \wedge H(t)$ "Alle Tische sind grün und 1m hoch"

2 ist äqu. zu:
- $\exists t,\ G(t): H(t)$ "Es gibt einen grünen Tisch, der 1m hoch ist"
- $\exists t: G(t) \wedge H(t)$ "Es gibt einen Tisch, der grün ist und 1m hoch"

⚠ Ist aber nicht äqu. zu: $\exists t: G(t) \Rightarrow H(t)$ "Es gibt einen Tisch mit der Eigenschaft: Wenn er grün ist, dann ist er 1m hoch"
↪ ist auch wahr, wenn es nur einen roten Tisch gibt!

**Zur Formulierung von Sätzen**

Mathematische Sätze in der Form "Satz: $A \Rightarrow B$" (A: Voraussetzung, B: Behauptung) benutzen fast immer Quantoren, was wir hier in Anwendungsbeispielen studieren möchten:

**1. Bsp.:** Satz: Sind $U, V$ nichtleere Mengen mit $U \cap V = \emptyset$, dann ist $V \not\subseteq U$.
(Vor. A; "$\Rightarrow$"; Beh. B)

Auch formulierbar als:
- $\forall U, V$ nichtleere Mengen, $U \cap V = \emptyset: V \not\subseteq U$. ①
- $\forall U, V$ Mengen: $\underbrace{U \neq \emptyset}_{A_1} \wedge \underbrace{V \neq \emptyset}_{A_2} \wedge \underbrace{U \cap V = \emptyset}_{A_3} \Rightarrow \underbrace{V \not\subseteq U}_{B}$. ②

Haben: ① $\Leftrightarrow$ ② laut obiger Bem. 1!

Als kompletter deutscher Satz z.B.: • Von zwei disjunkten nichtleeren Mengen kann die eine nicht Teilmenge der anderen sein.

LG3

-2-

Wir besprechen nun eine Anwendung von LG1:

Hatten in Notiz LG1 folgendes Lemma: Für beliebige Aussagen $A, B, C$ gilt:

$$(A \wedge B \Rightarrow C) \Leftrightarrow (A \Rightarrow (B \Rightarrow C))$$

Nach diesem Lemma ist $A_1 \wedge A_2 \wedge A_3 \Rightarrow B \Leftrightarrow A_1 \wedge A_2 \Rightarrow (A_3 \Rightarrow B)$ richtig, so dass wir folgern: (2) $\Leftrightarrow \forall U, V$ Mengen, $U \neq \emptyset \wedge V \neq \emptyset$: $U \cap V = \emptyset \Rightarrow V \not\subseteq U$.

"Für zwei nicht leere Mengen $U, V$ gilt: Ist $U \cap V = \emptyset$, dann ist $V \not\subseteq U$."

Wir merken uns: Ist in der Behauptung eines Satzes eine Implikation $A_2 \Rightarrow B$ formuliert, können die Voraussetzungen um $A_2$ ergänzt werden.

Ein Satz in der Formulierung: "Satz: Vor.: $A_1$
Beh.: $A_2 \Rightarrow B$"

ist also äquivalent zur Formulierung: "Satz: Vor.: $A_1 \wedge A_2$
Beh.: $B$" (Beweis: s. Lemma!)

Wenn man die Bedeutung eines Satzes/einer Aufgabenstellung erschließen will, kann man auf diesem Wege auch alle Voraussetzungen zusammenfassen, was oft einfacher/verständlicher sein kann.

Als praktischen Tipp: Schreiben Sie Ihre Lösung von Klausur-/Übungsaufgaben in der Form wie hier auf als: "Vor.: ...
Beh.: ...
Bew.: ... □"

} Dies ist für Ihren Korrektor übersichtlich und klar!

Als Beweis-Ende-Markierung dient das Zeichen "□"
oder auch "qed" = quod erat demonstrandum
bzw. "wzbw" = was zu beweisen war.

Der Satz im 1. Bsp wäre dann z.B. schreibbar als:

Vor.: Seien $U, V$ Mengen mit $U \neq \emptyset \wedge V \neq \emptyset \wedge U \cap V = \emptyset$.
Beh.: $V \not\subseteq U$.

Alternativ z.B.: Vor.: Seien $U, V$ Mengen mit $U \neq \emptyset \wedge V \neq \emptyset$.
Beh.: Gilt $U \cap V = \emptyset$, dann ist $V \not\subseteq U$.

Bemerkung: "Seien" bzw. "Sei" ist Konjunktiv I für "Sind", "Ist", weiter "gelte" von "gilt"...
Typischerweise drückt man Annahmen/Voraussetzungen auf diese Weise im Konjunktiv I aus.

2. Bsp.: Satz: Gerade Quadratzahlen sind durch 4 teilbar.

→ Umformulierung: Vor.: Sei $n$ gerade Quadratzahl. (Konjunktiv, um Annahme/Vor. auszudrücken)

Beh.: 4 teilt $n$.

In Formeln: Vor.: $n \in \mathbb{N}, \exists m \in \mathbb{N} : n = 2m, \exists k \in \mathbb{N} : n = k^2$. (Kommas heißen "und")

Beh.: $\exists \ell \in \mathbb{N} : n = 4\ell$.

Das Zerlegen der Aussage einer Aufgabe in ihre Bestandteile ist oft hilfreich wie hier, meist liegt der Beweis danach auf der Hand.

Zu Beweisen

Hier: "Bew.: Ist $n = 2m = k^2$, so folgt, dass $k$ gerade ist, also $k = 2j$ mit $j \in \mathbb{N}$.

Dann ist $n = k^2 = (2j)^2 = 4 \cdot j^2$, also ist mit $\ell = j^2$ die Beh. richtig. □"

Ein Bew. in Bsp. 1 wäre etwa:

"Bew.: Ist $U \neq \emptyset \neq V$ mit $U \cap V = \emptyset$, dann ist $x \in V \setminus U$ für jedes $x \in V$,

da $V \neq \emptyset$ folgt also $\exists x \in V : x \notin U$, also $\neg(\forall x \in V : x \in U)$, also $\neg(V \subseteq U)$. □"

Bem. dazu: • Anstelle der Wörter "Ist", "dann ist", "für jedes", "also" könnte man auch die entsprechenden Symbole $\Rightarrow$, $\forall$ usw. einsetzen, wenn man den Beweis ganz im "Kalkül" formulieren möchte. Diese drücken aber "Meta"-Überlegungen aus, wie Sie schließen, d.h. wie Sie eine Schlusskette aufbauen, so dass es sich anbietet, für den Leser des Beweises dies so klarzustellen. Symbole und "Meta"-Wörter zu sehr mischen (etwa nur ein "also" durch "$\Rightarrow$" zu ersetzen) ist meist verwirrend und sollte möglichst vermieden werden.

• Das Wort "also" mehrmals zu verwenden ist völlig ok, solche Wiederholungen sind erwünscht: Wir schreiben keine Deutschaufsätze, sondern möchten präzise und verständlich sein.

• Die Formulierung "$P(x)$ gilt für jedes $x \in V$" heißt "$\forall x \in V : P(x)$",

"$P(x)$ gilt für ein $x \in V$" heißt "$\exists x \in V : P(x)$".

Manche Leute schreiben "$P(x)$ gilt $\forall x \in V$", oder "$P(x)$ $\forall x \in V$", was eigentlich nicht erlaubt ist, da "Meta"-wörter durch Formelwörter ersetzt sind. Und die zweite Version ist darüberhinaus möglicherweise missverständlich.

Haben gesagt: Vor. ↓ Beh. ↓

Direkter Beweis von $A \Rightarrow B$: Angabe einer Schlusskette $A \Rightarrow C_1 \Rightarrow C_2 \Rightarrow \dots \Rightarrow C_k \Rightarrow B$ aus bekannten Implikationen $A \Rightarrow C_1$, $C_1 \Rightarrow C_2$, …, $C_k \Rightarrow B$.

Dies zeigen wir in noch einem weiteren Bsp.:

**3. Bsp.:** Satz: Sei $x$ reelle Zahl mit $x^2 = 1$. Dann ist $x = 1 \vee x = -1$.

Beweis: $x^2 = 1 \overset{\text{Umformen}}{\Rightarrow} x^2 - 1 = 0 \overset{\text{3. Bin. Formel}}{\Rightarrow} (x-1)(x+1) = 0 \overset{\text{Lemma: } xy = 0 \Leftrightarrow x = 0 \vee y = 0}{\Rightarrow} x - 1 = 0 \vee x + 1 = 0 \overset{\text{Umformen}}{\Rightarrow} x = 1 \vee x = -1$. □

- Hier ist die "Schlusskette" sehr klar. Ausführlicher mit "Meta"-sprache wäre etwa so:

Beweis: Sei $x^2 = 1$. Nach Umformen erhalten wir $x^2 - 1 = 0$. Die Anwendung der 3. binomischen Formel zeigt dann, dass $(x-1)(x+1) = 0$ ist. Weil im Bereich der reellen Zahlen ein Produkt genau dann Null ist, wenn einer der Faktoren Null ist, folgt $x - 1 = 0$ oder $x + 1 = 0$. Also ist (wieder nach Umformen) $x = 1$ oder $x = -1$. qed

- Fraglich, was übersichtlicher ist! Eine ausführliche Version kann deutlich verständlicher sein. Was besser ist, kommt im Einzelnen darauf an.

## Indirekte Beweise

1. Die erste Art des indirekten Beweises ist der Kontrapositionsbeweis, d.h. der direkte Beweis von $\neg B \Rightarrow \neg A$. Unter der Annahme $\neg B$ (die neue Vor. in diesem Beweis) wird $\neg A$ hergeleitet mittels einer Schlusskette $\neg B \Rightarrow C_1 \Rightarrow C_2 \Rightarrow \dots \Rightarrow C_k \Rightarrow \neg A$.

Beim Aufschreiben eines solchen Beweises muss zunächst $\neg B$ formuliert werden als Annahme, die manchmal auch im Konjunktiv steht.

**4. Bsp.:** Satz: Vor.: Sei $k \in \mathbb{N}$ und $10^k$ nicht durch 4 teilbar. Beh.: $k = 1$.

Bem.: Haben hier: $A_1 \wedge A_2 \Rightarrow B$, d.h. $\neg B \Rightarrow \neg A_1 \vee \neg A_2$ ~> 1. Version

Äquivalent dazu ist: $A_1 \Rightarrow (A_2 \Rightarrow B)$, d.h. $A_1 \Rightarrow (\neg B \Rightarrow \neg A_2)$ -> 2. Version

Bew. in 1. Version: Ist $k \neq 1$, dann ist $k \notin \mathbb{N}$ oder (wenn $k \in \mathbb{N}$) $k \geq 2$.

Also ist $k \notin \mathbb{N}$ oder (wenn $k \in \mathbb{N}$) $10^k = 4 \cdot 25 \cdot \underbrace{10^{k-2}}_{\in \mathbb{N},\ \text{da } k-2 \geq 0}$ durch 4 teilbar. □

Die 2. Version ist einfacher und klarer:

Bew. in 2. Version: Sei (für diesen Beweis) $k \in \mathbb{N}$. Ist $k \neq 1$, dann ist also $k \geq 2$.

Es folgt, dass $10^k = 4 \cdot 25 \cdot \underbrace{10^{k-2}}_{\in \mathbb{N},\ \text{da } k-2 \geq 0}$ durch 4 teilbar ist. □

Fazit: In Kontrapositionsbeweisen möchten wir "Grundannahmen" wie "Geltungsbereiche" als unveränderten Voraussetzungsteil beibehalten. Die Verwendung des Konjunktivs nur dafür macht "Grundannahmen" deutlich.

2. Die zweite Art des indirekten Beweises ist der Widerspruchsbeweis, dabei wird $A \wedge \neg B \Rightarrow C$ bewiesen (wo C falsch ist wie $0=1$ "Widerspruch"), was äqu. ist zu $A \Rightarrow B$, vgl. LG1.
Ein Widerspruchsbeweis ist also die Herleitung eines Widerspruchs C aus der Annahme $\neg B$ (und der Voraussetzung A), d.h. unter der Annahme, die Behauptung B sei falsch.

[Manche Leute verstehen das Wort "Annahme" nur so wie hier als Annahme des Gegenteils einer Behauptung in einem Widerspruchsbeweis. Nein: eine "Annahme" ist generell eine Voraussetzung, die man als wahr annimmt...]

Das Aufschreiben eines Widerspruchsbeweises geschieht in drei Schritten:
1. Formulierung der Annahme $\neg B$, wie z.B. "angenommen, B gelte nicht"
2. Formulierung eines direkten Beweises von $A \wedge \neg B \Rightarrow C$, d.h. die Herleitung von C aus der Annahme $\neg B$ und der Vor. A.
3. Feststellung, dass C falsch (oder $C \Leftrightarrow \neg A$) ist: "Widerspruch", "↯", und Beweis-Ende.

5.Bsp.: Satz: Für $x>9$ hat die Glg. $\sqrt{x} = 2$ keine Lösung.
Beweis (durch Widerspruch):
1. Angenommen, $x \in \mathbb{R}$ sei eine Lösung der Glg. $\sqrt{x} = 2$.
2. Dann folgt $2 = \sqrt{x} > \sqrt{9} = 3$, also $2 > 3$.
(↑ da $x>9$ und die $\sqrt{}$-Fkt. streng mon. w.)
3. Widerspruch, da $2>3$ falsch ist. □

Kürzer: Beweis (durch Widerspruch): Andernfalls / Ansonsten sei $x \in \mathbb{R}$ mit $\sqrt{x}=2$.
Dann folgte $2 = \sqrt{x} > \sqrt{9} = 3$, also wäre $2>3$ ↯. □

"Ja wenn die Gleichung eine Lösung x hätte, dann wäre $2=\sqrt{x}>\sqrt{9}=3$, was aber falsch ist." → Hier wird das indirekte Schließen mit dem Konjunktiv II (hätte/wäre..) ausgedrückt. Manche sagen, ein Widerspruchsbeweis sollte der Genauigkeit halber komplett im Konjunktiv II ausgedrückt werden, um den "irrealen Sachverhalt", der zum Widerspruch geführt wird, zu verdeutlichen. Bei langen Widerspruchsbeweisen würde ich nur die Annahme $\neg B$ im Konjunktiv II formulieren.

## Beweise von Sätzen mit Quantoren

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

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

$\exists k$: $2^{2^9}+1$ 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 $>1$ zusammengesetzt ist).

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

Oft kann eine solche explizite Konstruktion wie hier nicht geschafft werden. Gelegentlich kommen "Abzählargumente" zum Einsatz, das bekannteste ist das Dirichletsche Schubfachprinzip (engl. pigeonhole principle):

Werden $k$ Objekte auf $n$ Mengen $M_1, \dots, M_n$ verteilt, und ist $k > n$, so existiert eine Menge $M_j$, die (mind.) zwei Objekte enthält.

Heißen die Objekte $a_1, \dots, a_k$ (paarweise verschieden, d.h. $\forall u,v \in \{1,\dots,k\}, u \neq v : a_u \neq a_v$), dann folgt aus dem Prinzip:

$$\exists j \in \{1,\dots,n\}\ \exists u,v \in \{1,\dots,k\} : u \neq v \wedge a_u, a_v \in M_j.$$

[Eine andere Formulierung: Gilt $M = \bigcup_{i=1}^{n} T_i$ und hat $M$ genau $k$ Elemente ($k > n$), dann ex. ein $T_i$ mit mehr als einem Element.]

Beachten Sie, dass eine Menge $M_j$ mit mehr als einem Objekt nicht explizit angegeben werden kann. Alle Beweise, die auf diesem Prinzip beruhen, sind nicht konstruktiv in dem Sinne, dass sie reine Existenzbeweise sind, d.h. keine Konstruktion ermöglichen.

7. Bsp.: Satz: Es gibt im vollbesetzten Hörsaal M1 zwei Menschen, die am gleichen Tag Geburtstag haben.

Beweis: Im M1 haben 400 Personen Platz, das Jahr hat (maximal) 366 Tage. Nach dem Schubfachprinzip haben mind. 2 Personen am gleichen Tag Geburtstag. □

[Wer dies ist, kann der Beweis nicht sagen!]

Ein Beweis des Schubfachprinzips: Wenn die Beh. nicht stimmt, enthält in jeder Menge $M_i$ höchstens ein Element, dann gibt es höchstens soviele Elemente $k$ wie "Fächer" $M_i$, also $k \leq n$. □

2. Beweis eines Satzes mit dem Allquantor $\forall$: Satz: $A \Rightarrow \forall x \in M : P(x)$ (Voraussetzung; Behauptung 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 $M = M_1 \cup M_2 \cup \dots \cup M_n$ und beweist $P(x)$ für jedes $x \in M_i$, $i \in \{1, \dots, n\}$, 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:

8. Bsp., für 2.a): Satz: Für alle natürlichen Zahlen $k \leq 4$ 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.

9. Bsp., für 2.b): Satz: Für alle reellen Zahlen $x, y$ gilt $4xy \leq (x+y)^2 \leq 2(x^2+y^2)$.

Bew.: Zur 1. Beh. $4xy \leq (x+y)^2$: Es gilt $(x-y)^2 \geq 0 \Leftrightarrow x^2 - 2xy + y^2 \geq 0 \Leftrightarrow x^2 + 2xy + y^2 \geq 4xy$
$\Leftrightarrow (x+y)^2 \geq 4xy$.

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

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

10. Bsp., für 2.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. □

## Varianten von Beweisen ~> u.a.: "effiziente" Beweise

(1) **Der Ringschluss:** Hat eine Behauptung die Form $B_1 (\Leftrightarrow) B_2 (\Leftrightarrow) \dots (\Leftrightarrow) B_k$, z.B. als "... dann sind folgende Aussagen äquivalent: 1) $B_1$, 2) $B_2$, ..., k) $B_k$", so muss nicht jede Äquivalenz einzeln gezeigt werden! Es genügt, nur Beweise von 1.) $B_1 \Rightarrow B_2$, 2.) $B_2 \Rightarrow B_3$, 3) ..., k.) $B_k \Rightarrow B_1$ zu erbringen!
Ein Beweis von z.B. $B_2 \Leftarrow B_3$ folgt daraus bereits über den "Umweg" $B_3 \Rightarrow B_4 \Rightarrow \dots \Rightarrow B_k \Rightarrow B_1 \Rightarrow B_2$, und analog für die anderen Implikationen.
Hier wird ein Beweis effizient organisiert, indem für den Beweis überflüssige Implikationen ausgelassen werden. Der Ringschluss ist kein Zirkelschluss, wo fälschlicherweise die zu zeigende Behauptung in einem (falschen) Beweis verwendet wird.

(2) **Mengenvergleiche:** Soll die Gleichheit zweier Mengen $U = V$ gezeigt werden, genügt es, die beiden Behauptungen $U \subseteq V$ und $U \supseteq V$ einzeln zu beweisen. Meistens ist eine der beiden Inklusionen $\subseteq, \supseteq$ leicht zu zeigen.

**11. Bsp.:** Satz: Seien $U, V$ Mengen. Ist $U \subseteq V$, dann gilt $V \cup U = V$.
Beweis: „$\supseteq$" ist klar, zu „$\subseteq$": Sei $x \in V \cup U$, dann ist $x \in U$ oder $x \in V$.
Fallunterscheidung:
- Ist $x \in U$, so folgt $x \in V$ weil $U \subseteq V$ vorausgesetzt wurde.
- Ansonsten ist auch $x \in V$.

Somit folgt für jedes $x \in V \cup U$, dass $x \in V$ gilt, d.h. es folgt $V \cup U \subseteq V$. □

Bem.: Alternativen in Fallunterscheidungen sind mit "oder" verknüpft, denn $x \in M_1 \cup M_2 \cup \dots \cup M_n$ bedeutet $x \in M_1 \vee x \in M_2 \vee \dots \vee x \in M_n$.

(11) Zeigen Sie: Satz: Seien $U, V$ Mengen. Ist $U \subseteq V$, dann gilt $V \cap U = U$.
Wie ändert sich der obige Beweis hier?

(3) **Widerlegen von Sätzen / Beweise von negierten Quantorenaussagen:**

a) Ist ein Satz der Form $A \Rightarrow \forall x : P(x)$ zu widerlegen, wird $\neg(A \Rightarrow \forall x : P(x))$ gezeigt, was äqu. ist zu $A \wedge \neg(\forall x : P(x)) \Leftrightarrow A \wedge \exists x : \neg P(x)$. Dazu muss ein $x$ angegeben werden, für dass $\neg P(x)$ gilt, also ein Gegenbeispiel angegeben/konstruiert bzw. dessen Existenz bewiesen werden (unter der Vor. $A$).

b) Ist ein Satz der Form $A \Rightarrow \exists x : P(x)$ zu widerlegen, wird $\neg(A \Rightarrow \exists x : P(x))$ gezeigt, was äqu. ist zu $A \wedge \neg(\exists x : P(x)) \Leftrightarrow A \wedge \forall x : \neg P(x)$. Dazu muss für jedes $x$ dann $\neg P(x)$ gezeigt werden (unter der Vor. $A$).

# Vorlesung "Logische Grundlagen"

## LG4: Natürliche Zahlen und die vollständige Induktion

**Stichworte:** Peano-Axiome, Konstruktion der natürlichen Zahlen, Peano-Arithmetik, Rekursion/Iteration, Zeichen $\Pi$ und $\Sigma$, Grenzen der Peano-Arithmetik: Goodstein-Folgen, Prinzip der vollständigen Induktion, Beweise mit vollständiger Induktion

---

## §1: Konstruktion der natürlichen Zahlen

Die natürlichen Zahlen $\mathbb{N}_0 = \{0, 1, 2, ...\}$ werden erklärt durch ihre Eigenschaften, die von G. Peano axiomatisch formuliert wurden.
Diese sogenannten Peano-"Axiome" lauten wie folgt:
$\mathbb{N}_0$ ist eine Menge mit (i) einem Element $0 \in \mathbb{N}_0$, (ii) für jede natürliche Zahl $n \in \mathbb{N}_0$ gibt es einen Nachfolger $s(n) \in \mathbb{N}$,
(iii) $\forall n \in \mathbb{N}_0 : s(n) \neq 0$ „0 ist nicht Nachfolger einer nat. Zahl"
(iv) $\forall m, n \in \mathbb{N}_0 : s(m) = s(n) \Rightarrow m = n$. „Eindeutigkeit des Vorgängers"
(v) $\forall X$, $X$ Menge, $0 \in X : (\forall n \in X : s(n) \in X) \Rightarrow \mathbb{N}_0 \subseteq X$. „Induktionsprinzip"
Letztere Eigenschaft (v) besagt: Eine Menge, die 0 und mit jeder nat. Zahl $n$ darin auch ihren Nachfolger $s(n)$ enthält, enthält alle nat. Zahlen.
Auf dem Prinzip (v) beruht das Beweisverfahren der vollständigen Induktion, welches wir hier einführen und wofür wir später nützliche Varianten zeigen werden.
Die Eigenschaften (i)-(v) sind keine "echten" Axiome, da sie aus den Axiomen der Mengenlehre (die ZFC-Axiome) und denen der Prädikatenlogik (z.B. Hilbert-Kalkül) hergeleitet werden können:

### Existenz der natürlichen Zahlen

Die Existenz einer Menge $\mathbb{N}_0$ mit diesen Eigenschaften kann man nun wie folgt durch Angabe einer Konstruktion zeigen, die (i)-(v) erfüllt. Das ist etwa diese:
Ist $0 := \emptyset$ und für $n \in \mathbb{N}_0$ der Nachfolger $s(n)$ def. durch $s(n) := n \cup \{n\}$, haben wir
$0 := \emptyset$, $1 := s(0) = \emptyset \cup \{\emptyset\} = \{\emptyset\}$, $2 := s(1) = s(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$
$3 := s(2) = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}$, ...

Nun muss für diese Konstruktion gezeigt werden (mit den ZFC-Axiomen und der Prädikatenlogik wie z.B. im Hilbert-Kalkül gegeben), dass (i)-(v) gelten. Das stellt sich als machbar heraus. Insbesondere muss dafür das Unendlichkeitsaxiom verwendet werden, welches im wesentlichen besagt, dass es Mengen mit unendlich vielen Elementen gibt. Die präzise Fassung des Axioms lernen wir später noch kennen, wenn wir die ZFC-Axiome auflisten werden; nach diesem ist $\mathbb{N}_0$ eine unendliche Menge. Den Beweis für (i)-(v) lassen wir hier weg.

[Eine alternative Konstruktion von $\mathbb{N}_0$ ist $0 := \emptyset$, $s(n) := \{n\}$, d.h. $1 := \{\emptyset\}$, $2 := \{\{\emptyset\}\}$, ..., für diese kann ebenso (i)-(v) gezeigt werden, aber auch nicht einfacher.]

Man kann mit $s(n)$ die übliche Addition "+" erklären, nämlich mit

$$n+0 := n, \quad n+1 := s(n),$$

sowie $n+2 := s(s(n)), \ldots, \quad n+m := \underbrace{s(s(\ldots s(n))\ldots)}_{m\text{ mal } s \text{ anwenden}},$

bzw. $n+(m+1) := s(n+m)$ für alle $m \in \mathbb{N}_0$ ($s(m)$)

Die Addition hat dann die bekannten Rechenregeln als Eigenschaften (Assoziativität, ...).

Die Peano-Axiome und ihre daraus resultierenden Rechengesetze bezeichnet man als Peano-Arithmetik.

Das Axiom (v) von Peano hängt eng zusammen mit dem Begriff einer

**rekursiven/induktiven Definition:**

Sei $x(n)$ ein Objekt, welches von einer nat. Zahl $n \in \mathbb{N}_0$ abhängt, und sei eine feste Bildungsvorschrift $F$ gegeben, mit der ein neues Objekt $F(x(n))$ gebildet wird. Dieses nennen wir $x(n+1)$, d.h. $x(n+1) := F(x(n))$.

Zusammen mit einem Startwert $x(0)$ [oder irgendeinem $x(n_0)$ mit $n_0 \in \mathbb{N}$] erhalten wir eine Folge von Objekten

$$x(0),\ x(1) = F(x(0)),\ x(2) = F(F(x(0))),\ x(3) = F(F(F(x(0)))), \ldots$$
$$\ldots\ x(n) = \underbrace{F(F(\ldots F(x(0))\ldots))}_{n\text{-mal}} \ldots$$

- Diese Folge kann also durch Angabe von
  $x(0), \quad x(n+1) := F(x(n))$ definiert werden (rekursiv/induktiv)
- Ebenso kann dieselbe Folge iterativ definiert werden durch Angabe von
  $x(0), \quad x(n) := \underbrace{F(F(\ldots F(x(0))\ldots))}_{n\text{-mal}}$ mit "Pünktchen".
  Hier wird eine Definition

als eine (n-fache) Wiederholung von $F$ ausgedrückt.

Bei der rekursiven Definition wird auf bereits vorher definierte Objekte zurückgegriffen, um den Wert des "nächsten" Objekts für $n+1 = s(n)$ zu erklären. Das muss nicht nur ein einziges vorher definiertes Objekt sein, die Bildungsvorschrift $F$ kann auch mehrere Objekte betreffen, also z.B. $x(n+1) := F(x(1), x(2), x(n))$ oder $x(n+1) := F(x(n-2), x(n-1))$, ... sind möglich, wenn genügend Startwerte gegeben sind.

Schreibweisen mit "Pünktchen" sind meist gewisse Aufzählungen, die vom Kontext her klar sind, sie meinen meist eine iterative Bildungsvorschrift. Sie können durch eine rekursive Bildungsvorschrift oder explizite Angabe präzisiert werden. Hier einige Beispiele:

| Folge | Pünktchen | iterativ | rekursiv | explizit |
|---|---|---|---|---|
| Quadratzahlen | $1, 4, 9, 16, 25, 36, \ldots$ | $q_n = \underbrace{n+\ldots+n}_{n\text{ mal}}$ | $q_1 = 1,\ q_{n+1} = q_n + 2n + 1$ | $q_n = n^2$ |
| Dreieckszahlen | $1, 3, 6, 10, \ldots$ (Klar?) bzw. $1, 1+2, 1+2+3, \ldots$ (Klarer) | $d_n = 1+2+\ldots+n$ | $d_1 = 1,\ d_{n+1} = d_n + n + 1$ | $d_n = \frac{n(n+1)}{2}$ Kleines Gauß |
| Mengenvereinigungen | $X_1 = M_1,\ X_2 = M_1 \cup M_2, \ldots$ | $X_n = M_1 \cup \ldots \cup M_n$ | $X_1 = M_1,\ X_{n+1} = X_n \cup M_n$ | $X_n = \bigcup_{i=1}^{n} M_i$ |
| Mengendurchschnitte | $Y_1 = M_1,\ Y_2 = M_1 \cap M_2, \ldots$ | $Y_n = M_1 \cap \ldots \cap M_n$ | $Y_1 = M_1,\ Y_{n+1} = Y_n \cap M_n$ | $Y_n = \bigcap_{i=1}^{n} M_i$ |
| Summen | $a_1, a_1+a_2, a_1+a_2+a_3, \ldots$ | $s_n = a_1 + a_2 + \ldots + a_n$ | $s_1 = a_1,\ s_{n+1} = s_n + a_{n+1}$ | $s_n = \sum_{i=1}^{n} a_i$ |
| → Vielfache (von $a$) | $a, a+a, a+a+a, \ldots$ | $v_n = \underbrace{a+\ldots+a}_{n\text{-mal}}$ | $v_1 = a,\ v_{n+1} = v_n + a$ | $v_n = n \cdot a$ |
| Produkte = Fakultät | $a_1, a_1 \cdot a_2, a_1 \cdot a_2 \cdot a_3, \ldots$ bzw. $1, 1\cdot 2, 1\cdot 2\cdot 3, \ldots$ bzw. $1, 2, 6, 24, \ldots$ | $p_n = a_1 \cdot a_2 \cdot \ldots \cdot a_n$ $n! = 1 \cdot 2 \cdot \ldots \cdot n$ | $p_1 = a_1,\ p_{n+1} = p_n \cdot a_{n+1}$ $1! = 1,\ (n+1)! = (n!)\cdot(n+1)$ | $p_n = \prod_{i=1}^{n} a_i$ $n!$ |
| $(n$-te$)$ Potenz | $a, a\cdot a, a\cdot a\cdot a, \ldots$ | $P_n = \underbrace{a \cdot \ldots \cdot a}_{n\text{ mal}}$ | $P_1 = a,\ P_{n+1} = P_n \cdot a$ | $P_n = a^n$ |
| Fibonacci-zahlen | $0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$ | 2 jeder Versuch gibt unschöne Formeln | $f_1 = 0,\ f_2 = 1,\ f_{n+1} = f_{n-1} + f_n$ | $f_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$ (Binetsche Formel) |

- Da man häufig über Summen/Produkte/Potenzen spricht, hat man für sie die expliziten Zeichen $\sum_{i=n}^{m} a_i$, $\prod_{i=n}^{m} a_i$, $a^n$ $(=\prod_{i=n}^{n} a)$ erfunden. Ihre Definition ist wie oben rekursiv möglich. Dabei ist folgende Setzung der Startwerte nützlich:
  - Die leere Summe ist $:=0$, d.h. $\sum_{i=n}^{0} a_i := 0$.
  - Das leere Produkt ist $:=1$, d.h. $\prod_{i=n}^{0} a_i := 1$.

  (Die "leere Potenz" ist in diesem Sinne $a^0 := 1$.)

  Das Summenzeichen/Produktzeichen ist so zu verstehen, dass "$i$" ein Laufindex ist, der die Elemente von $\{1,2,\dots,n\}$ der Reihe nach "durchläuft". Eine Verallgemeinerung dieser Zeichen zu Laufindizes $i \in M$ mit einer geg. (endlichen) Menge $M$ ist möglich, häufig stehen sogar noch zusätzliche Bedingungen dabei, z.B.:

  $$M=\{2,4,6,8\} \rightsquigarrow \sum_{i\in M} a_i = \sum_{\substack{i\le 8 \\ i \text{ gerade}}} a_i = \sum_{\substack{i=1 \\ i \text{ gerade}}}^{8} a_i = \sum_{i=1}^{4} 2i = a_2+a_4+a_6+a_8.$$

  Sind die zusätzlichen Bedingungen unerfüllbar, d.h. falsch für die Elemente der Indexmenge, ist die Summe leer (also $=0$), bzw. das Produkt leer (also $=1$), z.B.: $\sum_{\substack{i=2 \\ 5 \text{ teilt } i}}^{4} a_i = 0$, $\prod_{\substack{i=2 \\ 5 \text{ teilt } i}}^{4} a_i = 1$.

- <u>Zusammenhang zwischen Rekursionen und dem Peano-Axiom (v):</u>
  Mit dem Peano-Axiom (v) kann man beweisen, dass stets eindeutig eine Folge existiert, die einer gegebenen rekursiven Bildungsvorschrift genügt. Laut diesem Satz ist es also möglich, Folgen über Rekursionen zu definieren. Da der Beweis dieses Satzes erstaunlich lang und kompliziert ist, lassen wir ihn hier weg.
- Weiter kann jede iterative Definition auch durch eine rekursive Definition ersetzt werden. Umgekehrt ist das nicht immer der Fall, wie man am Beispiel der Fibonacci-Folge sehen kann.
- Noch eine letzte theoretische Bemerkung zu den Peano-Axiomen: Die sogenannten <u>Goodstein-Folgen</u> lassen sich mit (i)-(v) definieren, aber ihre Eigenschaft, dass diese bei 0 enden (Satz von Goodstein), ist <u>nicht</u> mit (i)-(v) beweisbar. Um zu zeigen, dass Goodstein-Folgen bei 0 enden, müssen Verschärfungen von Axiom (v) herangezogen werden.

## Das Prinzip der Vollständigen Induktion (VI):

Es lautet:

(VI): $\forall A(x)$, Aussage/Prädikat in $x$: $A(0) \wedge (\forall n \in \mathbb{N}_0: A(n) \Rightarrow A(n+1)) \Rightarrow \forall n \in \mathbb{N}_0: A(n)$

und bedeutet: Für jede Aussage in $x$ gilt: Ist $A(0)$ wahr und ist für jede natürliche Zahl $n$ wahr, dass mit $A(n)$ auch $A(n+1)$ richtig ist, dann gilt die Aussage für alle natürlichen Zahlen $n \in \mathbb{N}_0$.

[anschaulich: $A(0) \Rightarrow A(1) \Rightarrow A(2) \Rightarrow A(3) \Rightarrow \ldots$]

Bem.:

1. Die Startaussage "$A(0)$" muss nicht unbedingt bei $n=0$ sein, das Prinzip ist auch für jeden anderen Startwert $n_0 \in \mathbb{N}$ richtig.
2. Die Startaussage "$A(0)$" heißt Induktionsanfang, die Implikation "$A(n) \Rightarrow A(n+1)$" heißt Induktionsschritt.
3. Nach dem Prinzip (VI) können Beweise von Aussagen über (alle) natürliche Zahlen geführt werden, man erhält so die Beweismethode der vollständigen Induktion, wofür wir gleich Beispiele bringen. Allerdings lässt sich nicht jede Aussage über natürliche Zahlen so beweisen.
4. Satz: Das Prinzip (VI) ist äquivalent zum Peano-Axiom (v).

Beweis: Halten (v): $\forall X$, $X$ Menge, $0 \in X: (\forall n \in X: s(n) \in X) \Rightarrow \mathbb{N}_0 \subseteq X$.

Zu (v) $\Rightarrow$ (VI): Zu $A(x)$ betr. $X := \{n \in \mathbb{N}_0;\ A(n) \text{ wahr}\}$. Da $A(0)$ gilt, ist $0 \in X$. Und aus $A(n) \Rightarrow A(n+1)$ für alle $n \in \mathbb{N}_0$ folgt, dass mit $n \in X$ stets $s(n) = n+1 \in X$ folgt. Nach (v) folgt $\mathbb{N}_0 \subseteq X$. Da $X \subseteq \mathbb{N}$ laut Def. von $X$ gilt, ist $\mathbb{N}_0 = X$. Also gilt $A(n)$ für alle $n \in \mathbb{N}_0$.

Zu (VI) $\Rightarrow$ (v): Zu $X$ betr. die Aussage $A(x) :\Leftrightarrow x \in X$. Da $0 \in X$ gilt, ist $A(0)$ wahr. Und aus $\forall n \in X: s(n) \in X$ folgt, dass aus $A(n)$ [d.h. $n \in X$] stets $A(n+1)$ folgt. Nach (VI) folgt, dass $A(n)$ für alle $n \in \mathbb{N}_0$ wahr ist, d.h. $\mathbb{N}_0 \subseteq X$. □

5. Jede explizite Formel für eine rekursiv definierte Zahlenfolge $z_0 \in \mathbb{N}_0$, $z_{n+1} := F(z_n)$ kann mit vollständiger Induktion bewiesen werden. Lautet $z_n = G(n)$ die zu zeigende explizite Formel, so gelingt der Induktionsschritt, falls $F(G(n)) = G(n+1)$ für alle $n \in \mathbb{N}$ gilt. Das sehen wir in den Beispielen.

1. Bsp.: Der Satz vom kleinen Gauß: Für die Dreieckszahlen $d_1 := 1$, $d_{n+1} = d_n + (n+1)$ gilt: $\forall n \in \mathbb{N}: d_n = \frac{n(n+1)}{2}$.

Beweis (vollst. Ind.):
- Induktionsanfang: ist $n = 1$, ist $d_1 = \frac{1(1+1)}{2}$ richtig.
- Induktionsschritt: ist für ein (beliebiges, aber festes) $n \in \mathbb{N}$ die Formel $d_n = \frac{n(n+1)}{2}$ richtig, dann folgt $d_{n+1} = d_n + (n+1) \overset{\text{Rekursion}}{=} \frac{n(n+1)}{2} + (n+1) \overset{\text{Induktions-voraussetzung}}{=} \frac{(n+1)(n+2)}{2} = \frac{(n+1)(n+1+1)}{2}$, also ist die Formel auch mit $n+1$ anstelle von $n$ richtig. Nach dem Prinzip (VI) folgt, dass die Formel für alle $n \in \mathbb{N}_0$ stimmt. □

ü 2. Bsp.: Für die Rekursion $w_1 = 2$, $w_{n+1} = w_n + (n+1)(n+2)$ kann so $w_n = \frac{n(n+1)(n+2)}{3}$ gezeigt werden.

Bem.: Wir zeigen noch zwei zum Induktionsprinzip äquivalente Varianten, die in der Praxis auch häufig benutzt werden. Ganz selten kommen sogar noch andere Varianten zum Einsatz, z.B. kann der Induktionsschritt durch die Implikationen $A(n) \Rightarrow A(2n)$, $A(n) \Rightarrow A(n-1)$ ersetzt werden.

Für die Variante brauchen wir noch das Zeichen "$\leq$" für natürliche Zahlen:

Def.: Für $n, m \in \mathbb{N}_0$ ist $n \leq m :\Leftrightarrow \exists\, k \in \mathbb{N}_0 : \underbrace{n+k}_{\text{wie oben definiert}} = m$.

Weiter: $n < m :\Leftrightarrow n \leq m \wedge n \neq m$.

1. Variante: (VI') Angenommen, $X \subseteq \mathbb{N}_0$ ist eine Teilmenge mit $0 \in X \wedge (\forall m \in \mathbb{N}_0, m < m: m \in X \Rightarrow m \in X)$. Dann ist $X = \mathbb{N}_0$.

2. Variante: (M) Jede nichtleere Teilmenge $X$ von $\mathbb{N}_0$ hat ein kleinstes Element $a \in X$, d.h. so dass $\forall m \in X: a \leq m$ gilt.

Satz: (VI) $\Leftrightarrow$ (VI') $\Leftrightarrow$ (M).

Beweis (durch Ringschluss):

[direkt] $\rightsquigarrow$ Zu (VI) $\Rightarrow$ (VI'): Sei $X \subseteq \mathbb{N}_0$ eine Menge, die die Eigenschaft in (VI') erfüllt. Setze $Y := \{n \in \mathbb{N}_0 \mid m \in X \text{ für alle } m \leq n\}$. Dann gilt $0 \in Y$. Wenn $n \in Y$, dann gilt $m \in X$ für alle $m \leq n$, also gilt dann $n+1 \in X$ [Eig. in (VI')] und damit auch $n+1 \in Y$. Es folgt $Y = \mathbb{N}_0$ [(VI) bzw. (V) auf $Y$ angewandt]. Da $Y \subseteq X \subseteq \mathbb{N}_0$ folgt $X = \mathbb{N}_0$.

Zu (VI') ⇒ (M): [durch Widerspruch]
Sei $\emptyset \neq X \subseteq \mathbb{N}_0$ eine nichtleere Menge, die kein kleinstes Element hat. Setze $Y := \mathbb{N}_0 \setminus X$.
Da 0 die kleinste nat. Zahl ist, folgt $0 \in Y$ [denn $0 \notin X$].
Wenn $\forall m < n: m \in Y$, so ist $n \notin X$, denn sonst wäre $n$ das kleinste Element von $X$.
Also gilt $n \in Y$. Nach (VI'), auf $Y$ angewandt, folgt $Y = \mathbb{N}_0$ und damit $X = \emptyset \lightning$.

Zu (M) ⇒ (VI): [durch Widerspruch] Ist $X \subseteq \mathbb{N}_0$ eine Menge, die die Eigenschaften in (v) [d.h. (VI)] erfüllt, setze $Y := \mathbb{N}_0 \setminus X$. Sei $Y \neq \emptyset$, dann gibt es laut (M) ein kleinstes Element $y \in Y$. Da $0 \in X$, ist $y > 0$. Folglich ist $y-1 \in X$, nach der Eigenschaft in (v) aber auch $y = (y-1)+1 \in X$, wir erhalten einen Widerspruch zu $X \cap Y = \emptyset$.
Deswegen ist doch $Y = \emptyset$, also $X = \mathbb{N}_0$. □

Bem.: Ebenso wie (v) ⇔ (VI) lässt sich eine Formulierung von (VI') finden, die zu Aussagen passt wie folgt:

$\forall A(x)$, Aussage/Prädikat in $x$: $A(0) \wedge (\forall n \in \mathbb{N}_0: (\forall m \in \mathbb{N}_0, m < n: A(m)) \Rightarrow A(n)) \Rightarrow \forall n \in \mathbb{N}_0: A(n)$

Diese Variante kommt etwa in mehrgliedrigen Rekursionen wie z.B. bei der Fibonacci-Folge (einer zweigliedrigen Rekursion $n-1, n \rightsquigarrow n+1$) zum Einsatz, wo die Richtigkeit der zu beweisenden Aussage/Formel nicht nur für $n$, sondern mehrere Vorgänger im Induktionsschritt angenommen werden muss. Für den Induktionsanfang müssen dann auch mehrere Startwerte überprüft werden.

3. Bsp.: Für die Folge $f_0 = 0, f_1 = 1, f_{n+1} = f_{n-1} + f_n$ der Fibonacci-Zahlen gilt $f_n = \frac{1}{\sqrt{5}}(\gamma^n - \gamma_0^n)$, wo $\gamma := \frac{1+\sqrt{5}}{2}$, $\gamma_0 := \frac{1-\sqrt{5}}{2}$.

Bew. (durch vollständige Induktion):
Ind.anfang: Für $n = 0$ ist $f_0 = 0 = \frac{1}{\sqrt{5}}(\gamma^0 - \gamma_0^0)$ wahr, für $n = 1$ ist $f_1 = 1 = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right)$ wahr.
Ind.schritt $n-1, n \rightsquigarrow n+1$: Sei die Formel wahr für $n-1$ und $n$, dann stimmt sie auch für $n+1$, weil gilt:

$$f_{n+1} = f_{n-1} + f_n = \frac{1}{\sqrt{5}}(\gamma^{n-1} - \gamma_0^{n-1} + \gamma^n - \gamma_0^n) = \frac{1}{\sqrt{5}}(\gamma^{n-1}\underbrace{(1+\gamma)}_{=\gamma^2} - \gamma_0^{n-1}\underbrace{(1+\gamma_0)}_{=\gamma_0^2})$$
$$= \frac{1}{\sqrt{5}}(\gamma^{n+1} - \gamma_0^{n+1}),$$

denn Nachrechnen zeigt: $\gamma^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+2\sqrt{5}+5}{4} = \frac{3+\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2} = 1+\gamma$

und analog: $\gamma_0^2 = \left(\frac{1-\sqrt{5}}{2}\right)^2 = \frac{1-2\sqrt{5}+5}{4} = \frac{3-\sqrt{5}}{2} = 1 + \frac{1-\sqrt{5}}{2} = 1+\gamma_0$. □

# Vorlesung "Logische Grundlagen"

## LG5: Kartesische Produkte, Relationen, Ordnungen, Schranken/Supremum

**Stichworte:** Paare/Kuratowski und kartesische Produkte, Relationen und namhafte Eigenschaften von Relationen, Ordnungen und totale Ordnungen, größtes/maximales Element, obere Schranke, Supremum, Zusammenhänge dieser Begriffe
[Kleinstes/minimales Element, untere Schranke, Infimum]

---

## §1: Kartesische Produkte

Die Elemente einer Menge haben keine bestimmte Reihenfolge,
z.B. $\{1,2\} = \{2,1\} = \{2,1,1\} = \{2,1,2,2\}$.

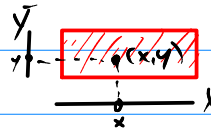
Man möchte aber auch eine Reihung von Elementen (die im Sinne der Mengenlehre auch selbst wieder Mengen sind) haben, speziell Paare von Mengen $(x,y)$ betrachten können, wo $x$ die erste Menge (= 1. Eintrag des Paars) und $y$ die zweite Menge (= 2. Eintrag des Paars) sein soll.
Dabei soll $(x,y) = (u,v)$ genau dann gelten, wenn $x=u$ und $y=v$ gilt.
Dies wird mit der Kuratowski-Konstruktion gelöst:

> Wir setzen $(x,y) := \{\{x\}, \{x,y\}\}$.
>
> Denn $(x,y) = (u,v)$ bedeutet dann ja $\{\{x\}, \{x,y\}\} = \{\{u\}, \{u,v\}\}$.
>
> Daraus folgern wir:
> - Ist $\{x\} = \{u\}$, so ist $x=u$ und $\{x,y\} = \{u,v\} \overset{x=u}{=} \{x,v\}$, also $v=y$.
> - Ist $\{x,y\} = \{u\}$, so ist $u=x=y$ und $\{x,y\} = \{u\} = \{x\}$, also $y=x=u=v=x$.

Man muss sich diese Konstruktion nicht merken.
Für uns ist nur wichtig, dass man in der Sprache der Mengen Paare $(x,y)$ mit der gewünschten Eigenschaft $(x,y) = (u,v) \Leftrightarrow x=u \wedge y=v$ bilden kann.

**Def.:** Sind $X$ und $Y$ Mengen, so besteht ihr kartesisches Produkt $X \times Y$ aus allen Paaren $(x,y)$ mit $x \in X$ und $y \in Y$, d.h.
$X \times Y := \{(x,y);\ x \in X \wedge y \in Y\}$. (sprich "X Kreuz Y")

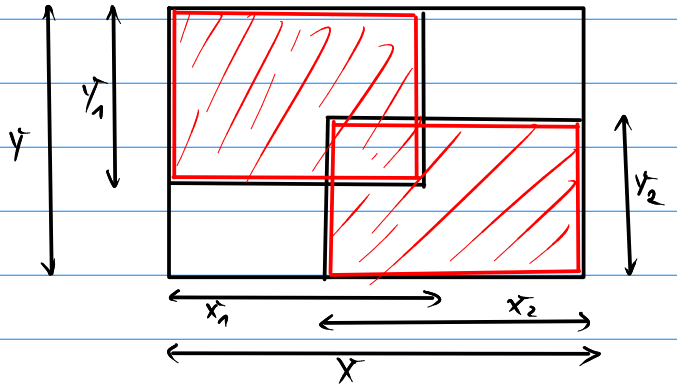
Graphische Anschauung:




"Kartesisches Koordinatensystem"

**Bsp.:** $\mathbb{R} \times \mathbb{R}$ ist eine Ebene, deren Punkte zwei reelle Koordinaten haben.

**Achtung:** Aus $X = X_1 \cup X_2$ und $Y = Y_1 \cup Y_2$ folgt noch lange nicht
$X \times Y = (X_1 \times Y_1) \cup (X_2 \times Y_2)$:




Ü Konstruieren Sie hierfür ein nichtgraphisches, formal richtiges Gegenbeispiel!

**Mehrfache Produkte:**

Für drei Mengen $X_1, X_2, X_3$ haben wir

$$(X_1 \times X_2) \times X_3 = \{((x_1, x_2), x_3) \mid x_1 \in X_1, x_2 \in X_2, x_3 \in X_3\}$$

sowie $$X_1 \times (X_2 \times X_3) = \{(x_1, (x_2, x_3)) \mid x_1 \in X_1, x_2 \in X_2, x_3 \in X_3\}.$$

Das ist zunächst ein formaler Unterschied, letztlich ist es aber egal, wie herum gruppiert wird, die Reihenfolge von $x_1, x_2, x_3$ steht fest. Wir nennen deswegen etwa $(x_1, x_2, x_3) := ((x_1, x_2), x_3)$ ein **Tripel** und bezeichnen in diesem Sinne mit $X_1 \times X_2 \times X_3 := \{(x_1, x_2, x_3) \mid x_1 \in X_1, x_2 \in X_2, x_3 \in X_3\}$ die Menge der Tripel.

Analog erhält man mit 4 Mengen **Quadrupel** usw.,
d.h. über die Rekursion $(x_1, x_2, \ldots, x_{n-1}, x_n) := ((x_1, \ldots, x_{n-1}), x_n)$ für $n \in \mathbb{N}$ können wir **n-Tupel** definieren.

Die Gleichheit zweier n-Tupel gilt dann ebenfalls komponentenweise.

Wir nennen $X_1 \times \ldots \times X_n$ das kartesische Produkt der Mengen $X_1, \ldots, X_n$, gelegentlich wird $\prod_{i=1}^{n} X_i$ dafür geschrieben.

Im Falle $X_1 = \ldots = X_n = X$ wird auch $X^n$ geschrieben,
also z.B. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ usw.

Mit dem kartesischen Produkt können nicht nur (mengentheoretisch) neue mathematische Objekte gebildet werden, andererseits dient es zur Def. des **Relationsbegriffs** (ein Spezialfall einer Relation ist die Abbildung/Funktion, vgl. später).

## §2: Relationen

**Def.:** Jede Teilmenge $R \subseteq X_1 \times \dots \times X_n$ von Mengen $X_1, \dots, X_n$ heißt **$n$-stellige Relation**.

Von besonderer Bedeutung sind die zweistelligen Relationen $R \subseteq X \times Y$.

**Bsp.:** $X = \{1,2\}$, $Y = \{1,3,5\}$, $R := \{(1,3), (1,5), (2,3), (2,5)\}$
ist die Relation "$<$", dabei ist $x < y \iff (x,y) \in R$ (im Sinne nat. Zahlen).
$\rightsquigarrow$ identifiziere $R$ mit $<$

Konvention: Schreiben $xRy$ für die Aussage $(x,y) \in R$.

**Beispiele für Relationen sind:** "$\leq$" und "$=$" in $\mathbb{N}$, "$\subseteq$" in Mengensystemen, "$\perp$" (senkrechtstehen) in der Menge aller Geraden, "$|$" (teilen) in $\mathbb{Z}$, ...

Im folgenden steht $R$ im abstrakten Sinne für so eine Relation ("Vergleich") von Elementen einer Menge $X$ mit denen einer anderen Menge $Y$ (laut Def. wie oben).
Oft ist $X = Y$, dann sagt man, es liegt eine zweistellige Relation in $X$ ($= Y$) vor.
Für Relationen sind vor allem folgende Eigenschaften von Interesse:

- Für $R \subseteq X \times Y$:

(1) $R$ **linkstotal** $:\iff \forall x \in X\ \exists y \in Y: xRy$
(2) $R$ **rechtstotal** $:\iff \forall y \in Y\ \exists x \in X: xRy$
(3) $R$ **bitotal** $:\iff$ (1) $\wedge$ (2)
(4) $R$ **linkseindeutig** $:\iff \forall x \in X\ \forall y \in Y\ \forall u \in X: xRy \wedge uRy \Rightarrow x = u$
(5) $R$ **rechtseindeutig** $:\iff \forall x \in X\ \forall y \in Y\ \forall v \in Y: xRy \wedge xRv \Rightarrow y = v$
(6) $R$ **eineindeutig** $:\iff$ (4) $\wedge$ (5)

- Für $R \subseteq X \times X$:

Anschaulich:

(7) $R$ **reflexiv** $:\iff \forall x \in X: xRx$ [$R$ enthält die "Diagonale" $\{(x,x); x \in X\}$]
(8) $R$ **symmetrisch** $:\iff \forall x,y \in X: xRy \Rightarrow yRx$ [$R$ ist symmetrisch zur "Diagonalen"]
(9) $R$ **asymmetrisch** $:\iff \forall x,y \in X: xRy \Rightarrow \neg(yRx)$ [$R$ ohne Diag. und ohne symmetrischen Paaren]
(10) $R$ **antisymmetrisch/identitiv** $:\iff \forall x,y \in X: xRy \wedge yRx \Rightarrow x = y$
[symmetrische Paare hat $R$ nur auf der Diagonalen]
(11) $R$ **konnex/linear** $:\iff \forall x,y \in X: xRy \vee yRx$ [je zwei El. können verglichen werden]
(12) $R$ **transitiv** $:\iff \forall x,y,z \in X: xRy \wedge yRz \Rightarrow xRz$

Bem.: • (7), (8), (12) def. eine Äquivalenzrelation → LG6
• (1), (5) def. eine Abbildung/Funktion → LG7
• Auf (7) bis (12) bauen sich die Ordnungsstrukturen ("$\leq$") auf, wir behandeln diese im Rest dieses Kapitels.

(Ü) Welche Eigenschaften haben die oben genannten Beispiele für Relationen? Welche Relationen kennen Sie noch?

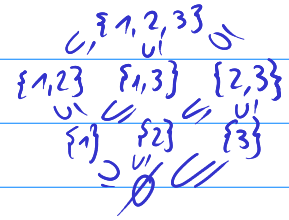
## §3: Ordnungen

Def.: • Eine Relation $R \subseteq X \times X$ heißt Ordnungsrelation/partielle Ordnung/Halbordnung in $X$, falls sie reflexiv (7), antisymmetrisch (10) und transitiv (12) ist.
• Eine Menge mit Ordnungsrelation heißt geordnete Menge.
• Eine Ordnungsrelation heißt Anordnung/totale Ordnung/lineare Ordnung, wenn sie zusätzlich konnex/linear (11) ist (11 wird manchmal auch "total" genannt).
• Eine Relation $R \subseteq X \times X$ heißt strenge Ordnungsrelation, wenn $R$ asymmetrisch (9) und transitiv (12) ist. Da (9) und (11) zusammen nicht gelten können, betr.
(11') $\forall x,y \in X: x \neq y \Rightarrow xRy \vee yRx$. Gilt (9) $\wedge$ (11') $\wedge$ (12), heißt die Relation eine strenge Anordnungsrelation.
• Eine Menge mit strenger (An-) Ordnungsrelation heißt streng (an) geordnete Menge.

Bem.: Die Eigenschaft (9) $\wedge$ (11') ist äquivalent zu:
(13) $R$ ist trichotomisch $:\Leftrightarrow \forall x,y \in X: xRy \dot{\vee} x=y \dot{\vee} yRx$
mit dem Zeichen "$\dot{\vee}$" für "entweder-oder",
gelegentlich wird dies zur Definition einer strengen Anordnungsrelation benutzt.

Wir machen die Begriffe Ordnung/Anordnung in Beispielen klar:

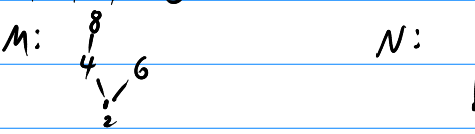
1. Sei $M$ eine (endliche) Menge und $X := \mathcal{P}(M)$ die Potenzmenge. Dann ist mit "$\subseteq$" eine Ordnungsrelation in $X$ erklärt. Wir schreiben $N_1 \subseteq N_2$ für $(N_1, N_2) \in \subseteq$.
z.B. $M = \{1,2,3\}$:




} der Übersichtlichkeit halber sind hier nicht alle Beziehungen mit "$\subseteq$" dargestellt, u.a. nicht $\emptyset \subseteq \emptyset$, $\{1\} \subseteq \{1\}$, usw.

2. Ebenso ist mit "$\subsetneq$" eine strenge Ordnungsrelation auf $X = \mathcal{P}(M)$ erklärt.

3. $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ bilden mit "$\leq$" jeweils eine total geordnete Menge.
4. Das Bsp. in 1. ist eine nicht total geordnete Menge, da $\{2\} \not\subseteq \{1,3\} \not\subseteq \{2\}$.
5. $\mathbb{N}$ ist mit "$|$" (teilen) geordnete Menge, aber nicht total, da $2 \nmid 5$, $5 \nmid 2$.
6. $M = \{2, 4, 6, 8\}$ ist mit "$|$" (teilen) geordnete Menge, aber nicht total geordnet:




$\rightsquigarrow$ es wird klar, warum eine totale Ordnung auch "lineare" Ordnung heißt: die Elemente einer total geordneten Menge lassen sich in einer Kette "linear" anordnen. Die Ordnungsbeziehungen von $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ lassen sich deswegen auf einem Zahlenstrahl / Zahlengeraden gut darstellen. Dies geht mit $\mathbb{C}$ nicht, jedenfalls nicht so, dass die Anordnung mit den Rechenregeln von $+, \cdot$ verträglich wäre:

- $i > 0 \overset{\text{Verträglichkeit von "} \leq \text{" mit "mal"}}{\Rightarrow} i \cdot i > 0 \cdot i = 0 \Rightarrow i^2 > 0 \Rightarrow -1 > 0$ ↯.
- $i < 0 \overset{\text{Verträglichkeit von "} \leq \text{" mit "mal"}}{\Rightarrow} i \cdot (-i) < 0 \cdot (-i) = 0 \Rightarrow -i^2 < 0 \Rightarrow 1 < 0$ ↯.

Daher bleibt man mit $\mathbb{C}$ anschaulich auf einer Zahlenebene, die man Komplexe Ebene nennt.

Die "Größen"vergleiche, die mit Ordnungsstrukturen möglich sind, führen zu neuen Begriffen über ausgezeichnete Elemente einer geordneten Menge:

**Def.:** Sei $X$ mit einer Relation, die wir "$\leq$" schreiben, geordnete Menge.

- $g \in X$ heißt <u>größtes Element</u> von $X$, falls $\forall x \in X: x \leq g$ (g ist mit allen El. von X vergleichbar)
  (g liegt über allen Elementen...) Notation: <u>grEl(X)</u>
- $m \in X$ heißt <u>maximales Element</u> von $X$, falls $\forall x \in X: m \leq x \Rightarrow x = m$ (m nicht unbedingt, aber unter den mit m vergleichbaren El. ist m das größte)
  (Kein El. ist größer als x: $\neg(\exists x \in X: \underbrace{m \leq x \wedge x \neq m}_{(m<x)})$) Notation: <u>max(X)</u>

(analog: <u>kleinstes / minimales Element</u>)

**Bem.:** Größtes und maximales Element sind i.a. <u>verschieden</u>! (immer: grEl ⇒ maxEl; "⇐" ist in total geordn. Mengen richtig)
Im 6. Bsp. oben gibt es in M kein größtes Element, da $6 \nmid 8$, aber 8 und 6 sind in M maximale Elemente, da alle mit 8 und 6 <u>vergleichbaren</u> Elemente kleinergleich 8 bzw. 6 sind.
In N ist $8 = \max(N) = \text{grEl}(N)$. Weiter: in $\mathbb{N}_0$ ex. <u>kein</u> max. El. und <u>kein</u> gr. El., aber $\mathbb{N}_0$ ist mit $\leq$ total geordnet.

**Satz:** Total geordnete Mengen besitzen höchstens ein maximales Element, das größtes Element ist, wenn es existiert. [Zusatz klar]

Erinnern Sie sich an den "High-landder"?

**Formal:** $\forall (X, \leq)$ total geordnete Menge $\forall m,n \in X$: $m$ ist $\max(X) \wedge n$ ist $\max(X) \Rightarrow m=n$.

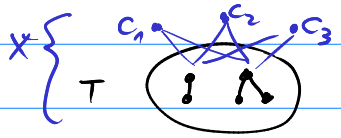
**Bew.:** Sei $(X, \leq)$ total geordnete Menge und $m, n$ seien maximale Elemente von $X$.
Dann ist $m \leq n$ oder $n \leq m$, weil die Menge total geordnet ist.
Somit gilt: Aus $m \leq n$ folgt $m = n$, da $n$ maximales Element.
Aus $n \leq m$ folgt $m = n$, da $m$ maximales Element.
In jedem Fall folgt $m = n$. □

**Bem.:** • Analog gilt der Satz mit minimalen/kleinsten Element.
Gibt es in total geordneten Mengen ein maximales/minimales Element, dürfen wir laut diesem Satz von dem (eindeutig bestimmten) maximalen/minimalen Element sprechen und den bestimmten Artikel benutzen. Dann dürfen wir auch $m = \max(X)$ bzw. $m = grEl(X)$ schreiben [Sonst: $m$ ist $\max(X)$, ...]

• Wird eine Ordnung $R$ in einer Menge $X$ auf eine Teilmenge $T \subseteq X$ eingeschränkt, so erhält man eine Teilordnung auf $T$, d.h. es wird $R_T := R \cap (T \times T)$ gebildet.

## §4: Schranken und Supremum/Infimum

**Bem.:** Sei $X$ mit $\leq$ geordnet und $T \subseteq X$, so dass die Teilordnung auf $T$ untersucht werden kann. Es muss in $T$ nicht unbedingt ein $grEl(T)$ existieren, aber es ist möglich, dass die Hinzunahme eines $c \in X \setminus T$ auf $c = grEl(T \cup \{c\})$ führt.




**Def.:** Sei $X$ mit $\leq$ geordnet und $T \subseteq X$.
Ein $c \in X$ heißt obere Schranke von $T$, falls $\forall x \in T: x \leq c$. Notation: $obSchr(T)$.
Existiert eine $obSchr(T)$, heißt $T$ nach oben beschränkt.

**Bem.:** • Es gilt: $c = obSchr(T) \Leftrightarrow c = grEl(T \cup \{c\})$.
• Existiert ein $grEl(T)$ (in $T$), so ist es auch $obSchr(T)$.

**Bsp.:** • $X = \mathbb{Q}$, $T = \{1 - \frac{1}{n} \mid n \in \mathbb{N}\}$ mit "$\leq$" hat die oberen Schranken $1, \frac{3}{2}, 2, 4, \ldots$ aber kein größtes Element. Hingegen ist $c = grEl(T \cup \{c\})$ richtig für jede $obSchr\, c$.

Für eine (nach oben) beschränkte Teilmenge ist das kleinste Element in der Menge aller oberen Schranken interessant (welches aber nicht immer ex. muss!):

**Def.:** Sei $X$ mit $\leq$ geordnet und $T \subseteq X$.
Ein $s \in X$ heißt **Supremum / obere Grenze** von $T$,
falls $s$ ein $kl\,El(\{c \mid c \text{ ist } obSchr(T)\})$ ist,
d.h. falls $s$ $obSchr(T)$ ist mit: $\forall c,\ c \text{ ist } obSchr(T): s \leq c$.

**Bem.:** • Aus der Def. folgt, dass $s$ eindeutig bestimmt ist, wenn es existiert.
[$s_1 \leq s_2 \wedge s_2 \leq s_1 \Rightarrow s_1 = s_2$, da $\leq$ antisymmetrisch ist]
Schreiben dann: $s = \sup(T)$.

• Existiert $s = \sup(T)$ und ist $s \in T$, so folgt $s = gr\,El(T)$.

• [Analog: untere Schranke, $unSchr(T)$, Infimum / untere Grenze, $\inf(T)$]

Zusammenhänge als Schaubild:

$$\max(T) \Leftarrow gr\,El(T) \Rightarrow \sup(T) \Rightarrow obSchr(T)$$
(wenn zu $T$ gehörig)

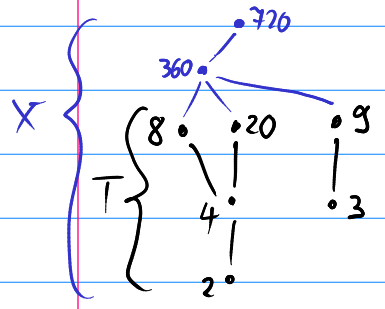
(Rückrichtungen gelten i.a. nicht)

**Bsp.:** • $X = \mathbb{Q}$, $T = \{1 - \frac{1}{n} \mid n \in \mathbb{N}\}$, dann ist $\mathcal{Y} = \{x \in \mathbb{Q};\ x \geq 1\}$ die Menge der $obSchr$ von $T$ und $\sup(T) = kl\,El(\mathcal{Y}) = 1$, sogar $1 = \min(\mathcal{Y})$, weil "$\leq$" hier eine totale Ordnung ist. (auch mit "$\geq$" richtig)

• $X = \mathbb{Q}$, $T = \{x \mid x^2 \leq 2\}$, dann ist $\mathcal{Y} = \{x \in \mathbb{Q};\ x^2 > 2\}$, und $\sup(T)$ existiert.

• $X = \mathbb{R}$, $T = \{x \mid x^2 \leq 2\}$, dann ist $\mathcal{Y} = \{x \in \mathbb{R};\ x \geq \sqrt{2}\}$, und $\sup(T) = \sqrt{2}$.
↝ $\mathbb{R}$ ist mit dem Vollständigkeitsaxiom "so gemacht", dass stets Suprema von nichtleeren, beschränkten Mengen existieren, vgl. LG6.

• $T = \{2, 3, 4, 8, 9, 20\}$, $X = T \cup \{360, 720\}$ (8·5·9), $R \subseteq X \times X$ geg. durch "$\mid$" (teilen)




$\sup(T) = 360$
8, 9, 20 sind jeweils $\max(T)$
$gr\,El(T)$ ex. nicht
2, 3 sind jeweils $\min(T)$
$kl\,El(T)$ ex. nicht
$\inf(T)$ ex. nicht
$unSchr(T)$ ex. nicht

$\mathcal{Y} := \{x \in X \mid x \text{ ist } obSchr(T)\}$
$= \{360, 720\}$
$kl\,El(\mathcal{Y}) = 360\ (= \sup(T))$

# Vorlesung "Logische Grundlagen"

## LG6: Äquivalenzrelationen

**Stichworte:** Ä-Relation, Ä-Klassen, Quotientenmengen, solche mit algebraischen Strukturen + · , Konstruktion der Zahlbereiche mit Ä-Relationen

---

## §1: Ä-Relationen und Ä-Klassen

**Def.:** Sei $X$ eine Menge. Eine Relation $R \subseteq X \times X$ in $X$ heißt eine **Äquivalenzrelation** (hier kurz: **Ä-Rel.**), wenn sie

**reflexiv** (7): $\forall x \in X : xRx$

**symmetrisch** (8): $\forall x, y \in X : xRy \Rightarrow yRx$

und **transitiv** (12): $\forall x, y, z \in X : xRy \wedge yRz \Rightarrow xRz$

ist (vgl. LG5).

Übliche Zeichen für Ä-Relationen sind $\sim$, $\simeq$, $\equiv$, $\cong$, $\approx$, etc. (die in bestimmten Kontexten aber meist auch spezielle Bedeutungen haben).
Wir wollen hier $\sim$ für eine Ä-Relation schreiben, also $x \sim y$ für $(x,y) \in R$.
↑ "Tilde"

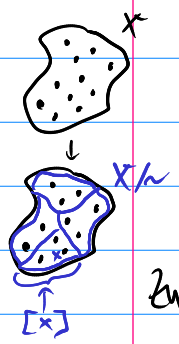
**Beispiele:** 1. "=" Gleichheit bei Mengen, Zahlen, Geraden, ...
2. "ist gleich alt wie" in der Menge der Menschen
3. "ist im gleichen Bierkasten" in der Menge der Bierflaschen
4. "ist parallel zu" in der Menge der Geraden
5. "ist kongruent zu" in der Menge der Strecken
6. "hat gleiche Parität wie" in $\mathbb{N}_0$ [$n, m$ haben dieselbe Parität, wenn sie beide gerade oder beide ungerade sind]
7. "hat dieselbe Richtung und Länge" in der Menge der Pfeile in der Ebene
8. "hat dieselbe Krümmung wie" in der Menge der Bananen

Jede Ä-Rel. $\sim$ in $X$ zerlegt $X$ in paarweise disjunkte, nichtleere Teilmengen, auch **Klasseneinteilung** genannt:

**Def.:** Die Menge aller zu $x \in X$ bzgl. $\sim$ in Relation stehenden Elemente von $X$ heißt Äquivalenzklasse und wird mit $[x]$ bezeichnet, d.h. $[x] := \{y \in X \mid y \sim x\}$

Andere Notationen: $[\![x]\!]$, $\underline{x}$, $\overline{x}$, $\langle x \rangle$, ...

**Bem.:**
- $[x]$ ist demnach die Äquivalenzklasse, die $x$ enthält: $x \in [x]$, so dass $[x] \neq \emptyset$ folgt [denn $\sim$ ist reflexiv]
- Es gilt: $\forall x,y \in X: \; x \sim y \Leftrightarrow [x] = [y]$ (obwohl hier $x \neq y$ gelten kann!)
  [$\Rightarrow$": Sei $x \sim y$. Zu "$\subseteq$": ist $z \in [x]$, folgt $z \sim x$, mit $x \sim y$ folgt aus der Transitivität $z \sim y$, also ist $z \in [y]$. Zu "$\supseteq$": analog.
  $\Leftarrow$": Sei $[x] = [y]$. Dann ist $x \in [x] = [y]$, also $x \sim y$.]
- Es gilt: $\forall x,y,z \in X: \; z \in [x] \wedge z \in [y] \Rightarrow [x] = [y]$. (Da $x \sim z \sim y$, also $x \sim y$.)




Umformuliert: $(\forall z \in X: z \in [x] \cap [y] \Rightarrow [x] = [y])$
$\Leftrightarrow \neg(\exists z \in X: z \in [x] \cap [y] \wedge [x] \neq [y])$
$\Leftrightarrow \neg([x] \cap [y] \neq \emptyset \wedge [x] \neq [y])$
$\Leftrightarrow ([x] \neq [y] \Rightarrow [x] \cap [y] = \emptyset)$

Zwei verschiedene Ä-klassen sind also disjunkt, d.h. ihr Durchschnitt ist $\emptyset$.
(Anders ausgedrückt: Jedes Element $z$ gehört zu genau einer Ä-klasse.)
- Die Vereinigung aller Ä-klassen ergibt $X$, d.h. $X = \bigcup_{x \in X} [x]$.
  [$\subseteq$": Ist $x \in X$, folgt $x \in [x]$, also $x \in$ v.S., "$\supseteq$": klar]
- Obige Überlegungen zeigen: $x \sim y \Leftrightarrow [x] = [y] \Leftrightarrow [x] \cap [y] \neq \emptyset$.

Eine Ä-Rel. erzeugt also eine neue Menge, die Menge aller Ä-klassen:

**Def.:** Sei $\sim$ eine Ä-Rel. in $X$. Dann heißt

$$X/\sim \; := \{[x] \mid x \in X\}$$

(sprich "$X$ modulo $\sim$", auch "$X$ durch $\sim$")

die Quotientenmenge von $X$ nach $\sim$.
- Ein (jedes) El. $y \in [x]$ heißt Repräsentant der Klasse $[x]$.
- Eine Menge $R \subseteq X$ heißt vollständiges Repräsentantensystem von $X/\sim$, wenn $R$ genau ein Element jeder Klasse von $X/\sim$ enthält.

**Beispiele:** in obigen Beispielen 1.–8. haben wir:

1. Ä-Kl.: Die für jedes $x$ zugehörige Ä-Klasse ist $[x] = \{x\}$.
   Also: $X/\sim = \{\{x\} \mid x \in X\}$ $\rightsquigarrow$ könnte mit $X$ identifiziert werden, denn kriegen nichts Neues! Weiter: Mer $Q = X$ ist vollst. Repr.system.
2. Alle Menschen mit gleichem Lebensjahr bilden jeweils eine Ä-Klasse.
3. Die Bierkästen sind genau die Ä-Klassen.
   [Letztlich erzeugt jede Partition $X = \dot{\bigcup}_{i \in I} X_i$ (alle $X_i \neq \emptyset$, und $\forall i \neq j: X_i \cap X_j = \emptyset$) von $X$ eine Ä-Rel. $\sim$ in $X$ durch $x \sim y :\Leftrightarrow \exists\, i \in \{1,\dots,m\}: x \in X_i \wedge y \in X_i$.]
4. Alle Geraden mit gleicher Richtung gehören zu einer Ä-Klasse. Man kann sagen, über die Parallelität / Ä-Klassenbildung kann "Richtung" erklärt werden.
5. Alle Strecken mit gleicher Länge gehören zu einer Ä-Klasse. Man kann sagen, über die Kongruenz / Ä-Klassenbildung kann "Länge" erklärt werden.
   (Alle zum "Urmeter" gleichlangen Stäbe sind 1m lang per Definition...)
6. Haben $\mathbb{N}_0/\sim = \{\mathcal{G}, \mathcal{U}\}$, wo $\mathcal{G} = \{2n \mid n \in \mathbb{N}_0\}$ die geraden und $\mathcal{U} = \{2n+1 \mid n \in \mathbb{N}_0\}$ die ungeraden Zahlen sind.
   Haben insb. $\mathbb{N}_0 = \mathcal{G} \dot{\cup} \mathcal{U}$. Bem.: Wir können mit El. von $\mathbb{N}_0/\sim$ "rechnen":
   erklären dies repräsentantenweise: $\leftarrow$ $\begin{cases} \mathcal{G}+\mathcal{G} := \mathcal{G},\ \mathcal{G}+\mathcal{U} := \mathcal{U}+\mathcal{G} := \mathcal{U},\ \mathcal{U}+\mathcal{U} := \mathcal{G} \\ \mathcal{G}\cdot\mathcal{G} := \mathcal{G},\ \mathcal{G}\cdot\mathcal{U} := \mathcal{U}\cdot\mathcal{G} := \mathcal{G},\ \mathcal{U}\cdot\mathcal{U} := \mathcal{U} \end{cases}$
   Haben ja: $\mathcal{G} = [0]$, $\mathcal{U} = [1]$,
   und $[0]+[0] := [0]$, aber auch $[4]+[6] := [10] = [0]$...
   und $[0]+[1] := [1]$, aber auch $[4]+[7] := [11] = [1]$...
   usw. Werden diese Idee später etwas vertiefen.
   (Nennen $\mathbb{N}_0/\sim$ auch $\mathbb{F}_2 \rightsquigarrow$ 2-elementiger Körper.)
7. Die Ä-Klassen sind die Vektoren, welche jeweils durch einen Pfeil repräsentiert werden, der vom Ursprung aus beginnt. Diese repräsentierenden Pfeile werden durch ihren Endpunkt an der Pfeilspitze dargestellt, den wir mit einem Tupel angeben.
8. Alle Bananen gleicher Krümmung gehören zu einer Ä-Klasse.
   Den Begriff "Krümmung" kann man mit Mitteln der Analysis präzisieren.

Gerade das Bsp. 6. zeigt neue interessante Strukturen (mit $+,\cdot$) auf, wollen es vertiefen/verallgemeinern. Dies zunächst in einem weiteren Bsp.:

9. Statt mit "gerade/ungerade" wollen wir mit den Resten "rechnen", die wir bei Division natürlicher Zahlen durch $M = 12$ erhalten:

Betr. $X = \mathbb{N}_0$ und

$n \sim m :\Leftrightarrow n$ und $m$ lassen denselben Rest bei Division durch 12

$\Leftrightarrow 12 \mid n-m \vee 12 \mid m-n$

$\Leftrightarrow \exists\, k \in \mathbb{N}_0 : n = m + 12k$ oder $m = n + 12k$

Dann ist also $[0] = [12] = [24] = \ldots = \{0, 12, 24, \ldots\}$ (alle mit Rest 0)

$[1] = [13] = [25] = \ldots = \{1, 13, 25 \ldots\}$ (alle mit Rest 1)

$\vdots$

$[11] = [23] = [47] = \ldots = \{11, 23, \ldots\}$ (alle mit Rest 11)

$\rightsquigarrow$ identifizieren die $\sim$-Klassen mit den 12 möglichen Resten $0, 1, \ldots, 10, 11$.

Haben: $\{0, 1, \ldots, 11\}$ ist vollst. Repr.system, aber auch z.B. $\{12, 1, \ldots, 9, 10, 23\}, \ldots$

Somit: $\mathbb{N}_0 / \sim \; = \{[0], [1], \ldots, [11]\} = \{[12], [1], \ldots, [10], [23]\}, \ldots$

diese Darstellung der $\sim$-Klassen gefällt uns am besten.

"Rechnen" mit Resten (d.h. mit $\sim$-Klassen, den El. von $\mathbb{N}_0/\sim$) erklären wir repräsentantenweise:

$$[k] + [l] := [k+l]$$
$$[k] \cdot [l] := [k \cdot l]$$

für $k, l \in \mathbb{N}_0$ (!). Wir haben hier die Def. von "$+$", "$\cdot$" auf $\mathbb{N}_0/\sim$ von $k, l$ abhängig gemacht, obwohl wir doch nur $[k]$, $[l]$ miteinander verknüpfen wollten; prinzipiell könnte je nach Repräsentantenwahl ein anderes Ergebnis nach der Verknüpfung herauskommen. Tut es hier aber nicht! Denn:

Es ist egal, welche Repräsentanten wir wählen für $[k]$, $[l]$,

sagen wir mal $[k] = [n]$ und $[l] = [v]$,

dann ist nämlich $[k+l] = [n+v]$.

müsste man genauer begründen...

- $k \sim n \Leftrightarrow \exists\, r \in \mathbb{N}_0 : k - n = 12r \vee n - k = 12r$, sei $\Leftrightarrow$ die 1. Alternative w,
- $l \sim v \Leftrightarrow \exists\, s \in \mathbb{N}_0 : l - v = 12s \vee v - l = 12s$, sei $\Leftrightarrow$ die 1. Alternative w.

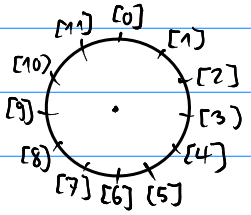
Somit: $k + l \sim n + v$, denn $k + l - (n+v) = (k-n) + (l-v) = 12(r+s)$.

Eine ähnliche Überlegung zeigt $[k \cdot l] = [n \cdot v]$.

Man sagt, aufgrund dieser Rechnung ist die gegebene Def. von $+,\cdot$ auf den $\tilde{A}$-Klassen in $\mathbb{N}_0/\sim$ repräsentantenunabhängig und deswegen wohldefiniert.

auch: "mod 12"

In diesem Beispiel sprechen wir vom Rechnen/der Arithmetik modulo 12.
(Die Zahl $M=12$ könnte auch durch einen anderen Modul $M$ ersetzt werden.)
Anschaulich ist die Arithmetik mod 12 das Rechnen mit Stunden auf einer Uhr:




$[7]+[6]=[8]$

$[9]+[4]=[13]=[1]$

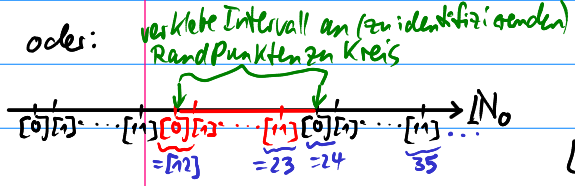
$[11]+[11]=[22]=[10]$, ...

$[13]+(-[5])=[8]$, ... usw.

↳ erkläre $-[5]$ als die Klasse mit $(-[5])+[5]=0$, d.h. $-[5]=[7]$

$[13]+[7]=[20]=[8]$ ...

oder:




Diese Verknüpfungen $+,\cdot$ auf $\mathbb{N}_0/\sim$ haben viele neue interessante Eigenschaften.

## §2: Konstruktion der Zahlbereiche

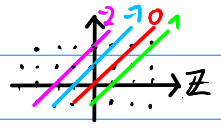
$\tilde{A}$-Relationen werden sehr vielfältig eingesetzt, um neue mathematische Strukturen zu definieren (z.B. Quotientenvektorräume, Quotientenkörper, Randverklebungen...).
Eine Hauptanwendung ist die Konstruktion der Zahlbereiche
$\mathbb{N}_0 \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$, die wir hier angeben (natürlich gibt es viele andere Möglichkeiten, dies zu tun):

(1.) $\mathbb{Z} := \mathbb{N}_0 \times \mathbb{N}_0/\sim$ mit der $\tilde{A}$-Relation

$$(n,m)\sim(\mu,\nu) :\Leftrightarrow n+\nu = m+\mu.$$

("$n-m$ = Konstante"...)

Darin ist $\mathbb{N}_0$ eingebettet in der Form $\{[(n,0)] \mid n\in\mathbb{N}_0\}$.
Weiter: $[(n,m)]+[(\mu,\nu)] := [(n+\mu, m+\nu)]$.
Die Zahl $-n$ für $n\in\mathbb{N}_0$ liegt vor als $[(0,n)]$,
denn $[(n,0)]+[(0,n)] = [(n,n)] = [(0,0)]$.




beide Konstruktion spielt nur der 1. Quadrant $\mathbb{N}_0\times\mathbb{N}_0$ eine Rolle!

(Ü) Wie geht die Definition von "$\cdot$" und "$\leq$"? (nicht naheliegend!)
Welche Eigenschaften haben $+,\cdot$ und $\leq$?

(2.) $\mathbb{Q} := \mathbb{Z} \times \underbrace{\mathbb{N}}_{\text{ohne } 0} / \sim$ mit der Äquivalenz-Relation

$(z,n) \sim (y,m) :\Leftrightarrow zm = ny$

Darin ist $\mathbb{Z}$ eingebettet in der Form $\{[(z,1)] \mid z \in \mathbb{Z}\}$.
Wir schreiben dann $\frac{z}{n}$ für $[(z,n)]$ und erhalten die üblichen Rechengesetze für $+, \cdot$, wenn wir erklären:

$\frac{z}{n} \cdot \frac{y}{m} := \frac{zy}{nm}$, $\quad \frac{z}{n} + \frac{y}{m} := \frac{zm+yn}{nm}$.

Def. $\leq$: $\frac{z}{n} \leq \frac{y}{m} :\Leftrightarrow zm \leq yn$.

(3.) $\mathbb{R} := \mathcal{C} / \sim$ mit der Menge

$\mathcal{C} := \{(a_n)_{n\in\mathbb{N}} \subseteq \mathbb{Q} \mid (a_n) \text{ ist Cauchyfolge in } \mathbb{Q}\}$

($\forall \varepsilon > 0 \; \exists N_\varepsilon \; \forall n,m \geq N_\varepsilon : |a_n - a_m| < \varepsilon$)

und der Äquivalenz-Relation $(a_n)_{n\in\mathbb{N}} \sim (b_n)_{n\in\mathbb{N}} :\Leftrightarrow (a_n - b_n)_{n\in\mathbb{N}}$ ist Nullfolge.
($\Leftrightarrow \forall \varepsilon > 0 \; \exists N_\varepsilon \; \forall n \geq N_\varepsilon : |a_n - b_n| < \varepsilon$)

**Satz:** Der Körper der reellen Zahlen ist "der" (bis auf Isomorphie) eindeutig bestimmte vollständige angeordnete Körper.

**Def.:** • Ein Körper $K$ (mit Verknüpfungen $+, \cdot$) und einer strikten Anordnung "$<$" (oder Anordnung) (die trichotomisch (13) und transitiv (12) ist) heißt **angeordneter Körper**, falls $\forall x,y,z \in K: x < y \Rightarrow x + z < y + z$ (Monotonie der Addition) und $\forall x,y,z \in K: x < y, z > 0 \Rightarrow xz < yz$ (Monotonie der Multiplikation) gilt.

• Ein angeordneter Körper heißt **archimedisch angeordnet**, falls

$\forall x \in K \; \forall y \in K, y > 0 \; \exists n \in \mathbb{N} : ny > x$.

(Dies ist genau dann der Fall, wenn die "natürlichen Zahlen in $K$" nicht beschränkt sind.)

**Satz:** Für angeordnete Körper $K$ sind äquivalent: (D.h.: (1) $\Leftrightarrow$ (2) $\Leftarrow$ (3) $\Leftrightarrow$ (4).)

(1) Jede nichtleere, nach oben beschr. Teilmenge von $K$ besitzt ein Supremum in $K$.

(2) Jede monoton wachsende, nach oben beschr. Folge aus $K$ konvergiert in $K$.

(3) $K$ ist archimedisch und jede Cauchyfolge aus $K$ konvergiert in $K$.

(4) $K$ ist archimedisch und im Durchschnitt jeder IV-Schachtelung liegt genau ein El. von $K$.
„Eine Intervallschachtelung ist eine Folge abgeschlossener, ineinander verschachtelter Intervalle, deren Länge gegen Null geht."

dies erfüllt $\mathbb{R}$ laut obiger Konstruktion (und damit auch (1), (2) und (4).)

**Def.:** Ein angeordneter Körper $K$ heißt **vollständig**, falls (1) „$\Leftrightarrow$ (2) $\Leftarrow$ (3) $\Leftrightarrow$ (4)" gilt.

**Bem.:** Wegen obigem Satz, dass $\mathbb{R}$ als vollständiger angeordneter Körper im wesentlichen eindeutig bestimmt ist, kann man auch mit der Charakterisierung von $\mathbb{R}$, d.h. den Körperaxiomen plus dem "Vollständigkeitsaxiom", meist in der Form (1), beginnen und damit Analysis betreiben, ohne je eine Konstruktion von $\mathbb{R}$ zu benutzen. Denn die explizit konstruierten Elemente von $\mathbb{R}$ – entweder $\sim$-Klassen von Cauchyfolgen, unendlich lange Dezimalbrüche, ... sind zu kompliziert zum damit Rechnen/Aufschreiben.

(4.) $\mathbb{C} := \mathbb{R}^2$ mit $(x,u)+(y,v) := (xy+uv)$

$(x,u)\cdot(y,v) := (xy-uv, xv+uy)$

ist die einfachste Konstruktion von $\mathbb{C}$. Es gibt viele andere, eine andere ist diese:

$\mathbb{C} := \mathbb{R}[X]/\sim$ mit den reellen Polynomen $\mathbb{R}[X] := \{\sum_{i=0}^{m} a_i X^i \mid m\in\mathbb{N}_0, a_i\in\mathbb{R}\}$

und der $\sim$-Relation $f(X)\sim g(X) :\Leftrightarrow \exists\, h(X)\in\mathbb{R}[X]$:

$$f(X)-g(X) = h(X)\cdot(X^2+1).$$

$\rightsquigarrow$ die $\sim$-Klassen sind El. von $\mathbb{C}$ und wir erklären $+,\cdot$ durch

$$\circledast\quad \begin{cases} [f(X)]+[g(X)] := [f(X)+g(X)] \\ [f(X)]\cdot[g(X)] := [f(X)\cdot g(X)] \end{cases}$$

← deutlich natürlichere Def.!

Jede Klasse $[f(X)]$ enthält genau ein Polynom der Form $a_0+a_1X$ ist also durch ein Zahlenpaar $(a_0,a_1)$ eindeutig bestimmt, die wieder auf Real- und Imaginärteil führen.

Beachten Sie:

$[X^2+1] = [0]$, und weiter ist

$$[X]\cdot[X] = [X^2] = [X^2+1-1] = [X^2+1]+[-1] = [-1],$$

d.h. $[X]$ ist eine Zahl mit $[X]^2 = [-1]$,

die würden wir ja wohl "$i$" nennen...

**Bem. zum Schluss:** Oft vererben sich Eigenschaften von "$+$", "$\cdot$" auf Quotientenmengen, wenn diese wie in $\circledast$ erklärt werden, wie z.B. Assoziativität etc., aber nicht immer. Deswegen sind Beweise erforderlich.

# Vorlesung "Logische Grundlagen"

## LG7: Abbildungen / Funktionen

**Stichworte:** Def. Abbildung als Relation, Bild einer Teilmenge, Urbild einer Teilmenge, Abbildungstypen: surjektiv/injektiv/bijektiv, Komposition und (Rechts-/Links-) inverse Abb., $\mathrm{Sym}(X)$, besondere Abb.: charakteristische Abb., Folgen, Abbildungen bei Quotientenmengen

---

## §1: Abbildungen

Bisher hatten wir nur zweistellige Relationen $R \subseteq X \times X$ mit einer Menge $X$ näher untersucht, wenn Vergleiche zweier Elemente von $X$ interessant sind. Wir möchten nun auch Relationen $R \subseteq X \times Y$ mit zwei unterschiedlichen Mengen untersuchen, also Elemente von $X$ mit denen von $Y$ "vergleichen", z.B. $R \subseteq \mathbb{N} \times \mathbb{R}$, $R \subseteq \{\text{Geraden}\} \times \{\text{Vektoren}\}$, $R \subseteq \{\text{Äpfel}\} \times \{\text{Birnen}\}$, ... Wenn die beiden Mengen sehr unterschiedlich sind, würde man eher nicht mehr von "Vergleich", sondern von "Zuordnung" sprechen, so dass man auf diesem Wege zum Begriff der Abbildung kommt. Relationen stellen i.a. keine eindeutigen Beziehungen zwischen Mengen her, d.h. einem Element in $X$ können durchaus mehrere Elemente aus $Y$ zugeordnet sein. Von einer Abbildung wird verlangt, dass sie die ganze Menge $X$ eindeutig in die andere Menge $Y$ abbilden: Jedem $x \in X$ wird genau ein $y \in Y$ zugeordnet.

**Def.:** Eine linkstotale (1), rechtseindeutige (5) Relation $f \subseteq X \times Y$ heißt **Abbildung** (auch: **Funktion**, Kurz: Abb. / Fkt.).

[vgl. LG5: $f$ linkstotal $:\Leftrightarrow \forall x \in X\ \exists y \in Y : x f y$

$f$ rechtseindeutig $:\Leftrightarrow \forall x \in X\ \forall y \in Y\ \forall v \in Y : x f y \wedge x f v \Rightarrow y = v$]

beides: $\exists!\, y \in Y : x f y$

**Notation:** Statt $x f y$ bzw. $(x,y) \in f$ schreibt man auch $x \mapsto y$ oder $x \mapsto f(x)$ mit $f(x) = y$. Statt $f \subseteq X \times Y$ wird $f : X \to Y$ oder $X \xrightarrow{f} Y$ geschrieben.

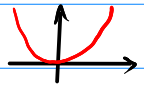
**Bem.:** Eine Abbildung ist – als Menge – dasselbe wie ihr Graph/Schaubild. Diese Def. mit Mengen muss man sich nicht merken, vielmehr ist ihre Eigenschaft wichtig, dass jedem $x \in X$ ein zugehöriges $y \in Y$ eindeutig zugeordnet wird. Die Bezeichnung $f(x)$ macht die Abhängigkeit des Elements $y = f(x)$ von $x$ deutlich.

**Def.:** In einer Abb. $f: X \to Y$ heißt die Menge $X$ der Definitionsbereich bzw. Definitionsmenge und die Menge $Y$ der Zielbereich / Wertebereich / Bildbereich bzw. Zielmenge / Wertemenge / Bildmenge [Letzteres wegen Verwechslungsgefahr nicht so gerne, zu "Bild" / "Bildmenge" s.u.]. Die Menge $f = \{(x, f(x)) \mid x \in X\} \subseteq X \times Y$ heißt Graph von $f$. ("Schaubild")

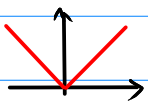
**Bem.:** • Eine Abb. wird durch 3 Angaben festgelegt: Def.bereich/Zielbereich/Abb.vorschrift. Zwei Abbildungen $f, g: X \to Y$ heißen gleich, falls $\forall x \in X: f(x) = g(x)$.

• Eine Abb. $g: U \to Y$ heißt Einschränkung von $f: X \to Y$, falls $U \subseteq X$ und $g(u) = f(u)$ für alle $u \in U$. Notation: $g = f|_U$. $g: V \to Y$ heißt Fortsetzung von $f: X \to Y$, falls $X \subseteq V$ und $f = g|_X$.

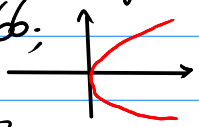
**Bsp.:** 1. $f: \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ Standardparabel



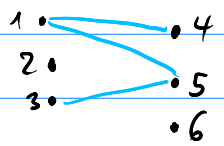
2. $f: \mathbb{R} \to \mathbb{R}$, $x \mapsto |x| = \begin{cases} x, & \text{falls } x \geq 0, \\ -x, & \text{falls } x < 0. \end{cases}$ Absolutbetrag



3. $R \subseteq \mathbb{R} \times \mathbb{R}$, $R = \{(x^2, x) \mid x \in \mathbb{R}\}$ ist keine Abb.; nur eine rechtseindeutige, linkstotale Relation

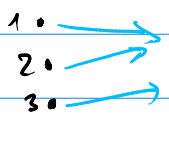


4. $R \subseteq \{1,2,3\} \times \{4,5,6\}$, $f: \{1,2,3\} \to \{4,5,6\}$




1R4
1R5
3R5

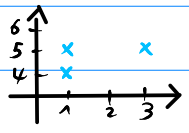
R ist Relation, keine Fkt.



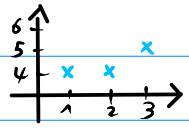

$f(1) = 4 = f(2)$, $f(3) = 5$

von jedem El. des Def.bereichs geht genau ein Pfeil aus ⇝ f ist Abb.

Graph/Schaubild: R:




f:




**Def.:** Wenn $y = f(x)$ gilt, so heißt $y$ das Bild von $x$ und $x$ das Urbild von $y$.

**Bem.:** Jedes $x$ hat genau ein Bild, nämlich $f(x)$. Aber ein $y \in Y$ kann kein, ein oder mehrere Urbilder haben. Das Konzept "Bild"/"Urbild" lässt sich wie folgt auf Teilmengen von $X$ bzw. $Y$ übertragen:

**Def.:** Ist $A \subseteq X$, so heißt $f(A) := \{f(a) \mid a \in A\} \subseteq Y$ das **Bild von $A$**.
Ist $B \subseteq Y$, so heißt $f^{-1}(B) := \{x \in X \mid f(x) = b\} \subseteq X$ das **Urbild von $B$**.

**Bem./Zusatz:**
- $f^{-1}(B)$ ist ein reines Symbol, mit $f^{-1}$ ist keine Abb. gemeint.
- Ist $A = X$, so heißt $f(X)$ das Bild von $X$ unter $f$ bzw. Bild von $f$.
- Ist $B = Y$, so heißt $f^{-1}(Y)$ das Urbild von $X$ unter $f$ bzw. Urbild von $f$.
- Für $x \in X$ ist $f(\{x\}) = \{f(x)\}$ einelementig, für $y \in Y$ kann $f^{-1}(\{y\})$ aber aus keinem, einem oder mehreren Elementen bestehen.
  Man schreibt einfache auch $f^{-1}(y)$ für $f^{-1}(\{y\})$.

**Bsp.:** Für $f: \mathbb{R}^2 \to \mathbb{R}$, $f(u,v) = u+v$ ist $f^{-1}(z) = \{(u,v) \mid u+v = z\} = \{(u, z-u) \mid u \in \mathbb{R}\}$

eigentlich: $f((u,v))$, lassen überflüssige Klammern weg wenn Kontext klar...

$\rightsquigarrow$ Alle Punkte einer Geraden $g: y = -x + z$ werden von $f$ auf den $y$-Achsenabschnitt $z$ abgebildet.

## §2: Abbildungstypen

**Def.:** Eine Abb. $f: X \to Y$ heißt

- **injektiv**, falls es zu jedem $y \in Y$ **höchstens** ein $x$ gibt mit $f(x) = y$
  $\lceil \forall y \in Y \quad \forall x_1, x_2 \in X: f(x_1) = y = f(x_2) \Rightarrow x_1 = x_2$
  bzw. $\forall y \in Y: f^{-1}(y)$ ist höchstens einelementig $\rfloor$
- **surjektiv**, falls es zu jedem $y \in Y$ **mindestens** ein $x$ gibt mit $f(x) = y$
  $\lceil \forall y \in Y \; \exists x \in X: f(x) = y$
  bzw. $\forall y \in Y: f^{-1}(y)$ ist mindestens einelementig $\rfloor$
- **bijektiv**, falls es zu jedem $y \in Y$ **genau** ein $x$ gibt mit $f(x) = y$
  $\lceil \forall y \in Y \; \exists! \, x \in X: f(x) = y$
  bzw. $\forall y \in Y: f^{-1}(y)$ ist einelementig $\rfloor$

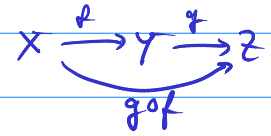
Somit: bijektiv $\Leftrightarrow$ injektiv $\wedge$ surjektiv

**Bsp.:**

| Bestr. Abb.: | $f: \mathbb{R} \to \mathbb{R}$ | $f(x) = x^2$ |
|---|---|---|
| injektiv, nicht surj.: | $f(x) = e^x$ | $f: \mathbb{R}_{\geq 0} \to \mathbb{R}$ |
| surjektiv, nicht inj.: | $f(x) = x^3 - x$ | $f: \mathbb{R} \to \mathbb{R}_{\geq 0}$ |
| nicht inj., nicht surj.: | $f(x) = x^2$ | $f: \mathbb{R} \to \mathbb{R}$ |
| bijektiv: | $f(x) = x^3$ | $f: \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ |

## §3: Komposition und Inverse von Abbildungen

**Def.:** Seien $f: X \to Y$ und $g: Y \to Z$ Abbildungen.
Dann heißt $g \circ f: X \to Z$, $g \circ f(x) := g(f(x))$ die
Komposition / Hintereinanderausführung von $f$ und $g$.
Lies: "$g$ nach $f$" für $g \circ f$, man beachte die Reihenfolge!
("$g$ nach $f$" heißt: erst $f$, dann $g$ anwenden...)




**Def.:** Auf jeder Menge $X$ ($\neq \emptyset$) kann die Identität (sa Abb.) / identische Abb.
definiert werden durch $id_X: X \to X$, $x \mapsto x$.

**Bem.:**
- Für jede Abb. $f: X \to Y$ gilt $id_Y \circ f = f$ und $f \circ id_X = f$.
  → "neutrale" Abbildungen $id_X$, $id_Y$ bzgl. $\circ$
- Klar gilt i.a. $f \circ g \neq g \circ f$, auch wenn $f, g: X \to X$, z.B. $f, g: \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, $g(x) = x+1$
  $\rightsquigarrow f(g(1)) = f(2) = 4 \neq 2 = g(1) = g(f(1))$.

**Def.:** Seien $f: X \to Y$ und $g: Y \to X$ Abbildungen zwischen Mengen $X$ und $Y$.
Dann heißt $g$ eine
- Rechtsinverse von $f$, falls $f \circ g = id_Y$
- Linksinverse von $f$, falls $g \circ f = id_X$
- Inverse von $f$, falls $g \circ f = id_X$ und $f \circ g = id_Y$, d.h.
  falls $g$ sowohl Links- als auch Rechtsinverse von $f$ ist.
  (Gelegentlich auch Umkehrabb. von $f$ genannt.)

Wir zeigen, dass diese Begriffe eng mit obigen Abbildungstypen zusammenhängen.

**Lemma A:** Sei $f: X \to Y$ eine Abb. Dann sind äquivalent: (i) $f$ ist injektiv
「Merkregel: **in**jektiv ⟺ **Lin**ksinverse」 (ii) $f$ hat eine Linksinverse

**Beweis:** Zu (i)⇒(ii): Wähle $z \in X$ bel. Wir def. $g: Y \to X$ durch

$$g(y) := \begin{cases} x, & \text{falls } f(x) = y \text{ gilt,} \\ z, & \text{falls es kein } x \text{ mit } f(x) = y \text{ gibt.} \end{cases}$$

Da es zu jedem $y \in Y$ nach Annahme "injektiv" höchstens ein $x \in X$ mit $f(x) = y$ gibt,
können wir $g$ so definieren. Für ein bel. $x \in X$ gilt dann $g(f(x)) = x$, also $g \circ f = id_X$.

Zu (ii)⇒(i): Sei $g$ eine Linksinverse. Angenommen, $u, v \in X$ mit $u \neq v$. Dann gilt
$g(f(u)) = u \neq v = g(f(v))$, also folgt $f(u) \neq f(v)$. Dies zeigt, dass $f$ injektiv. □

Analog gilt (muss aber anders bewiesen werden):

**Lemma B**: Sei $f: X \to Y$ eine Abb. Dann sind äquivalent: (i) $f$ ist surjektiv
「Merkregel: surjektiv $\Leftrightarrow$ rechtsinverse」 (ii) $f$ hat eine Rechtsinverse

**Beweis**: Zu (i)$\Rightarrow$(ii): Sei $f$ surjektiv, zu jedem $y \in Y$ gibt es dann mind. ein $x \in X$ mit $f(x)=y$. Wir wählen zu jedem $y$ ein solches $x$ aus und setzen $g(y)=x$. Dann gilt nach Konstruktion $f(g(y)) = f(x) = y$, also ist $g$ Rechtsinverse.
Zu (ii)$\Rightarrow$(i): Sei $g$ eine Rechtsinverse. Für jedes $y \in Y$ gilt dann $f(g(y)) = f \circ g(y) = y$, also hat $g(y)$ als Bild (unter $f$) genau das Element $y$, d.h. $y$ hat mind. ein Urbild. □

**Bem.**: Lemma B ist tiefer, als es aussieht: Zum Beweis von (i)$\Rightarrow$(ii) haben wir zu jedem $y \in Y$ ein Urbild "ausgewählt". Dass man das tun kann, ist nicht selbstverständlich, aber ein wichtiges Prinzip der Mengenlehre, nämlich das sogenannte "Auswahlaxiom" (tatsächlich ist Lemma B dann äquivalent; später mehr dazu).

Wir fassen Lemma A und B zusammen:

**Lemma C**: Sei $f: X \to Y$ eine Abb. Wenn $f$ eine Linksinverse $g: Y \to X$ und eine Rechtsinverse $h: Y \to X$ hat, dann ist $g=h$ und $f$ ist bijektiv.

**Beweis**: Nach Voraussetzung gilt $f \circ h = id_Y$ und $g \circ f = id_X$, also folgt
$g(y) = g(f \circ h(y)) = g(f(h(y))) = g \circ f(h(y)) = h(y)$ für alle $y \in Y$. Also ist $g=h$. □

**Korollar**: Eine bijektive Abb. $f: X \to Y$ hat genau eine Inverse.

**Beweis**: Seien $g$ und $h$ Inverse von $f$. Dann ist insb. $g$ Rechtsinverse von $f$ und $h$ Linksinverse von $f$, nach Lemma C folgt $g=h$. □

**Bsp.**:
- $\exp: \mathbb{R} \to \mathbb{R}_{>0}$ ist bij., die Inverse heißt $\log: \mathbb{R}_{>0} \to \mathbb{R}$ (Logarithmus), es gilt $\exp(\log(x)) = x$ bzw. $\log(\exp(y)) = y$ für alle $x, y \in \mathbb{R}$, $x > 0$.
- $q: \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $x \mapsto x^2$ ist bij., die Inverse heißt $\sqrt{}: \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ (Wurzel), d.h. $\sqrt{y}$ ist eine Zahl $\geq 0$ mit $(\sqrt{y})^2 = q \circ \sqrt{}(y) = y = \sqrt{} \circ q(y) = \sqrt{y^2}$, sofern $y \geq 0$ ist.
- $\tilde{q}: \mathbb{R} \to \mathbb{R}_{\geq 0}$, $x \mapsto x^2$ ist surj., die Rechtsinverse ist $\tilde{\sqrt{}}: \mathbb{R}_{\geq 0} \to \mathbb{R}$, es gilt $\tilde{q} \circ \tilde{\sqrt{}}(y) = (\sqrt{y})^2 = y$.
- $p_n: \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $x \mapsto x^n$ ist bij., die Inverse ist (per Def.) die n-te Wurzel $= \sqrt[n]{}$.

identifizieren mit $\sqrt{}$, wollen mal nicht so pingelig sein

Die bijektiven Abbildungen einer Menge auf sich haben mit "$\circ$" eine besondere Struktur:

**Def.:** Sei $X$ eine nichtleere Menge. Eine bijektive Abb. $f: X \to X$ heißt auch Permutation von $X$. Die Menge aller Permutation bezeichnet man als $\mathrm{Sym}(X)$, d.h.

$$\mathrm{Sym}(X) := \{ f : X \to X \mid f \text{ ist bijektiv} \}.$$

**Bem.:**
- Sind $f, g \in \mathrm{Sym}(X)$, so ist auch $f \circ g \in \mathrm{Sym}(X)$ (und ebenso $g \circ f \in \mathrm{Sym}(X)$), da die Komposition bijektiver Abb.en wieder bijektiv ist.
- Weiter ist $\mathrm{id}_X \in \mathrm{Sym}(X)$ und haben $f \circ \mathrm{id}_X = f = \mathrm{id}_X \circ f$ für jedes $f \in \mathrm{Sym}(X)$.
- Zu jedem $f \in \mathrm{Sym}(X)$ gibt es eine inverse Abb., d.h. ein $g \in \mathrm{Sym}(X)$ mit $f \circ g = \mathrm{id}_X = g \circ f$ (s. Korollar für $\mathrm{Sym}(X)$).

$\rightsquigarrow$ **Fazit:** $\mathrm{Sym}(X)$ erfüllt mit $\circ$ die Axiome einer Gruppe $(G, \circ)$, d.h.

(i) Assoziativität: $\forall f, g, h \in G: (f \circ g) \circ h = f \circ (g \circ h)$ ← bei $\mathrm{Sym}(X)$ etwas mühsam zu zeigen, aber nicht schwer

(ii) Ex. eines neutr. El.: $\exists e \in G \; \forall f \in G: e \circ f = f = f \circ e$

(iii) Ex. von inversen El.: $\forall f \in G \; \exists g \in G: g \circ f = e = f \circ g$

**Bem.:**
- Da $(\mathrm{Sym}(X), \circ)$ eine Gruppe ist, heißt $\mathrm{Sym}(X)$ auch symmetrische Gruppe von $X$. Im Gegensatz zu den üblichen Zahlenbereich-Gruppen $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, gibt $\mathrm{Sym}(X)$ das wichtigste Bsp. für eine nicht kommutative / nichtabelsche Gruppe.

  (Eine Gruppe $(G, \circ)$ heißt abelsch / kommutativ, falls $\forall f, g \in G: f \circ g = g \circ f$.)
- Haben hier für eine allgemeine Verknüpfung $\circ: G \times G \to G$ auch "$\circ$" geschrieben, man könnte auch $*$ oder andere Symbole schreiben ($+, \cdot, \times, \ldots$), die in anderen Zusammenhängen aber meist eine spezifischere Bedeutung haben.
- Wir nennen eine bel. Abb. $*: X \times X \to X$ für eine nichtleere Menge $X$ eine Verknüpfung.
- Es ist üblich, eine Gruppe als ein Paar $(G, \circ)$ zu schreiben, d.h. durch Angabe der Menge $G$ und der Verknüpfung $\circ$. Manchmal schreibt man auch $(G, \circ, e)$, wenn das neutrale Element $e$ genannt werden soll (es ist übrigens eindeutig bestimmt).
- Mit $g^2$ ist $g \circ g$ gemeint. Def. rekursiv: $g^{n+1} := g^n \circ g$, $g^0 := e$ für $n \in \mathbb{N}_0$.

**Bsp.:** Betr. $X = \{1, 2, 3\}$, neben $\mathrm{id}_X$ gibt es die Abb. $T_1 : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases}$, $T_2 : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 1 \end{cases}$, $T_3 : \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \end{cases}$

und $D_1 : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases}$ und $D_2 : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{cases}$ es ist $\mathrm{Sym}(X) = \{\mathrm{id}_X, T_1, T_2, T_3, D_1, D_2\}$.

Haben: $D_1 \circ D_2 = \mathrm{id}_X = D_2 \circ D_1$, $T_1^2 = T_2^2 = T_3^2 = \mathrm{id}_X$, weiter $T_1 \circ D_1 = T_3$ usw.

# §4: Besondere Abbildungen

## 4.1. Charakteristische Abbildungen

**Def.:** Ist $X$ eine Menge und $A \subseteq X$, so def. wir eine zugehörige Abb. durch

$$\chi_A : X \to \{0,1\}, \quad \chi_A(x) = \begin{cases} 1, & \text{falls } x \in A, \\ 0, & \text{falls } x \notin A. \end{cases}$$

Man nennt $\chi_A$ die charakteristische Funktion von $A$. Klar: $\chi_A = \chi_B \Leftrightarrow A = B$.

**Bem.:** Ist umgekehrt eine Abb. $f: X \to \{0,1\}$ geg., so ist $f = \chi_A$ mit $A := \{x \in X \mid f(x) = 1\}$, d.h. jede 0-1-Abb. ist eine charakterische Fkt.

## 4.2. Folgen

**Def.:** • Eine Abb. $x: \mathbb{N} \to X$ in eine Menge $X$ heißt Folge und wird als $(x_n)_{n \in \mathbb{N}}$ geschrieben, d.h. schreiben $x_n$ für $x(n)$.

• $\mathbb{N}$ heißt Indexmenge der Folge.

**Bem.:** • Für $X = \mathbb{R}$ hat man die in der Analysis gebräuchlichen reellen Zahlenfolgen, mit deren Hilfe man die Approximation an andere reelle Zahlen untersucht ("Konvergenz").

• Natürlich können auch Folgen von Folgen etc. untersucht werden.

• Für Teilmengen $A \subseteq \mathbb{N}_0$ kann die zugehörige charakteristische Fkt. als zugehörige 0-1-Folge (d.h. Abb. $\mathbb{N}_0 \to \{0,1\}$) aufgefasst werden und umgekehrt.

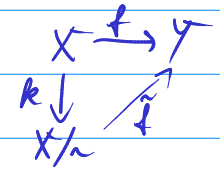
## 4.3. Abbildungen bei Quotientenmengen

Sei $X$ eine nichtleere Menge und $\sim$ eine Äquivalenz-Relation. Die Quotientenmenge ist $X/\sim = \{[x] \mid x \in X\}$, die Menge der Äquivalenzklassen $[x] = \{y \in X \mid y \sim x\}$.

Es gibt immer eine "natürliche" Abb. $k: X \to X/\sim$

$x \mapsto [x]$, die jedem $x$ ihre Klasse $[x]$ zuordnet, oft auch Kanonische Abb. genannt (sie ist übrigens surjektiv).

Ist eine Abb. $f: X \to Y$ derart, dass sie konstant auf den Klassen $[x]$ ist, d.h. $\forall x \in X \; \forall y,z \in [x]: f(y) = f(z)$, dann gibt es eine Abb. $\tilde{f}: X/\sim \to Y$, die sich auf den $[x]$ wie $f$ verhält ("von $f$ induziert wird"), d.h. für die $f = \tilde{f} \circ k$ gilt: Es ist einfach $\tilde{f}([x]) := f(x)$ erklärt. Diese Def. ist wohldefiniert (d.h. auch hier repräsentantenunabh.) nach Vor.




ein solches Skalbild heißt "kommutatives Diagramm"

falls $f = \tilde{f} \circ k$

**Bsp.:** $X = \mathbb{Z}$, $m \sim n :\Leftrightarrow 3 \mid m-n$, $\mathbb{Z}/\sim = \{[0],[1],[2]\}$. Die Abb. $f: \mathbb{Z} \to \mathbb{C}$, $f(n) := e^{\frac{2\pi i n}{3}}$ induziert $\tilde{f}: \mathbb{Z}/\sim \to \mathbb{R}$, $\tilde{f}([0]) = 1$, $\tilde{f}([1]) = e^{\frac{2\pi i}{3}}$, $\tilde{f}([2]) = e^{\frac{4\pi i}{3}}$.

# Vorlesung "Logische Grundlagen"

## LG8: Endliche Mengen

**Stichworte:** endliche Menge, Kardinalität $\#X = n$, Ergebnisse über endliche Mengen, Kombinatorik, Permutationen, $\binom{n}{k}$, Binomialsatz, Multinomialsatz, Potenzreihen als kombinatorisches Hilfsmittel

---

### §1: Endliche Mengen und ihre Kardinalität

**Def.:** • Eine Menge $X$ heißt **endlich**, wenn es eine nat. Zahl $n \in \mathbb{N}_0$ und eine bijektive Abbildung $f: \{1, 2, \dots, n\} \to X$ gibt. Dann gilt $X = \{f(1), f(2), \dots, f(n)\}$ und $f(i) \neq f(j)$ für $i \neq j$.

• Die Zahl $n$ heißt dann **Kardinalität / Mächtigkeit / Länge** von $X$.
Notation: $\#X = n$ (oder $|X| = n$ oder $\mathrm{card}(X) = n$)

**Bem.:** • Es gilt: $\#X = 0 \iff X = \emptyset$.

• Eine Menge $X$ heißt **unendlich**, wenn sie nicht endlich ist, vgl. LG9.

Man kann den Kardinalitätsbegriff verallgemeinern zu beliebigen Mengen:

**Def.:** Zwei Mengen $X, Y$ haben dieselbe **Mächtigkeit / Kardinalität**, wenn es eine bijektive Abbildung $f: X \to Y$ gibt.

Wir zeigen einige Ergebnisse über endliche Mengen (die für unendliche Mengen i.a. falsch sind):

**Lemma A:** Es seien $X$ und $Y$ endliche Mengen und $f: X \to Y$ eine surjektive Abb. Wenn $\#X \leq \#Y$ gilt, dann ist $f$ bijektiv und es gilt $\#X = \#Y$.

**Bew.:** Setze $m = \#X$ und $n = \#Y$, $X = \{x_1, \dots, x_m\}$. Dann nimmt $f$ höchstens $m$ verschiedene Werte an, nämlich $f(x_1), \dots, f(x_m)$. Nach Vor. gilt $Y = \{f(x_1), \dots, f(x_m)\}$, also ist $m \geq n$. Wegen der Vor. $m \leq n$ folgt $m = n$. Würde $f$ einen Wert mehrfach annehmen, wäre $m > n$, im $\lightning$ zu $m = n$. Also ist $f$ injektiv und damit bijektiv. $\square$

**Lemma B:** Es seien $X$ und $Y$ endliche Mengen und $f: X \to Y$ eine injektive Abb. Wenn $\#X \geq \#Y$ gilt, dann ist $f$ bijektiv und es gilt $\#X = \#Y$.

**Bew.:** Setze $m = \#X$ und $n = \#Y$, $X = \{x_1, \dots, x_m\}$. Da $f$ injektiv ist, hat $\{f(x_1), \dots, f(x_m)\}$ genau $m$ Elemente. Sie liegt in $Y$, also ist $m \leq n$. Wegen der Vor. $m \geq n$ folgt $m = n$ und $Y = \{f(x_1), \dots, f(x_m)\}$, d.h. $f$ ist surjektiv. □

**Korollar:** Es seien $X$ und $Y$ endliche Mengen mit $\#X = \#Y$ und sei $f: X \to Y$ eine Abb. Dann sind äquivalent: (i) $f$ ist bijektiv
(ii) $f$ ist injektiv
(iii) $f$ ist surjektiv.

**Bem.:** Ein Bsp., warum dies für unendliche Mengen i.a. falsch ist:

- Sei $f: \mathbb{N}_0 \to \mathbb{N}_0$, $f(x) = \begin{cases} 0, & x = 0 \\ x-1, & x \geq 1 \end{cases}$ $\rightsquigarrow$ $f$ ist surjektiv, aber nicht injektiv, da $f(0) = 0 = f(1)$.
- Sei $g: \mathbb{N}_0 \to \mathbb{N}_0$, $g(x) = 2x$ $\rightsquigarrow$ $g$ ist injektiv, aber nicht surjektiv, da $\neg \exists x \in \mathbb{N}_0 : g(x) = 1$.

Wir beschäftigen uns jetzt in LG 8 noch mit der Möglichkeit, Elemente endlicher Mengen in Reihenfolgen zu bringen, z.B. die Reihenfolge von Zahlen in einem $n$-Tupel. Mit solchen Fragestellungen beschäftigt sich die Kombinatorik, die vielfältige Anwendungen hat, speziell auch in der Spieltheorie / Statistik / Wahrscheinlichkeitstheorie bzw. "Unterhaltungsmathematik". Sie ist auch eng verbunden mit der Graphentheorie und Zahlentheorie.

## §2: Permutationen endlicher Mengen

**Def.:** Für $n \in \mathbb{N}$ ist $S_n := \mathrm{Sym}(\{1, 2, \dots, n\}) = \{\sigma : \{1, \dots, n\} \to \{1, \dots, n\} \mid \sigma \text{ bijektiv}\}$ die symmetrische Gruppe von $\{1, \dots, n\}$.
Die Elemente von $S_n$ heißen Permutationen (von $\{1, \dots, n\}$).

**Bsp.:** $S_2 = \{\mathrm{id}_{\{1,2\}}, \tau\}$ mit $\tau(1) = 2$, $\tau(2) = 1$.

- Ist $X$ eine endliche Menge mit $\#X = n$, dann ist $\mathrm{Sym}(X)$ als Gruppe isomorph zu $S_n$, denn mit $X = \{x_1, \dots, x_n\}$ (bei irgendeiner Reihenfolge der El. von $X$) ist durch $T: S_n \to \mathrm{Sym}(X)$, $k \mapsto x_k$ für $k \in \{1, \dots, n\}$ ein (Gruppen-) Isomorphismus gegeben, d.h. $T$ ist bijektiv, $\forall \sigma, \tau \in S_n: T(\sigma \circ \tau) = T(\sigma) \circ T(\tau)$
- Somit: Um $\mathrm{Sym}(X)$ einer Menge $X$ mit $\#X = n$ zu untersuchen, reicht es, $S_n$ zu untersuchen. Ergebnisse über die Gruppenstruktur von $S_n$ übertragen sich dann zu solchen über die von $\mathrm{Sym}(X)$.

**Bem:** Jede Gruppe der Ordnung $n$ ist zu einer Untergruppe von $S_n$ isomorph (Satz von Cayley: $G = \{a_1, \dots, a_n\}$ $\rightsquigarrow$ jedem $a_i$ kann man eind. $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_i * a_1 & a_i * a_2 & \dots & a_i * a_n \end{pmatrix} \in S_n$ zuordnen). Zur Gruppentheorie "reicht" also das Studium der $S_n$...

1. **Satz:** $\forall n \in \mathbb{N}: \#S_n = n!$ $(= 1 \cdot 2 \cdot 3 \cdot \dots \cdot n)$.

**Bew.:** Nach obigem Kor. genügt es, die Anzahl der injektiven Abbildungen $\sigma: \{1, \dots, n\} \to \{1, \dots, n\}$ zu bestimmen. Für den Wert $\sigma(1)$ gibt es $n$ Möglichkeiten. Da $\sigma$ injektiv sein soll, bleiben für $\sigma(2)$ noch $n-1$ Möglichkeiten, für $\sigma(3)$ dann noch $n-2$ Möglichkeiten, ..., für $\sigma(n)$ noch $1$ Möglichkeit (gehen also induktiv vor). Insgesamt haben wir $n(n-1)\dots 2 \cdot 1 = n!$ viele Möglichkeiten, eine injektive Abb. anzugeben. □

**Bsp.:** • $S_3$ hat 6 Elemente, s. LG 7 auf S. 6 unten. Letzlich bedeutet dies, dass man 6 Möglichkeiten hat, die drei Zahlen 1, 2, 3 bzw. die drei Buchstaben a, b, c in eine Reihenfolge zu bringen:

| | | | |
|---|---|---|---|
| 1 2 3 | 2 1 3 | 3 1 2 | } lexikographisch angeordnet |
| 1 3 2 | 2 3 1 | 3 2 1 | |

- Entsprechend ist $n!$ die Anzahl der möglichen Reihenfolgen von $1, 2, \dots, n$.

**Bem.:** Eine Permutation $\sigma \in S_n$ kann man schreiben als $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$, d.h. z.B. die Abb. $\sigma \in S_3$ mit $\sigma: \begin{matrix} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{matrix}$ ist $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

Noch kompakter ist die Zykelschreibweise:

$\tau = (1\,2)\,(3\,7\,5)\,(6\,8\,9)$ ist $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 7 & 4 & 3 & 8 & 5 & 9 & 6 \end{pmatrix} \in S_9$ (4 ↓ Fixpunkt)

$\rightsquigarrow$ obiges $\sigma$ ist $\sigma = (1\,3\,2)$

(ii) Berechnen Sie $\tau^{-1}$ und $\tau^6$ in $S_9$.

Tipp: 1. zeilenvertauschen und neuordnen, 2. Potenzen von Zykeln untersuchen.

2. Satz: Eine $n$-elementige Menge hat $2^n$ Teilmengen. Kurz: $\#X = n \Rightarrow \#\mathcal{P}(X) = 2^n$.

Bew.: (Vollst. Ind.) $n=0$: Ist $X=\emptyset$, so ist $\mathcal{P}(\emptyset) = \{\emptyset\}$ einelementig, d.h. $\#\mathcal{P}(\emptyset) = 1 = 2^0$. ✓

$n \rightsquigarrow n+1$: Sei $\#X = n+1$ und $x \in X$. Dann ist $\mathcal{P}(X) = \{T \subseteq X \mid x \in T\} \cup \{T \subseteq X \mid x \notin T\}$ disjunkte Vereinigung zweier Mengen aus je $2^n$ vielen Elementen nach Ind. vor., also ist $\#\mathcal{P}(X) = 2 \cdot 2^n = 2^{n+1}$. □

Bem.: Aufgrund des 2. Satzes schreibt man manchmal auch $2^X$ für die Potenzmenge $\mathcal{P}(X)$ einer Menge $X$.

3. Satz: Eine $n$-elementige Menge besitzt $\binom{n}{k}$ verschiedene $k$-elementige Teilmengen mit $0 \le k \le n \in \mathbb{N}_0$.

Bem.: Die Zahl $\binom{n}{k}$ heißt Binomialkoeffizient (da sie als Koeffizient in der allgemeinen binomischen Formel $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ erscheint). Sie ist rekursiv definiert über

$\binom{n}{n} = \binom{n}{0} := 1$ für alle $n \in \mathbb{N}_0$, $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ für $1 \le k \le n$.

(Eine vollst. Ind. zeigt die Formel $\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{1 \cdot 2 \cdots k} = \frac{n!}{k!(n-k)!}$.)

Bew.: (Vollst. Ind.) Für $n=0$ ist bei $X=\emptyset$ nichts zu zeigen, haben $\binom{0}{0} = 1$.

$n \rightsquigarrow n+1$: Sei $\#X = n+1$, etwa $X = \{x_0, x_1, \dots, x_n\}$ und $0 \le k \le n+1$.

zu zeigen: $X$ hat $\binom{n+1}{k}$ viele (verschiedene) $k$-elementige Teilmengen.

Für $k=0$ (Teilmenge $\emptyset$) oder $k=n+1$ (Teilmenge $X$) ist dies wegen $\binom{n+1}{0} = \binom{n+1}{n+1} = 1$ richtig, sei also $1 \le k \le n$.

Haben wieder $\{T \subseteq X \mid \#T = k\} = \{T \subseteq X \mid x_0 \in T, \#T = k\} \cup \{T \subseteq X \mid x_0 \notin T, \#T = k\}$ als disjunkte Vereinigung,

$= \{T \subseteq \{x_1, \dots, x_n\} \mid \#T = k\}$, hat $\binom{n}{k}$ viele Elemente nach Ind. vor.

Da $\{T \subseteq X \mid x_0 \in T, \#T = k\} \longrightarrow \{T' \subseteq \{x_1, \dots, x_n\} \mid \#T' = k-1\}$

$T \longmapsto T \setminus \{x_0\}$

eine bijektive Abb. ist, haben beide Mengen gleich viele Elemente, nach Induktionsvoraussetzung nämlich $\binom{n}{k-1}$ viele.

Insgesamt hat $\{T \subseteq X \mid \#T = k\}$ also $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ viele Elemente. □

Der 2. und 3. Satz zusammen zeigt, dass $2^n = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k}$ gilt.

**Bem.:** Der 3. Satz liefert eine kombinatorische Deutung der Binomialkoeffizienten. Mit dieser kann der allgemeine binomische Satz bewiesen werden wie folgt:

$$(x+y)^n = \underbrace{(x+y)\cdot(x+y)\cdots(x+y)}_{n\text{-mal}} = \sum_{Z \subseteq \{1,\dots,n\}} x^{\#Z} y^{n-\#Z} = \sum_{k=0}^{n} \sum_{Z \subseteq \{1,\dots,n\},\ \#Z=k} 1 \cdot x^k y^{n-k}.$$

$Z$: mögliche Auswahl von Faktoren im Produkt $(x+y)\cdots(x+y)$, wo Summand "$x$" zum Ausmultiplizieren genommen wird

$\#Z = k$: $= \binom{n}{k}$ laut 3. Satz

**4. Satz:** Sei $X$ mit $\#X = n$ und $k_1, \dots, k_r \in \mathbb{N}_0$ mit $k_1 + k_2 + \dots + k_r = n$. Dann gibt es genau $\frac{n!}{k_1! \cdots k_r!}$ Abbildungen $f: X \to \{1, \dots, r\}$, die jedes $i$ genau $k_i$ mal als Wert annehmen, in Formeln:

$$\frac{n!}{k_1! \cdots k_r!} = \#\{f: X \to \{1,\dots,r\} \mid \#f^{-1}(i) = k_i \text{ für } i = 1, \dots, r\}.$$

[ohne Bew., wäre nicht schwer]

**Korollar:** Die **multinomische Formel** / der **Multinomialsatz**: ("$r$-nomischer Satz")

$$(x_1 + \dots + x_r)^n = \sum_{\substack{k_1, k_2, \dots, k_r \in \mathbb{N}_0 \\ \text{mit } k_1 + \dots + k_r = n}} \frac{n!}{k_1! \cdots k_r!} x_1^{k_1} \cdots x_r^{k_r}.$$

**Bew.:**

$$(x_1 + \dots + x_r)^n = \sum_{f: \{1,\dots,n\} \to \{1,\dots,r\}} x_1^{\#f^{-1}(1)} \cdots x_r^{\#f^{-1}(r)} = \sum_{\substack{k_1, k_2, \dots, k_r \in \mathbb{N}_0 \\ \text{mit } k_1 + \dots + k_r = n}} \sum_{f: \dots,\ \#f^{-1}(i) = k_i} 1 \cdot x_1^{k_1} \cdots x_r^{k_r}.$$

$= \frac{n!}{k_1! \cdots k_r!}$ laut 4. Satz

**Bem.:** Die kombinatorische Interpretation der Koeff. im $r$-nomischen Satz kann bei Kombinatorikproblemen helfen, sogesehen können Polynome / Potenzreihen ein kombinatorisches Werkzeug sein, Bsp.: Wieviele Möglichkeiten gibt es, einen Euro in Kleingeldmünzen (1-, 2-, 5-, 10-, 20-, 50-Cent-Münzen) zu wechseln? Die gesuchte Zahl ist der Koeff. vor $x^{100}$ im Polynom

$$\left(\sum_{n=0}^{100} x^n\right)\left(\sum_{n=0}^{50} x^{2n}\right)\left(\sum_{n=0}^{20} x^{5n}\right)\left(\sum_{n=0}^{10} x^{10n}\right)\left(\sum_{n=0}^{5} x^{20n}\right)\left(\sum_{n=0}^{2} x^{50n}\right)$$

und kann zu 4562 berechnet werden.

Anderes Bsp.: Die Identität $\left(\sum_{n=0}^{9} x^n\right)\left(\sum_{n=0}^{9} x^{10n}\right)\left(\sum_{n=0}^{9} x^{100n}\right)\cdots = \frac{1}{1-x}$ ist äquivalent zu dem Satz, dass jede natürliche Zahl auf genau eine Art im Dezimalsystem geschrieben werden kann.

# Vorlesung "Logische Grundlagen"

## LG9: Große Zahlen und unendliche Mengen

**Stichworte:** große Zahlen, abzählbar unendlich, $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ sind gleichmächtig, Lemma von Cantor, überabzählbar, $\mathcal{P}(\mathbb{N})$ und $\mathbb{R}$ sind überabzählbar, Cantorsche Diagonalverfahren, Hilberts Hotel

---

### §1: Große Zahlen

#Minuten pro Woche: $7 \cdot 24 \cdot 60 = 10.080 \approx 10^4$

#Mögl., ein 3×3-TicTacToe-Feld in 3 Farben anzumalen: $3^9 = 19.683 \approx 20.000 = 2 \cdot 10^4$

#Haare pro Mensch (im Schnitt): $100.000 = 10^5$

#Stunden in 114 Jahren: $\approx 1000.000 = 10^6$ (eine Million)

Erdumfang: $40.074\,km \approx 4 \cdot 10^7\,m$

#Sandkörner in einem Basketball: $\approx 20.000.000.000 = 2 \cdot 10^{10}$

# 9-buchstabige Wörter mit 26 Buchstaben a–z: $26^9 \approx 5.43 \cdot 10^{12}$

# Möglichkeiten, ein Schachbrett schwarz/weiß zu bemalen: $2^{64} \approx 18.5 \cdot 10^{19}$

Avogadro-Konstante (Teilchenzahl in Stoffmenge "1 Mol"): $6.02 \cdot 10^{23}$

#Atome in der Erde: $\approx 10^{50}$

#Mögl., 48 Punkte auf irgendeine Art miteinander zu verbinden: $\approx 10^{61}$

#Atome im beobachtbaren Universum: $\approx 10^{80}$

Zählwörter:

| | deutsch | englisch | chinesisch/japanisch | |
|---|---|---|---|---|
| $10^3$ | Tausend | thousand | $10^4$ | 万 |
| $10^6$ | Million | million | $10^8$ | 1億 |
| $10^9$ | Milliarde | billion | $10^{12}$ | 兆 |
| $10^{12}$ | Billion | trillion | ⋮ | ⋮ |
| $10^{15}$ | Billiarde | quadrillion | in 4er Gruppen aufsteigend | |
| $10^{18}$ | Trillion | quintillion | | |
| $10^{21}$ | Trilliarde | sextillion | | |
| $10^{24}$ | Quadrillion | septillion | | |
| ⋮ | | ⋮ | | |

Sehr große Zahlen:

Die Zahl $10^{100}$ (10 Sexdezilliarden) heißt auch 1 Googol (engl.); der Firmenname "google" ist davon abgeleitet.

Das beobachtbare Universum mal $10^{20}$ = 100 Trillionen hat $\approx$ 1 Googol Atome.

# Mögl., ein 10×10-Quadrat mit 10 Farben zu bemalen: $10^{100}$ = 1 Googol

# verschiedener QR-Codes (zum Einscannen): $2^{\underbrace{23.648}_{\text{"Bitzahl" laut Hersteller}}} = 10^{23.648 \cdot \frac{\log 2}{\log 10}} \approx 10^{7119}$

größte bekannte Primzahl:

$2^{74.207.281} - 1$ mit 22.338.618 vielen Dezimalstellen [vgl. GIMPS]

Exponentialtürme: $10^{10^{100}} = 10^{(10^{100})} = 10^{10^{10^2}}$ (10 hoch 1 Googol)

Skewes-Zahl: $10^{10^{10^{34}}}$ Nach S. Skewes benannt, der 1933 gezeigt hatte, dass $\int_2^x \frac{dt}{\log t} - \pi(x)$ noch vor dieser Zahl einen Vorzeichenwechsel besitzt, $\pi(x) := \#\{p \leq x \mid p \text{ prim}\}$.

Mittlerweile weiß man, dass nahe $1.4 \cdot 10^{316}$ ein solcher Vzwechsel stattfindet.

Zur Demonstration verglich G.H. Hardy die Skewes-Zahl mit der Anzahl möglicher Züge (Austausch zweier Atome), würde man mit allen Atomen des Universums Schach spielen.

Mittlerweile spielen auch noch größere Zahlen (bei endlichen Zahlen) eine Rolle in der Mathematik.

## §2: Unendlich große Mengen

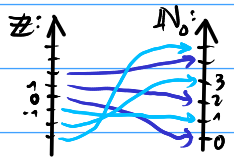
Angesichts dessen, dass die Vorstellungskraft für sehr große Zahlen schnell nachlässt und unser Universum endlich ist, erscheint es merkwürdig, von unendlich großen Mengen überhaupt zu sprechen. Dennoch ist das Konzept sehr nützlich in Anwendungen, wo die Wirklichkeit damit idealisiert und einfach beschrieben werden kann ("Kontinuum", etc....). In der Mathematik akzeptieren wir deswegen unendlich große Mengen auf natürliche Weise.

Das Unendlichkeitsaxiom von ZFC besagt (im wesentlichen), dass $\mathbb{N}$ (bzw. $\mathbb{N}_0$) eine unendlich große Menge ist. Nach Def. heißt dies, dass es für kein $n \in \mathbb{N}$ eine Bijektion $f: \{1, \dots, n\} \to \mathbb{N}$ gibt.

Def.: Eine Menge $X$ heißt abzählbar, wenn es eine injektive Abb. $X \to \mathbb{N}_0$ gibt.
Eine Menge $X$ heißt abzählbar unendlich, wenn $X$ abzählbar und unendlich ist.

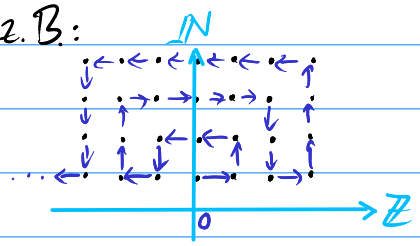
1. Bsp.: Unmittelbar klar ist, dass jede endliche Menge abzählbar ist.
Ebenso: $\mathbb{N}$ ist abzählbar unendlich.

2. Bsp.: $\mathbb{Z}$ ist abzählbar (unendlich), denn $f: \mathbb{Z} \to \mathbb{N}_0$, $f(z) := \begin{cases} 2z, & z \geq 0 \\ -(2z+1), & z < 0 \end{cases}$ ist injektiv.




3. Bsp.: $\mathbb{Q}$ ist abzählbar: Es gibt (wie im 2. Bsp.) viele Möglichkeiten, eine injektive Abb. $\mathbb{Q} \to \mathbb{N}_0$ zu konstruieren.
Jeder Bruch $q \in \mathbb{Q}$ lässt sich eindeutig als gekürzten Bruch $\frac{a}{b}$ mit $a \in \mathbb{Z}, b \in \mathbb{N}$ darstellen, daher ist $\mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$, $q = \frac{a}{b} \mapsto (a,b)$ injektiv.
Somit muss nur noch eine Bijektion $\mathbb{Z} \times \mathbb{N} \to \mathbb{N}_0$ hintergeschaltet werden,

z.B.:




oder:

$(0,1) \to (0,2) \to (0,3) \to (0,4) \ldots$
$(1,1) \leftarrow (1,2) \quad (1,3) \leftarrow (1,4) \ldots$
$(-1,1) \quad (-1,2) \leftarrow (-1,3) \quad (-1,4) \ldots$
$(2,1) \leftarrow (2,2) \quad (2,3) \leftarrow (2,4) \ldots$
$(-2,1) \quad (-2,2) \quad (-2,3) \quad (-2,4) \ldots$
$\vdots \quad \vdots \quad \vdots \quad \vdots$

(d.h. also: $(0,1) \mapsto 0$, $(0,2) \mapsto 1$, $(1,1) \mapsto 2$, $(-1,1) \mapsto 3, \ldots$)

Letzteres Abzählverfahren ist auch als 1. Cantorsches Diagonalverfahren bekannt.

Fazit: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ sind abzählbar unendlich und haben daher dieselbe Mächtigkeit, denn:

**Lemma:** Eine unendliche Menge $X$ ist genau dann abzählbar, wenn es eine bijektive Abb. $g: X \to \mathbb{N}_0$ gibt.

**Bew.:** „$\Rightarrow$": Wenn es eine solche Abb. $g$ gibt, ist $X$ abzählbar nach Def.
„$\Leftarrow$": Sei $X$ abzählbar, etwa $f: X \to \mathbb{N}_0$ injektiv. Dann ist
$f(X) = \{n_0, n_1, n_2, \ldots\}$ mit $n_0 < n_1 < n_2 < \ldots$, da $X$ unendlich.
Definiere $h: f(X) \to \mathbb{N}_0$, $n_j \mapsto j$. Dann ist $g := h \circ f: X \to \mathbb{N}_0$ bijektiv. □

**Def.:** Eine Menge $M$, die nicht abzählbar ist, heißt überabzählbar.

**Korollar:** Die Potenzmenge von $\mathbb{N}$, d.h. $\mathcal{P}(\mathbb{N}) := \{M \subseteq \mathbb{N}\}$, ist überabzählbar.

**Bew.:** Es kann nach dem Lemma von Cantor (s.u.) keine bijektive Abb. $\mathcal{P}(\mathbb{N}) \to \mathbb{N}$ geben. Nach dem Lemma folgt die Beh. □

**Lemma von Cantor:** $X$ Menge $\Rightarrow$ es gibt keine surjektive Abb. $X \to \mathcal{P}(X)$.

**Bew.:** Sei $f: X \to \mathcal{P}(X)$ eine Abb. Dann ist $f$ nicht surjektiv:
Es gilt: $f$ ordnet jedem $x \in X$ eine Teilmenge $f(x) \in \mathcal{P}(X)$ zu.
Setze $A := \{x \in X;\ x \notin f(x)\} \in \mathcal{P}(X)$.
Dann hat $A$ kein Urbild unter $f$, d.h. ex. kein $x \in X$ mit $f(x) = A$. [$\Rightarrow f$ nicht surj.]
Denn: • Für $x \in A$ ist $x \notin f(x)$, also $f(x) \neq A$ weil $x \in A \setminus f(x)$.
• Für $x \in X \setminus A$ ist $x \in f(x)$, also $f(x) \neq A$
[wäre $f(x) = A$, müsste für $x \in f(x) = A$ dann $x \notin f(x)$ sein. ↯]. □

Damit können wir zeigen, dass $\mathbb{R}$ überabzählbar ist. Somit gibt es (mindestens) zwei "Sorten" von Unendlichkeit, nämlich abzählbar unendlich und überabzählbar.

**Satz:** $\mathbb{R}$ ist überabzählbar.

Bem.: das Beweisverfahren hier, so oder ähnlich, heißt 2. Cantorsches Diagonalverfahren.

**Bew.:** Ziel: Konstruieren injektive Abb. $h: \mathcal{P}(\mathbb{N}) \to \mathbb{R}$.
[dies genügt: dann $\mathbb{R}$ überabzbar, weil $\mathcal{P}(\mathbb{N})$ überabz'bar laut Cantor-Lemma.]

Ist $A \subseteq \mathbb{N}$, def. charakteristische Fkt. $\chi_A: \mathbb{N} \to \{0,1\}$, $j \mapsto \begin{cases} 1, & j \in A \\ 0, & j \notin A \end{cases}$

Def. Fkt. $h: \mathcal{P}(\mathbb{N}) \to \mathbb{R}$, $A \mapsto h(A) := \sum_{j=1}^{\infty} \chi_A(j) \cdot 10^{-j} = 0,\underbrace{\chi_A(1)}_{\text{Dezimalbruch}}\underbrace{\chi_A(2)}_{}\ldots$

mit der Dezimaldarstellung einer reellen Zahl mit 0en und 1en als Nachkommastellen, welche so eind. bestimmt ist.

• Vgt. der Reihe klar wegen $0 \leq h(A) \leq \sum_{j=1}^{\infty} 10^{-j} = 0,111\ldots = \frac{1}{9}$,
Reihe ist monoton wachsend, also Vgt.

• Eind. der Darstellung (d.h. Injektivität von $h$) beweisbar:
$h(A) = h(B) \Rightarrow \sum_{j=1}^{\infty} \chi_A(j) 10^{-j} = \sum_{j=1}^{\infty} \chi_B(j) 10^{-j} \Rightarrow \sum_{j=1}^{\infty} \underbrace{(\chi_A(j) - \chi_B(j))}_{\in \{-1,0,1\}} \cdot 10^{-j} = 0$ (*)

Ann.: $k$ minimal mit $\chi_A(k) \neq \chi_B(k)$.
Dann: $10^{-k} = |\chi_A(k) - \chi_B(k)| \cdot 10^{-k} = \left|\sum_{j \geq k+1} (\chi_B(j) - \chi_A(j)) \cdot 10^{-j}\right|$, (aus (*))

aber $|r.S.| \leq \sum_{j \geq k+1} 10^{-j} = 10^{-k-1} \cdot \sum_{j=0} 10^{-j} = 10^{-k-1} \cdot \frac{1}{1 - \frac{1}{10}} = 10^{-k-1} \cdot \frac{10}{9} = 10^{-k} \cdot \frac{1}{9}$, ↯

Also sind alle $\chi_A(k) = \chi_B(k)$, also $A = B$. Also ist $h$ injektiv. □

**Bem.:** Häufig wird das 2. Cantorsche Diagonalverfahren wie folgt skizziert:
Wäre $\mathbb{R}$ abzählbar, dann auch das Intervall $[0,1] \subseteq \mathbb{R}$. Angenommen, man hätte eine Abzählung dieser reellen Zahlen (gegeben als Dezimalbrüche) wie folgt ($a_{ij} \in \{0,\dots,9\}$):

$\alpha_1 = 0, a_{11}\, a_{12}\, a_{13}\, a_{14} \dots$
$\alpha_2 = 0, a_{21}\, a_{22}\, a_{23}\, a_{24} \dots$
$\alpha_3 = 0, a_{31}\, a_{32}\, a_{33}\, a_{34} \dots$
$\vdots$

Betr. die Zahl $\beta = 0, b_1\, b_2\, b_3\, b_4 \dots$ mit $b_i := \begin{cases} 1, & a_{ii} \neq 1 \\ 2, & a_{ii} = 1 \end{cases}$, dann ist $\beta \neq \alpha_1$ da $b_1 \neq a_{11}$, $\beta \neq \alpha_2$ da $b_2 \neq a_{22}$, ..., also kommt $\beta$ nicht in der Abzählung vor, ↯. □

## §3: Hilberts Hotel

Um die Paradoxie des Begriffes "Unendlichkeit" zu demonstrieren, gab D. Hilbert die folgende bekannte Anekdote [vgl. auch F. Wille, Eine mathematische Reise]:
Hilberts Hotel hat unendlich viele Zimmer 1, 2, 3, 4, ... und ist vollbelegt.

(1.) Ein ankommender zusätzlicher Gast kann untergebracht werden.
(M zusätzliche Gäste können ebenso untergebracht werden.)
Wie?

(2.) Ein Bus mit unendlich vielen Gästen $g_1, g_2, g_3, \dots$ kommt an. Alle Gäste können untergebracht werden. Wie?

(3.) Unendlich viele Busse $b_1, b_2, b_3, \dots$ mit je unendlich vielen Gästen $b_1: g_{11}, g_{12}, g_{13}, \dots$, $b_2: g_{21}, g_{22}, g_{23}, \dots$, $b_3: g_{31}, g_{32}, g_{33}, \dots$ kommen an, alle Gäste können untergebracht werden.
Wie?

(4.) Ein Schiff mit Gästen, die mit (allen) reellen Zahlen $\in [0,1]$ durchnumeriert sind, kommt am Hafen an. Können alle Gäste im Hotel untergebracht werden?
Warum?

(5.) Im Hotel herrscht Rauchverbot. Es dürfen keine Zigaretten mitgebracht werden. Die Gäste wissen sich zu helfen: Gast Nr. 2 gibt Gast Nr. 1 eine Zigarette, Gast Nr. 3 gibt Gast Nr. 2 zwei Zigaretten, Gast Nr. 4 gibt Gast Nr. 3 drei Zigaretten, ... Am Ende hat jeder Gast eine Zigarette. Warum ist dies ein Trugschluss?

**Fazit:**
- unendliche Teilmengen einer unendlichen Menge sind deshalb nicht unbedingt "kleiner".
- unendliche Mengen werden nicht unbedingt "größer", wenn man sie mit einer disjunkten unendlichen Menge vereinigt

# Vorlesung "Logische Grundlagen"

## LG10: Das Auswahlaxiom

Stichworte: Familien, beliebige (Durch-) Schnitte/Vereinigungen/Produkte, Auswahlaxiom, dazu äquivalente Formulierungen (surj. $\Rightarrow \exists$ Rechtsinverse, bel. Produkte nichtleerer Mengen sind $\neq \emptyset$, Lemma von Zorn, jeder VR hat eine Basis), Fixpunktsatz von Bourbaki impliziert mit dem Auswahlaxiom das Lemma von Zorn

## §1: Familien, beliebige Schnitte/Vereinigungen/Produkte

1. Def.: Für eine bel. Menge $X \neq \emptyset$ und eine Abb. $\xi : \mathbb{N} \to X$ schreibt man auch $\xi(j) = \xi_j$ und $\xi = (\xi_j)_{j \in \mathbb{N}}$ und nennt $\xi$ eine Folge (in $X$). $\mathbb{N}$ heißt dann die Indexmenge der Folge.

2. Def.: Ist $J$ irgendeine Menge ($\neq \emptyset$) und $\xi : J \to X$ eine Abb., so schreibt man $\xi(j) = \xi_j$ und $\xi = (\xi_j)_{j \in J}$ und nennt $\xi$ eine Familie (in $X$) mit Indexmenge $J$.

Bem.: Für eine Familie $(\xi_j)_{j \in J}$ kann $J$ endlich oder unendlich sein. Ist $J$ endlich, etwa $J = \{j_1, \dots, j_n\}$, dann ist $(\xi_j)_{j \in J}$ ein $n$-Tupel und schreibt $(\xi_{j_1}, \xi_{j_2}, \dots, \xi_{j_n})$.

3. Def.: Ist $X \neq \emptyset$ eine Menge (von Mengen), so gilt:
$$\bigcap X := \{a \mid \forall A \in X : a \in A\},$$
diese Menge heißt Durchschnitt von $X$.

Bem.: Alle Elemente, die in allen Elementen von $X$ vorkommen, werden zu $\bigcap X$ zusammengefasst.

Bsp.: $\bigcap \{P, Q\} = P \cap Q$, $\bigcap \{P\} = P$, $\bigcap \{P, \{Q\}, \{\{R\}\}\} = P \cap \{Q\} \cap \{\{R\}\}$.

Notation: Ist $(X_j)_{j \in J}$ eine Familie von Mengen ($X_j$ sind Mengen), so schreibt man
$$\bigcap_{j \in J} X_j = \bigcap \{X_j \mid j \in J\} = \{a \mid \forall j \in J : a \in X_j\}$$

4. Def.: Ist $X \neq \emptyset$ eine Menge (von Mengen), so gilt:
$$\bigcup X := \{a \mid \exists A \in X : a \in A\},$$
diese Menge heißt Vereinigung von $X$.

Bem.: die Elemente aller Elemente von $X$ werden zu $\bigcup X$ zusammengefasst.

Bsp.: $\bigcup\{P,Q\} = P \cup Q$, $\bigcup\{P\} = P$, $\bigcup\emptyset = \emptyset$, $\bigcup\{\emptyset\} = \emptyset$,
$\bigcup\{P, \{Q\}, \{\{R\}\}\} = P \cup \{Q\} \cup \{\{R\}\}$.

Notation: Ist $(X_j)_{j\in J}$ eine Familie von Mengen ($X_j$ sind Mengen), so schreibt man
$$\bigcup_{j\in J} X_j = \bigcup\{X_j \mid j\in J\} = \{a \mid \exists\, j\in J : a\in X_j\}$$

5. Def.: • Sei $(X_j)_{j\in J}$ eine Familie von Mengen.
Das kartesische Produkt $\prod_{j\in J} X_j$ besteht aus allen Familien $(\xi_j)_{j\in J}$ mit $\xi_j \in X_j$.

• Falls $J$ endlich ist, $J = \{1,2,\dots,n\}$, schreibt man auch (wie gehabt)
$$\prod_{j\in J} X_j = \prod_{j=1}^{n} X_j = X_1 \times \dots \times X_n,$$
die Elemente $(\xi_1,\dots,\xi_n)$ mit $\xi_j \in X$ sind $n$-Tupel.
Ist zusätzlich $X_1 = X_2 = \dots = X_n = X$, schreibt man auch $\prod_{j=1}^{n} X = \underbrace{X\times\dots\times X}_{n\text{ mal}} = X^n$.
Ein anderes gebräuchliches Zeichen für $\prod_{j\in J}$ ist $\bigtimes_{j\in J}$.

Wir benötigen diese Grundbegriffe für beliebige Indexmengen zur Formulierung des Auswahlaxioms, und um es genauer studieren zu können.

## §2: Das Auswahlaxiom

Auswahlaxiom: Ist $X \neq \emptyset$ eine Menge und $P := \{A \subseteq X \mid A \neq \emptyset\}$ die Menge aller nichtleeren Teilmengen von $X$, dann gibt es eine Funktion (die wir Auswahlfunktion nennen) $c : P \to X$, die jeder Menge $A \in P$ ein Element $c(A)$ zuordnet ("auswählt").

Dieses Axiom haben wir bereits in LG 7 benutzt, um zu zeigen, dass jede surjektive Abb. eine Rechtsinverse besitzt. Umgekehrt kann man aus dieser Aussage wiederum das Auswahlaxiom herleiten.

Bem.: Im Auswahlaxiom geht es um Teilmengen von $X$. Teilmengen der Potenzmenge $\mathcal{P}(X) = \{A \subseteq X\}$ werden auch Systeme von Teilmengen von $X$ genannt.

Wir lernen jetzt noch weitere Umformulierungen des Axioms kennen.
Zunächst zeigen wir mit dem Auswahlaxiom folgendes.

**Satz:** Ist $(X_j)_{j\in J}$ eine Familie nichtleerer Mengen,
dann ist $\prod_{j\in J} X_j$ nicht leer.

**Bew.:** Sei $X = \bigcup_{j\in J} X_j$, sei $P = \mathcal{P}(X)\setminus\{\emptyset\}$ und sei $c: P \to X$
eine Auswahlfunktion. Nach Vor. gilt $X_j \in P$ für alle $j\in J$.
Sei $\xi_j = c(X_j)$. Dann gilt $\xi_j \in X_j$ für jedes $j\in J$, also $(\xi_j)_{j\in J} \in \prod_{j\in J} X_j$. □

- **Bem.:** Auch die Umkehrung, dass aus der Aussage des Satzes wieder das Auswahlaxiom folgt, kann gezeigt werden.
- **Bem.:** Der Satz zeigt, dass es für jede Folge $X_1, X_2, \ldots$ nichtleerer Teilmengen einer Menge $X$ eine Folge $x_1, x_2, x_3, \ldots$ von Elementen gibt, d.h. mit $x_j \in X_j$ für alle $j\in\mathbb{N}$. Dieses "Folgenauswahlaxiom" wird vom Beginn der Analysis an ständig (intuitiv) verwendet, z.B. im Beweis, dass jede folgenstetige Funktion das $\varepsilon$-$\delta$-Kriterium erfüllt. Sogesehen ist die Verwendung des Auswahlaxioms an vielen Stellen der gängigen Mathematik "versteckt", meist so, dass man es kaum noch bemerkt.

**Problem des Auswahlaxioms:** Die Aussage des Axioms ist eine reine Existenzaussage, es kann keineswegs eine explizite Auswahlfunktion angeben werden, und das ist dann auch mit den Konsequenzen des Auswahlaxioms so, dass diese reine Existenzaussagen liefern ohne jede Konstruktionsvorschrift. Das mag manchmal unbefriedigend sein. Besonders krass ist das wohl bei der Konsequenz, dass jeder Vektorraum (auch unendlichdimensionale!) eine Basis hat: man kann i.a. keine Basen in beliebigen Vektorräumen angeben, obwohl es sie laut Auswahlaxiom gibt! Wie man dieses Ergebnis aus dem Auswahlaxiom herleitet, werden wir nun kennenlernen.

Davon zunächst wiederum eine weitere Umformulierung, die auch als Zornsches Lemma bzw. Lemma von Zorn bekannt ist. Es handelt von (Halb-) und total geordneten Mengen, vgl. LG5. Wir brauchen noch zusätzlich:

6. **Def.:** Ist $M$ bzgl. $\leq$ (halb-) geordnet, so heißt eine bzgl. $\leq$ totalgeordnete Teilmenge $T$ von $M$ eine Kette. (Wir haben solche Mengen in LG5 schon ausdrücklich "Kette" genannt.)

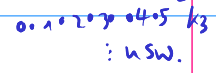
**Lemma von Zorn:** Sei $M$ eine Menge $\neq \emptyset$ mit (Halb)ordnung $\leq$ so, dass es für jede Kette $T \subseteq M$ ein $x \in M$ gibt $x \geq y$ für alle $y \in T$.
(M.a.W.: jede Kette habe eine obere Schranke in $M$.)
Dann hat $M$ (mindestens) ein maximales Element.

**Bem.:** Auch hier ist die Behauptung eine reine Existenzaussage. Eine Anleitung zur Konstruktion eines maximalen Elements liefert das Lemma nicht.

**Satz:** Es gilt: Auswahlaxiom $\Leftrightarrow$ Lemma von Zorn.

**Bew.:** Wir zeigen nur „$\Rightarrow$". Dazu benötigen wir im Beweis den Fixpunktsatz von Bourbaki (s.u.).
Sei nun zum Beweis des Lemmas von Zorn $M \neq \emptyset$ eine geordnete Menge. Betr. das System $S \subseteq \mathcal{P}(M)$ aller Ketten von $M$, bzgl. der Inklusion „$\subseteq$" ist $S$ geordnet. Also: $S = \{K \subseteq M \mid K \text{ Kette}\}$.
Dann hat jede Kette in $S$ ein Supremum (= kleinste obere Schranke in $S$), denn das Supremum über ein total geordnetes System $\mathcal{J} \subseteq S$ von Ketten ist einfach ihre Vereinigung $\bigcup_{K \in \mathcal{J}} K = \sup \mathcal{J}$ (ist ja Kette von $M$, also $\in S$).

„Kette von Ketten" ...




Def. nun eine Abb.

$$f: S \to S,\ K \mapsto f(K) := \begin{cases} K \cup \{x\}, & \text{falls } x \notin K \text{ ex. so, dass } K \cup \{x\} \text{ Kette,} \\ K, & \text{sonst.} \end{cases}$$

Hierfür benötigen wir das Auswahlaxiom, um für alle $K$ unter den jeweils möglichen $x$ eines auszuwählen. Nach dem Fixpunktsatz von Bourbaki (s.u.) hat nun $f$ einen Fixpunkt, es gibt also eine maximale Kette $K_{max} \subseteq M$. Eine obere Schranke einer solchen maximalen Kette ist dann notwendig ein maximales Element von $M$. □

**Fixpunktsatz von Bourbaki:** Ist $S$ eine bzgl. $\leq$ geordnete Menge, in der jede Kette ein Supremum in $S$ besitzt, so hat jede Abbildung $f: S \to S$ mit der Eigenschaft $f(x) \geq x$ für alle $x \in S$ einen Fixpunkt $s \in S$, d.h. es ist $f(s) = s$.

Der Beweis dieses Fixpunktsatzes ist etwas aufwändiger und kommt im Anschluss an folgendes Korollar zum Zornschen Lemma.

Zusammenhänge: Auswahlaxiom ⇓ Zornsches Lemma ⇐ Fixpunktsatz von Bourbaki ⇓ Jeder VR hat eine Basis.

**Satz:** Jeder Vektorraum $V$ hat eine Basis.

Wir benutzen dafür die folgende Charakterisierung des Begriffs "Basis":

Aus Lin.Alg.I: $S \subseteq V$ ist Basis $\Leftrightarrow$ $S$ ist maximale lin. unabh. Teilmenge von $V$, d.h. $S$ ist lin.unabh. und jede Obermenge von $S$ ist lin.abh.

**Bew. des Satzes:**

Sei $M$ die Menge der lin. unabh. Teilmengen von $V$, mit der Halbordnung "$\subseteq$".

Das Zornsche Lemma liefert die Existenz einer maximalen lin. unabh. Teilmenge von $M$, also eine Basis, sofern die Voraussetzungen erfüllt sind, welche wir nur noch zu überprüfen brauchen:

Es bleibt z.z.: Ist $T \subseteq M$ total geordnet bzgl. $\subseteq$, d.h. eine Kette in $M$, so gibt es eine lin. unabh. Teilmenge $S \subseteq V$ mit $S' \subseteq S$ für alle $S' \in T$.

Wähle $S := \bigcup_{S' \in T} S'$, dann gilt $S' \subseteq S$ für alle $S' \in T$.

Es bleibt z.z.: $S$ ist lin. unabh., d.h. $S \in M$.

Dazu seien $v_1, \dots, v_n \in S$ und $\lambda_1, \dots, \lambda_n \in K$ geg. mit $\lambda v_1 + \dots + \lambda_n v_n = 0$.

Jedes $v_i$ liegt in einem $S_i \in T$. Da $T$ Kette ist, gilt nach Umnumerierung $S_1 \subseteq S_2 \subseteq \dots \subseteq S_n$, also sind $v_1, \dots, v_n \in S_n$.

Da $S_n$ lin. unabh. ist, folgt aus $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$ bereits, dass alle $\lambda_1 = \lambda_2 = \dots = \lambda_n = 0$ sind.

Also ist $S$ lin. unabh. □

**Bew. des Fixpunktsatzes von Bourbaki:** Seien $S$ und $f$ laut Vor. gegeben.

1. Bem.: $S$ besitzt notwendig ein kleinstes Element, nämlich $k = \sup \emptyset$, denn $\emptyset$ ist Kette.

2. Nur für den Beweis benötigen wir folgende Definition: Eine Teilmenge $T \subseteq S$ heißt Turm (in Bezug auf $f$) genau dann, wenn gilt: a) das kleinste Element $k$ von $S$ gehört zu $T$, b) aus $t \in T$ folgt $f(t) \in T$, c) ist $K \subseteq T$ eine Kette, so gehört auch $\sup K$ zu $T$.

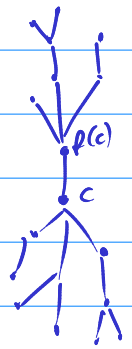
3. Bem.: Es reicht nun, einen Turm $T$ zu finden, der auch Kette ist, denn dann ist $\sup T$ das größte Element von $T$ und damit ein Fixpunkt von $f$. Der Schnitt über alle Türme in $S$ ist offensichtlich der bzgl. "$\subseteq$" kleinste Turm von $S$, wir nennen ihn $R$. Beh.: $R$ ist Kette. (Ist dies gezeigt, sind wir fertig.)
Def.: Ein El. $c \in R$ des kleinsten Turmes $R$ heißt eng, falls $\forall a \in R: a < c \Rightarrow f(a) \leq c$.
$[\Leftrightarrow (f(a) > c \Rightarrow a \geq c)]$

4. Beh. (1): Sei $c \in R$ eng, dann: $\forall x \in R: x \leq c \vee f(c) \leq x$.
Bew.: Gen.z.z.: $R_c = \{x \in R \mid x \leq c \vee f(c) \leq x\}$ ist Turm. Dann $R_c = R$.
Zu a): Klar ist $k \in R_c$. Zu c): Ist $K \subseteq R_c$ eine Kette, so folgt $\sup K \in R_c$.
Zu b): aus $t \in R_c$ folgt $f(t) \in R_c$, was aus "$c$ eng" folgt: $t < c \vee f(c) \leq t \leq f(t) \vee t = c$
$\Rightarrow f(t) \leq c$ / $\Rightarrow f(t) \in R_c$ ; $\Rightarrow f(c) \leq f(t)$ (nach vor.) / $\Rightarrow f(t) \in R_c$ ☒

5. Beh. (2): Jedes Element $a \in R$ ist eng.
Bew.: Gen.z.z.: $E := \{c \in R \mid c \text{ eng}\}$ ist Turm. Dann $E = R$. Zu a): Klar ist $k \in E$.
Zu b): Zu $t \in E$ folgt $f(t) \in E$, denn für $t$ eng folgt aus $a < f(t)$ schon $a \leq t$ laut Beh. (1).
Zu c): Noch z.z.: $\forall K \subseteq E$, $K$ Kette: $b := \sup K \in E$.
Sei dazu $a \in R$ und $a < b$, z.z. ist $f(a) \leq b$.
Wenn $a < c$ für ein $c \in K$, so folgt wegen $c$ eng sofort $f(a) \leq c \leq b$.
• Wenn nicht, so gilt $a \geq c$ für alle $c \in K$, folglich $a \geq b$ im $\lightning$ zur Annahme. ☒

6. Beweisende: Beh. (2) und (1) zeigt, dass $R$ total geordnet ist. $f(c) \geq c$,
Also ist $R$ sowohl ein Turm als auch eine Kette,
und $\sup R$ ist ein Fixpunkt von $f$. □

Bemerkung zur Anschauung: Anschaulich beschreiben $S$ und $f$ mehr oder weniger geordnetes Schlangestehen, etwa um in ein Flugzeug zu gelangen. Dann wäre $S$ eine Menge möglicher Standplätze und $f$ eine Vorschrift, die die Reisenden in jedem Zeitschritt von einem Standplatz zu einem besseren Standplatz vorrücken lässt oder aber stehenbleiben lässt. Ein enges Element einer unter $f$ in sich abgebildete Teilmenge $R \subseteq S$ wäre etwa ein Standplatz direkt vor einem Drehkreuz, an dem die Bordkarten eingesammelt werden und alle Reisenden auf Standplätzen aus $R$ einzeln vorbeigehen müssen, um ins Flugzeug zu gelangen. An einem engen El. hat $S$ einen "Flaschenhals".



# Vorlesung "Logische Grundlagen"

## LG11: Die ZFC-Axiome

**Stichworte:** alle 10 ZFC-Axiome mit Besprechung, Erweiterungen von ZFC, Widerspruchsfreiheit von ZFC, Gödelsche Unvollständigkeitssätze, Kontinuumshypothese

---

## §1: ZFC

Die ZFC-Axiome der Mengenlehre bilden (zusammen mit der Prädikatenlogik) seit knapp 100 Jahren die Grundlage für die moderne Mathematik. So gut wie alle bewiesenen Sätze der Mathematik lassen sich als beweisbare Aussagen aus ZFC ableiten.

Dabei steht Z für E. Zermelo (1871–1953)
F für A. Fraenkel (1891–1965)
und C für "choice" = "Auswahl", d.h. dem Auswahlaxiom.

Die ZFC-Mengenlehre ist eine Erweiterung der Zermelo-Mengenlehre um Axiome/Anregungen von A. Fraenkel (um 1920), speziell die Idee, dass alle Objekte der Mathematik letztlich Mengen sind, geht auf Fraenkel zurück.

Wir listen die 10 ZFC-Axiome im folgenden auf. Vielen sind wir in der Vorlesung bereits begegnet als "intuitiv klar" – wie es "gute" Axiome sein sollten.

Axiom 1: Extensionalitätsaxiom

Mengen sind genau gleich, wenn sie dieselben Elemente enthalten.

$$\forall A,B: \quad A = B \Leftrightarrow \forall C: (C \in A \Leftrightarrow C \in B)$$

Bem.: Damit ist jede Menge durch ihre Elemente bestimmt.

Axiom 2: Leermengenaxiom (Älter: Nullmengenaxiom)

Es gibt eine Menge, die keine Elemente hat.

$$\exists A \, \forall X: \; X \notin A$$

Bem.: Dies garantiert die Existenz "der" leeren Menge: Aus Axiom 1 folgt bereits die Eindeutigkeit von $\emptyset$.

Axiom 3: Paarmengenaxiom

Für alle $A$ und $B$ gibt es eine Menge, die $A$ und $B$ als Elemente hat.

$\forall A,B\ \exists C\ \forall D: (D \in C \Leftrightarrow D = A \vee D = B)$

Bem.: $C$ ist nach Axiom 1 wieder eindeutig bestimmt, wir schreiben $C = \{A,B\}$.

Axiom 4: Vereinigungsaxiom

Für jede Menge $A$ gibt es eine Menge $B$, deren Elemente genau die Elemente der Elemente von $A$ sind: $\forall A\ \exists B\ \forall C: (C \in B \Leftrightarrow \exists D: D \in A \wedge C \in D)$

Bem.: $B$ ist nach Axiom 1 eindeutig bestimmt und heißt die Vereinigungsmenge von $A$, geschrieben $B = \bigcup A$. Wir haben diese allgemeine Vereinigungsmenge schon in LG10 eingeführt – das Axiom 4 garantiert die Existenz der Vereinigungen.
Weiter: sind $A,B$ Mengen, ex. nach Axiom 3 die Menge $\{A,B\}$ und somit nach Axiom 4 dann $A \cup B := \bigcup\{A,B\}$.

Axiom 5: Potenzmengenaxiom

Zu jeder Menge $A$ gibt es eine Menge $B$, deren Elemente genau die Teilmengen von $A$ sind: $\forall A\ \exists B\ \forall C: C \in B \Leftrightarrow (\underbrace{\forall D: D \in C \Rightarrow D \in A}_{\text{Kurz: } C \subseteq A})$

Bem.: Nach diesem Axiom existiert die Potenzmenge $\mathcal{P}(A) := \{C \subseteq A\}$.

Axiom 6: Aussonderungsaxiom

Ist $A$ eine Menge und $\Phi$ eine Aussage/Bedingung (genau: ein Prädikat), so gibt es eine Teilmenge $B$ von $A$, die genau die Elemente $C$ von $A$ enthält, für die $\Phi(C)$ wahr ist.

$\forall A\ \exists B\ \forall C: C \in B \Leftrightarrow C \in A \wedge \Phi(C)$

Bem.: Somit existieren "eingeschränkte" Mengen der Form $\{C \in A \mid \Phi(C)\}$; die Elemente von $A$, für die $\Phi$ wahr ist, werden "ausgesondert".
Genaueres zu $\Phi$: dies muss ein einstelliges Prädikat sein, in dem die Variable $B$ nicht vorkommt.

Weitere Bem. zum Aussonderungsaxiom:

(i) Die Einschränkung auf eine Grundmenge $A$ im Axiom ist nötig, um die Russelsche Antinomie zu vermeiden: Sonst impliziert Axiom 5 mit $\exists B \forall C: (C \in B \Leftrightarrow C \notin C)$ die Existenz der Menge aller Mengen, die sich nicht selbst enthalten – die Russel-Menge $R$, die den logischen Widerspruch $R \in R \Leftrightarrow R \notin R$ erzeugt.

(ii) Die Annahme, dass es eine Menge aller Menge gäbe, also $\exists A \forall B: B \in A$ führt mit Axiom 4 zu einem Widerspruch.

(iii) Mit Axiom 6 kann man Axiom 2 ersetzen durch "Es gibt überhaupt eine Menge $A$", die leere Menge erhält man dann durch Aussondern: $\emptyset = \{C \in A \mid C \notin A\}$. (Auch Axiom 8 würde die Existenz von Mengen implizieren.)

Axiom 7: Ersetzungsaxiom (nach Fraenkel)

Ist $A$ eine Menge und $\Phi$ eine Aussage/Bedingung (genau: ein Prädikat), die jeder Menge $B$ genau eine Menge $\Phi_B$ zuordnet, so ist $D = \{\Phi_F \mid F \in A\}$ wieder eine Menge.

$$\forall A: \left(\forall B \exists! \underbrace{C}_{\uparrow (\text{als } \Phi_B \text{ geschrieben})}: \Phi(B,C) \Rightarrow \left(\exists D \forall E: E \in D \Leftrightarrow \exists F: F \in A \wedge \Phi(F,E)\right)\right)$$

Bem.: Wird jedes Element von $A$ durch eine neue Menge ersetzt, entsteht eine neue Menge; die Ersetzung wird mit zweistelligen Prädikaten vorgenommen.

Die Menge $D$ schreiben wir als $D = \{E \mid F \in A \wedge \Phi(F,E)\}$

bzw. $D = \{E \mid \exists F \in A: \Phi(F,E)\}$.

Axiom 8: Unendlichkeitsaxiom

Es gibt eine Menge $A$ mit $\emptyset \in A$ und $\forall B: B \in A \Rightarrow B \cup \{B\} \in A$.

Bem.: Diese Menge $A$ enthält offenbar alle natürlichen Zahlen: Vgl. LG4 und die dort angegebenen Konstruktion der natürlichen Zahlen. Die "Peano-Axiome" sind keine Axiome im eigentlichen Sinn sondern können aus ZFC hergeleitet werden, wofür Axiom 8 grundlegend ist. Die aus den "Peano-Axiomen" herleitbaren Aussagen fasst man unter dem Begriff "Peano-Arithmetik" zusammen. Insb. Axiom 8 impliziert, dass $\mathbb{N}$ eine unendl. Menge ist (gemäß Def. aus LG9).

Axiom 9: Fundierungsaxiom / Regularitätsaxiom

Jede nichtleere Menge A enthält ein Element B, so dass A und B disjunkt sind.

$$\forall A: A \neq \emptyset \Rightarrow \exists B: B \in A \wedge \forall C: \underbrace{C \notin A \vee C \notin B}_{\Leftrightarrow \neg (C \in A \wedge C \in B)}$$

Bem.: Axiom 9 wurde später von Zermelo hinzugefügt, um unendliche aber zyklische Ketten der Form $a_1 \ni a_2 \ni a_3 \ni \dots$ auszuschließen, wie von Fraenkel gefordert wurde.
[Sonst hätte die Menge $A = \{a_1, a_2, \dots\}$ die Eigenschaft $\forall i: a_{i+1} \in \{a_i\} \cap A$ im Widerspruch zu Axiom 9.]

Somit kann eine Menge nicht sich selbst als Element enthalten. [Die Kette $A \ni A$ ist ausgeschlossen]

Axiom 10: Auswahlaxiom

Ist A eine Menge von paarweise disjunkten nichtleeren Mengen, so gibt es eine Menge B, die genau ein Element aus jedem Element von A enthält.

$$\forall A: \emptyset \notin A \wedge (\forall C, D, E: C \in A \wedge D \in A \wedge E \in C \wedge E \in D \Rightarrow C = D)$$
$$\Rightarrow (\exists B \; \forall F: F \in A \Rightarrow \exists! G: G \in F \wedge G \in B)$$

1. Bem.: Jedem Element F von A wird also ein Element G von F zugeordnet; im Sinne einer Auswahlfunktion wie in LG10 formuliert.
Dort haben wir einige Umformulierungen von Axiom 10 kennengelernt, es gibt noch mehr, u.a. das sogenannte Wohlordnungssatz ("Jede Menge lässt sich wohlordnen", bewiesen (mit dem Auswahlaxiom) von E. Zermelo).
Das Auswahlaxiom ist das umstrittenste Axiom der Mathematik. Mathematiker, die es ablehnen, heißen Konstruktivisten. Die Problematik haben wir in LG10 schon besprochen. Letztlich führt es auch zu kontraintuitiven Aussagen wie dem Banach-Tarski-Paradoxon.
2. Bem.: Das ZFC-System ist redundant, d.h. die folgenden Axiome sind entbehrlich:
- Das Aussonderungsaxiom folgt aus dem Ersetzungsaxiom.
- Das Leermengenaxiom folgt aus dem Aussonderungsaxiom und der Existenz irgendeiner Menge (z.B. Unendlichkeitsaxiom).
- Das Paarmengenaxiom folgt aus dem Ersetzungsaxiom und dem Potenzmengenaxiom.

## §2: Erweiterungen und Widerspruchsfreiheit von ZFC

ZFC ist grundlegend für die gesamte moderne Mathematik.
Es gibt Ausnahmen, wo ZFC nicht mehr ausreicht, z.B. wo man mit echten Klassen statt Mengen arbeiten muss (typischerweise manche Strukturen in Algebra), dafür gibt es dann passende Erweiterungen von ZFC.

Seit 1918 wurde im Rahmen des Hilbert-Programms ein Beweis für die Widerspruchsfreiheit von ZFC gesucht.
K. Gödel zeigte um 1930 seinen zweiten Unvollständigkeitssatz, der zeigt, das ein solcher Beweis im Rahmen der ZFC-Mengenlehre unmöglich ist, ja sogar, dass jede hinreichend mächtige formale, widerspruchsfreie System nicht die eigene Widerspruchsfreiheit beweisen kann.
Der erste Unvollständigkeitssatz von Gödel gesagt, dass jedes hinreichend mächtige formale System entweder widersprüchlich oder unvollständig (d.h. nicht jede im System formulierbare wahre Aussage kann darin bewiesen werden) ist.
Die Annahme der Widerspruchsfreiheit der ZFC-Mengenlehre wird letztlich nur durch die Erfahrung belegt, dass ZFC seit ca. 100 Jahren benutzt wird ohne dass sich je ein Widerspruch gezeigt hat. Daher geht man eher von der Unvollständigkeit der modernen Mathematik aus, z.B. dass die Riemannsche Vermutung wahr aber unbeweisbar sein könnte (meines Wissens weiß man nur, dass sie mit ZFC widerlegbar ist, sollte sie falsch sein, nämlich ganz einfach durch die explizite Angabe einer Ausnahmenullstelle von $\zeta$ im kritischen Streifen).

Eine weitere interessante Fragestellung im Zusammenhang mit ZFC ist die Kontinuumshypothese (CH): Für keine Menge $X$ ist $\#\mathbb{N} < \#X < \#\mathbb{R}$.
Hier bezeichnet $\#X$ für eine (bel. unendl.) Menge $X$ die Kardinalzahl von $X$, welche als Äquivalenzklasse von $X$ bzgl. der Äq.-Rel. $X \sim Y :\Leftrightarrow \exists$ Bijektion $X \to Y$ definiert wird. D. Hilbert präsentierte CH als 1. Problem (von 23) auf dem Mathematiker-Kongress 1900.
- K. Gödel zeigte 1938: ist ZFC widerspruchsfrei, dann auch ZFC mit (CH) als Axiom
- P. Cohen zeigte 1963: ist ZFC widerspruchsfrei, dann auch ZFC mit $\neg$(CH) als Axiom

Damit ist (CH) unabh. von ZFC und kann hinzugenommen werden oder sein Gegenteil oder nicht.