Mathematik I für Informatiker

Mathias Schacht

Fachbereich Mathematik
Universität Hamburg

WiSe 2016/17

Stand: 21. Oktober 2016

Termine

Vorlesung	Do	10:15 – 11:45	Erzwiss H (VMP 8)
	Fr	16:15 – 17:45	Hörsaal A (ESA 1)

Übung
- 16 Gruppen (Zuordnung über STiNE)
- Do 14-16, Fr 10-12, 12-14, 14-16 und 18-20
- 45 Minuten Hausaufgabenbesprechung
- 45 Minuten Präsenzübung
- Beginn heute

Tutorium
- 2 reguläre Termine
- Mi 12-14 und Do 16-18
- Beginn heute
- sporadische Zusatztermine (Klausurvorbereitung) - Mi 18-21

- zwei **Bonusklausuren** im Semester während der VL (Termine später)
- Klausurtermine

Spielregeln

Übungsblätter

- wöchentliche Aus- und schriftliche Abgabe in den Übungsgruppen
- Bearbeitung und Abgabe in 2er Gruppen (Einzelabgabe erlaubt)
- Zulassungskriterium für die Klausur ist das Erreichen von mindestens 50% der Punkte über alle Übungsblätter

Klausur

- zwei mögliche Termine in der vorlesungsfreien Zeit
- Ergebnisse der beiden Bonusklausuren (dieses Semesters) werden positiv verrechnet
- Klausurergebnis entspricht der Modulnote MafI1
  $\longrightarrow$ Abschneiden bei den UE-Blättern nur für die Teilnahme wichtig

Webseite

- Weitere Informationen, das Skript, die Folien und die UE-Blätter:
  www.math.uni-hamburg.de/home/schacht/lehre/WS16/VL_MafI1.html

1. Mathematische Grundlagen und Logik

Naive Mengenlehre

Fragen im 19. Jahrhundert:

- Was sind die Grundlagen der Mathematik/Arithmetik?
- Was sind Zahlen? Was sind Mengen? Darf es unendliche Mengen geben?

Idee/Definition (Ende 19. Jahrhundert, Cantor 1895)

Mengen sind ungeordnete Zusammenfassungen von wohlunterschiedenen Objekten (unseres Denkens) zu einem Ganzen.

Beispiele: $\{10^{10}, 1, \pi, 19, 2001\}$, Menge der natürlichen Zahlen, $\{A, x, 1, B\}$

Definition (Frege 1893)

Für jedes sprachliche Prädikat P gibt es die **Menge** M_P aller der Objekte O, auf die das Prädikat P zutrifft

$$M_P = \{O\colon P(O) \text{ gilt}\}\,.$$

Objekte O für die $P(O)$ gilt, heißen **Elemente von** M_P

$$O \in M_P\,.$$

Russels Paradoxon

Antinomie (Russel 1903)

Sei P das Prädikat „x enthält sich nicht selbst als Element“, d. h.

$$M_P := \{O\colon P(O) \text{ gilt}\} = \{O\colon O \notin O\}\,.$$

Widerspruch: $M_P \notin M_P$ genau dann, wenn $M_P \in M_P$.

Beweis: Auf der einen Seite erhalten wir

$$\begin{aligned} M_P \notin M_P &\overset{\text{Def.}\notin}{\Longrightarrow} M_P \text{ enthält sich nicht selbst als Element} \\ &\overset{\text{Def.}P}{\Longrightarrow} P(M_P) \text{ gilt} \overset{\text{Def.}M_P}{\Longrightarrow} M_P \in M_P \qquad ↯ \end{aligned}$$

und auf der anderen Seite erhalten wir

$$\begin{aligned} M_P \in M_P &\overset{\text{Def.}\in}{\Longrightarrow} M_P \text{ enthält sich selbst als Element} \\ &\overset{\text{Def.}P}{\Longrightarrow} P(M_P) \text{ gilt nicht} \overset{\text{Def.}M_P}{\Longrightarrow} M_P \notin M_P \qquad ↯ \qquad \square \end{aligned}$$

$\Longrightarrow$ M_P kann nicht existieren
Freges Ansatz ist nicht widerspruchsfrei!

Auflösung des Paradoxons

Probleme in Freges Definition:

- Was ist ein Prädikat? Wann ist ein Prädikat „wahr“, wann „gilt“ es?
- Was sind Objekte? Gibt es eine „Grundmenge“ aller Objekte?

Ausweg:

- Formalisierung mathematischer Sprache (**Aussagen**) und **Regeln**
  $\longrightarrow$ mathematische Logik
- Benennung als wahr angenommener Grundaussagen (**Axiome**)
  $\longrightarrow$ axiomatische Mengenlehre
- der Wahrheitswert aller anderen Aussagen wird formal mit Hilfe der Regeln aus den Axiomen hergeleitet (**Beweis**) $\longrightarrow$ Mathematik

Probleme:

- (innere) Widerspruchsfreiheit der Regeln und Axiome unentscheidbar
- Vollständigkeit – Sind alle wahren Aussagen beweisbar? Nein, Gödel

Bemerkungen

- Standardaxiomensystem benannt nach Zermelo und Fraenkel
- hinzu kommt oft das sogenannte Auswahlaxiom (Axiom of **C**hoice)
  $\rightarrow$ ZFC-Axiome
- Axiome etablieren Grundmengen und zulässige Operationen, um aus bestehenden Mengen weitere Mengen abzuleiten
- Großteil der Mathematik kann innerhalb **ZFC** bewiesen werden
- Innerhalb von ZFC lassen sich die *üblichen* Zahlenmengen

$$\begin{aligned}
\mathbb{N} &= \text{Menge der natürlichen Zahlen},\\
\mathbb{Z} &= \text{Menge der ganzen Zahlen},\\
\mathbb{Q} &= \text{Menge der rationalen Zahlen},\\
\mathbb{R} &= \text{Menge der reellen Zahlen},\\
\mathbb{C} &= \text{Menge der komplexen Zahlen}
\end{aligned}$$

definieren und Aussagen darüber beweisen.

ZFC – Axiome der Mengenlehre Teil 1

1. **Existenz der leeren Menge**: Es existiert eine Menge die kein Element enthält.
$$(\exists x)(\forall y)(y \notin x)$$

2. **Extensionalitätsaxiom**: Zwei Mengen sind genau dann gleich, wenn sie die gleichen Elemente enthalten.
$$(\forall x)(\forall y)\Big((x = y) \Leftrightarrow \Big((\forall z)\big((z \in x) \Leftrightarrow (z \in y)\big)\Big)\Big)$$

3. **Paarmengenaxiom**: Für je zwei Mengen A, B existiert die Menge $\{A, B\}$.
$$(\forall x)(\forall y)(\exists z)(\forall u)\Big((u \in z) \Leftrightarrow \big((u = x) \vee (u = y)\big)\Big)$$

4. **Vereinigungsmengenaxiom**: Für jede Menge A gibt es eine Menge $\bigcup A$ deren Elemente die Elemente der Elemente von A sind.
$$(\forall x)(\exists y)(\forall z)\Big((z \in y) \Leftrightarrow \big((\exists u)\big((u \in x) \wedge (z \in u)\big)\big)\Big)$$

5. **Potenzmengenaxiom**: Für jede Menge A existiert die **Potenzmenge** $\wp(A)$ die alle Teilmengen von A als Elemente enthält.
$$(\forall x)(\exists y)(\forall z)\Big((z \in y) \Leftrightarrow \big((\forall u \in z)(u \in x)\big)\Big)$$

6. **Aussonderungsaxiom**: Für jede Menge A und jede Aussageform $p(x)$ existiert die Menge $\{A' \in A\colon p(A')\}$, die Teilmenge von A deren Elemente $p(x)$ erfüllen.
$$(\forall x)(\exists y)(\forall z)\Big((z \in y) \Leftrightarrow \big(z \in x) \wedge p(z)\big)\Big)$$

ZFC – Axiome der Mengenlehre Teil 2

7. **Unendlichkeitsaxiom**: Es gibt eine Menge N, die die leere Menge als Element enthält und für jede Menge A, die ein Element von N ist, auch den **Nachfolger** $A^+ := A \cup \{A\}$ in N als Element enthält.

$$(\exists x)\Big((\varnothing \in x) \wedge (\forall y \in x)((y \cup \{y\}) \in x)\Big)$$

8. **Ersetzungsaxiom**: Das „Bild einer Menge unter einer Funktion" ist eine Menge. Für jede Aussagenform $p(x, y)$ mit der Eigenschaft, dass für jede Menge A genau eine Menge B existiert für die $p(A, B)$ gilt, und für jede Menge M ist die Zusammenfassung der N', für die eine $N \in M$ mit $p(N, N')$ existiert, eine Menge.

$$(\forall x)(\exists y)(\forall z)\big((z \in y) \Leftrightarrow ((\exists u \in x)p(u, z))\big)$$

9. **Fundierungsaxiom**: Jede nicht leere Menge A enthält ein Element A', deren Schnitt mit A leer ist.

$$\big((\forall x)(x \neq \varnothing)\big) \Rightarrow \big((\exists y \in x)(\forall z \in y)(z \notin x)\big)$$

10. **Auswahlaxiom**: Für jede nicht leere Menge A bestehend aus paarweise disjunkten nicht leeren Mengen existiert eine Menge B, die aus jeder Menge $A' \in A$ genau ein Element enthält.

$$(\forall x)\Big(\big((\forall y \in x)(y \neq \varnothing)\big) \wedge (\forall y \in x)(\forall z \in x)\big((y \neq z) \Rightarrow (y \cap z = \varnothing)\big)\Big)$$
$$\Rightarrow (\exists u)(\forall y \in x)(\exists! z \in y)(z \in u)$$

Hierbei steht $\exists!$ für „es existiert genau ein", d. h. $(\exists! x)p(x)$ ist genau dann **wahr**, wenn die Aussage $(\exists x)\big(p(x) \wedge (\forall y)((y \neq x) \Rightarrow \neg p(y))\big)$ wahr ist.

Mengen

- Angabe der Axiome in dieser VL nur zur Kenntnisnahme
  $\longrightarrow$ explizit **nicht** klausurreleveant
- in dieser VL reicht der folgende intuitive Mengenbegriff von Cantor

Definition (Mengen)

Eine Menge ist eine Zusammenfassung bestimmter, wohlunterschiedener Objekte, die die Elemente der Menge genannt werden.

- Vermeidung des Russelschen Paradoxon wird dadurch erreicht, dass in Mengendefinitionen jeweils eine Grundmenge angeben werden muss

$$M = \{x \in X \colon x \text{ erfüllt } \dots\}$$

  und die „Menge aller Mengen“ **keine** Menge ist.
- Außerdem gibt es keine Mengen, die sich selbst als Element enthalten.

Mengenlehre

- Mengen sind ungeordnet, d. h. Elemente haben keine Reihenfolge
- Elemente können nicht mehrfach in Mengen vorkommen

$\Rightarrow$ jede Menge ist eindeutig durch ihre Elemente bestimmt und zwei Mengen sind gleich, wenn sie dieselben Elemente enthalten

$$\{x, y, z\} = \{y, z, x\} = \{y, z, x, x, z\}$$

- $x \in M$ steht für „x ist ein Element der Menge M"
- $B \subseteq A$ steht für „die Menge B enthält nur Elemente aus A"
  $\rightarrow$ B ist eine Teilmenge von A
- $\varnothing$ (auch $\{\,\}$) steht für die leere Menge, die Menge ohne Elemente

Beispiel

$$M = \{m, n, o\},\ \ N_1 = \{a, b, \ldots, z\},\ \ N_2 = \{\{a, b, c\}, \{b, c, d\}, \ldots, \{x, y, z\}\}$$

Dann gilt:

$$\varnothing \neq M \subseteq N_1\,, \quad M \notin N_1\,, \quad M \nsubseteq N_2 \quad \text{und} \quad M \in N_2\,.$$

Aussagenlogik

Definition (Aussagen)

Aussagen sind Zeichenfolgen (Ausdrücke) bestehend aus (u. U. verzierten) lateinischen, griechischen, hebräischen, ... Buchstaben (Bezeichner) und Symbolen (,), {, }, usw., $\varnothing$, $\in$, $\subseteq$, $=$, $:$, $\neg$, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$, und xor.

Hierbei liest man „: “ als „*so dass*“ und

$\neg$ als *nicht* ... ,	xor als *entweder* ... , *oder* ... ,
$\vee$ als ... *oder* ... ,	$\wedge$ als ... *und* ... ,
$\Rightarrow$ als *wenn* ... , *dann* ... ,	$\Leftrightarrow$ als ... *genau dann, wenn* ... .

- Für je zwei Mengen A und B sind die Ausdrücke „$A \in B$“ und „$A \subseteq B$“ **primitive Aussagen**.
- Für zwei Aussagen p und q sind „$\neg p$“, „$p \operatorname{xor} q$“, „$p \vee q$“, „$p \wedge q$“, „$p \Rightarrow q$“ und „$p \Leftrightarrow q$“ **zusammengesetzte Aussagen**.

Bemerkung

- Etwas allgemeiner gefasst ist eine Aussage ein Satz, für den man im Prinzip eindeutig feststellen kann, ob er **wahr** oder **falsch** ist.

Verknüpfte Aussagen

Definition (Zusammengesetzte Aussagen)

Für Aussagen p und q nennt man

$\neg p$	die Negation von p	nicht p
$p \operatorname{xor} q$	die ausschließende Disjunktion von p und q	entweder p oder q
$p \vee q$	die Disjunktion von p und q	p oder q
$p \wedge q$	die Konjunktion von p und q	p und q
$p \Rightarrow q$	die Implikation von p nach q	wenn p, dann q
$p \Leftrightarrow q$	die Äquivalenz von p und q	p genau dann, wenn q

und diese Aussagen heißen zusammengesetzte Aussagen.

- xor heißt auch exklusives Oder bzw. ausschließendes Oder
- an Stelle von $\Rightarrow$ und $\Leftrightarrow$ benutzt man auch $\rightarrow$ und $\leftrightarrow$
- für $p \Rightarrow q$ sagt man auch p impliziert q bzw. q folgt aus p

Wahrheitsgehalt von Aussagen

- *Primitive Aussagen* der Form „$a \in A$“ (bzw. „$A \subseteq B$“) sind **wahr**, wenn a, A und B in der Beziehung $a \in B$ (bzw. $A \subseteq B$) stehen und ansonsten sind sie **falsch**.
- Für aus Aussagen p und q *zusammengesetzte Aussagen* gilt:

$$\neg p \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn } p \text{ falsch ist,} \\ \textbf{falsch} & \text{sonst, d. h. wenn } p \text{ wahr ist,} \end{cases}$$

$$p \operatorname{xor} q \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn genau eine der Aussagen } p \text{ oder } q \text{ wahr ist,} \\ \textbf{falsch} & \text{sonst, d. h. wenn beide Aussagen } p \text{ und } q \text{ wahr oder falsch sind,} \end{cases}$$

$$p \vee q \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn mindestens eine der Aussagen } p \text{ oder } q \text{ wahr ist,} \\ \textbf{falsch} & \text{sonst, d. h. wenn keine der Aussagen } p \text{ und } q \text{ wahr ist,} \end{cases}$$

$$p \wedge q \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn beide Aussagen } p \text{ und } q \text{ wahr sind,} \\ \textbf{falsch} & \text{sonst, d. h. wenn höchstens eine der Aussagen } p, q \text{ wahr ist,} \end{cases}$$

$$p \Rightarrow q \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn } q \text{ wahr ist oder wenn } p \text{ falsch ist,} \\ \textbf{falsch} & \text{sonst, d. h. wenn } p \text{ wahr und } q \text{ falsch ist,} \end{cases}$$

$$p \Leftrightarrow q \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn } p \text{ und } q \text{ beide wahr oder wenn beide falsch sind,} \\ \textbf{falsch} & \text{sonst, d. h. wenn } p \text{ und } q \text{ unterschiedliche W'werte haben.} \end{cases}$$

- **wahr** wird oft durch **w**, 1 und **falsch** durch **f**, 0 abgekürzt

Wahrheitstafeln

- Wahrheitswerte zusammengesetzter Aussagen lassen sich einfach über Wahrheitstafeln darstellen

p	q	$\neg p$	$\neg q$	$p \operatorname{xor} q$	$p \vee q$	$p \wedge q$	$p \Rightarrow q$	$p \Leftrightarrow q$
0	0	1	1	0	0	0	1	1
0	1	1	0	1	1	0	1	0
1	0	0	1	1	1	0	0	0
1	1	0	0	0	1	1	1	1

Mit Wahrheitstafeln kann man leicht folgende Aussagen beweisen:

Satz

Für Aussagen p, q und q' gilt

- $\neg(\neg p)$ ist äquivalent zu p (doppelte Negation)
- $\neg(p \operatorname{xor} q)$ ist äquivalent zu $p \Leftrightarrow q$
- $p \wedge (q \vee q')$ ist äquivalent zu $(p \wedge q) \vee (p \wedge q')$ (Distributivität)
- $p \Rightarrow q$ ist äquivalent zu $(\neg q) \Rightarrow (\neg p)$ (Kontraposition)

Distributivgesetz: $p \wedge (q \vee q') \Leftrightarrow (p \wedge q) \vee (p \wedge q')$

Beweis (mit Wahrheitstafeln)

p	q	q'	$q \vee q'$	$p \wedge (q \vee q')$	$p \wedge q$	$p \wedge q'$	$(p \wedge q) \vee (p \wedge q')$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

$\square$

Reductio ad absurdum

Widerspruchsbeweis bzw. indirekter Beweis

Mit Hilfe der Kontraposition kann eine Aussage p durch **Widerspruch** bewiesen werden. Dafür muss für eine bekannte falsche Aussage q die Implikation

$$(\neg p) \Rightarrow q$$

bewiesen werden, d. h. man beweist die Richtigkeit der Aussage

„wenn p falsch ist, dann ist q wahr.“

Da q aber falsch ist, kann p somit nicht falsch sein, also muss p wahr sein.

Bsp.: $p =$„$\sqrt{2}$ ist irrational“ und $q =$„es gibt teilerfremde a, b für die a/b kürzbar ist“

- q ist offensichtlich falsch
- Angenommen $\neg p$ ist wahr $\Rightarrow \sqrt{2} = a/b$ für teilerfremde natürliche Zahlen a, b

$\Rightarrow$ $2b^2 = a^2 \Rightarrow 2$ teilt a^2

$\Rightarrow$ da 2 eine Primzahl ist, teilt 2 somit auch a, d. h. $a = 2a_1$ für geeignetes a_1

$\Rightarrow$ $2b^2 = a^2 = 4a_1^2 \Rightarrow b^2 = 2a_1^2 \Rightarrow 2$ teilt $b^2 \Rightarrow 2$ teilt b, d. h. $b = 2b_1$

$\Rightarrow$ $a/b = (2a_1)/(2b_1) = a_1/b_1 \Rightarrow q$ ist wahr ↯

- Also muss $\neg p$ falsch sein und somit ist p wahr, d. h. $\sqrt{2}$ ist irrational $\square$

Aussageformen

Definition (Aussageform)

Eine Aussageform ist eine Aussage, in der eine Konstante durch eine freie Variable ersetzt wurde. So erhält man aus einer Aussage p eine Aussageform $p(x)$.

Beispiel

Sei $p(x)$ die Aussageform „x ist gerade“ und $q(x)$ die Form „x^2 ist durch 4 teilbar“.

- $p(x) \Rightarrow q(x)$ bedeutet „wenn x gerade ist, dann ist x^2 durch 4 teilbar“
  wahr für natürliche Zahlen x
- $q(x) \Rightarrow p(x)$ bedeutet „wenn x^2 durch 4 teilbar ist, dann ist x gerade“
  wahr für natürliche Zahlen x

Für natürliche Zahlen x gilt also

$p(x) \Leftrightarrow q(x)$, „$x$ is genau dann gerade, wenn x^2 durch 4 teilbar ist“

Quantoren: Allquantor $\forall$ und Existenzquantor $\exists$

Definition (Allaussagen und Existenzaussagen)

Sei $p(x)$ eine Aussageform und M eine Menge. Dann ist

- $(\forall x \in M)p(x)$ eine Aussage – Allaussage „für alle x in M gilt $p(x)$“
- $(\exists x \in M)p(x)$ eine Aussage – Existenzaussage „es gibt ein x in M, so dass $p(x)$ gilt“

Die freie Variable x in $p(x)$ heißt dann gebundene Variable in der All-/Existenzaussage.

In All-/Existenzaussagen kann durch Einführung neuer Variablen eine neue Aussageform gebildet werden, die durch weitere Quantoren wieder gebunden werden können.

Definition (Wahrheitswerte von All- und Existenzaussagen)

Für eine Aussageform $p(x)$ und eine Menge M gilt:

$$(\forall x \in M)p(x) \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn } p(x) \text{ für jedes } x \in M \text{ wahr ist} \\ \textbf{falsch} & \text{sonst, d. h. wenn es ein } x \in M \text{ gibt für das } p(x) \text{ falsch ist,} \end{cases}$$

$$(\exists x \in M)p(x) \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn es ein } x \in M \text{ gibt, so dass } p(x) \text{ wahr ist} \\ \textbf{falsch} & \text{sonst, d. h. } p(x) \text{ ist falsch für jedes } x \in M. \end{cases}$$

$$\neg\big((\forall x \in M)p(x)\big) \Leftrightarrow \big((\exists x \in M)\neg p(x)\big)\,, \quad \neg\big((\exists x \in M)p(x)\big) \Leftrightarrow \big((\forall x \in M)\neg p(x)\big)$$

Mengenoperationen

Definition

Seien A und B Mengen, dann ist

- $A \cup B := \{x\colon x \in A \vee x \in B\}$ die Vereinigung von A und B,
- $A \cap B := \{x\colon x \in A \wedge x \in B\}$ der Schnitt von A und B,
- $A \setminus B := \{x\colon x \in A \wedge x \notin B\}$ die Differenz A ohne B,
- $\wp(A) := \{x\colon x \subseteq A\}$ die Potenzmenge von A.

Für eine feste Grundmenge M mit $A \subseteq M$, ist

$$\overline{A} := M \setminus A = \{x \in M\colon x \notin A\}$$

das Komplement von A in M.

- mengentheoretische $\cup$ (bzw. $\cap$) „entspricht" logischem $\vee$ (bzw. $\wedge$)
- Potenzmenge wird auch mit $\mathcal{P}(A)$, 2^A, $\mathbb{P}(A)$, $\mathrm{pow}(A)$ bezeichnet
- $\wp(\varnothing) = \{\varnothing\} \neq \varnothing$ und $\wp\big(\wp(\varnothing)\big) = \big\{\varnothing, \{\varnothing\}\big\}$
- $\varnothing \in \wp(A)$ für jede Menge A, da $\varnothing \subseteq A$ für jede Menge A
- $\overline{(\overline{A})} = \overline{\overline{A}} = \overline{M \setminus A} = M \setminus (M \setminus A) = A$ für jede Menge $A \subseteq M$

Distributivitätsgesetz für Mengen

Satz

Für beliebige Mengen A, B, $C \subseteq M$ gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Beweis (mit Wahrheitstafeln)
Aus den Definitionen der Vereinigung und des Schnittes folgt

$$A \cap (B \cup C) = \{x \in M \colon x \in A \wedge (x \in B \vee x \in C)\}\,.$$

Für ein beliebiges $x \in M$ seien a_x, b_x und c_x die (primitiven) Aussagen $x \in A$, $x \in B$ und $x \in C$. Somit gilt

$$x \in A \cap (B \cup C) \iff a_x \wedge (b_x \vee c_x) \text{ ist wahr.}$$

Wegen dem Distributivgesetz des logischen „und" und „oder" (bewiesen durch Wahrheitstafeln) gilt

$$a_x \wedge (b_x \vee c_x) \iff (a_x \wedge b_x) \vee (a_x \wedge c_x)\,,$$

und somit gilt

$$\begin{aligned} x \in A \cap (B \cup C) &\iff (a_x \wedge b_x) \vee (a_x \wedge c_x) \text{ ist wahr} \\ &\iff (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \text{ ist wahr} \end{aligned}$$

und die Aussage des Satzes folgt, da $x \in M$ beliebig war. $\square$

Satz

Für beliebige Mengen A, B, $C \subseteq M$ gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Beweis

Wir beweisen beide Teilmengenbeziehungen

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \quad \text{und} \quad A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$$

einzeln, wodurch sich die Gleichheit ergibt.

„$\subseteq$“ Sei $x \in A \cap (B \cup C)$ beliebig. Das bedeutet $x \in A$ und

$$x \in B \cup C\,. \tag{$*$}$$

Falls $x \in B$, dann gilt auch $x \in A \cap B$ und somit auch $x \in (A \cap B) \cup (A \cap C)$.

Falls $x \notin B$, dann gilt $x \in C$ wegen $(*)$ und somit auch $x \in A \cap C$ und wieder folgt $x \in (A \cap B) \cup (A \cap C)$.

In jedem Fall gilt also $x \in (A \cap B) \cup (A \cap C)$ und da x beliebig aus $x \in A \cap (B \cup C)$ gewählt war folgt die gesuchte Inklusion

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)\,.$$

Satz

Für beliebige Mengen A, B, $C \subseteq M$ gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Beweis

Wir beweisen beide Teilmengenbeziehungen

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \quad \text{und} \quad A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$$

einzeln, wodurch sich die Gleichheit ergibt.

„$\supseteq$“ Sei nun $x \in (A \cap B) \cup (A \cap C)$ beliebig.

$\Rightarrow$ $x \in A \cap B$ oder $x \in A \cap C$

- Falls $x \in A \cap B$
  $\Rightarrow x \in A$ und $x \in B$
  $\Rightarrow x \in A$ und $x \in B \cup C$
  $\Rightarrow x \in A \cap (B \cup C)$.
- Der Fall $x \in A \cap C$ ist analog mit B und C vertauscht.

Somit gilt $x \in A \cap (B \cup C)$ und da x beliebig gewählt war, folgt auch die Inklusion $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

Beide Inklusionen zusammen ziehen die Gleichheit der Mengen nach sich. $\square$

De Morgansche Regeln

Satz (De Morgan)

Für beliebige Mengen $A, B \subseteq M$ gilt

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \qquad \text{und} \qquad \overline{A \cup B} = \overline{A} \cap \overline{B}\,.$$

Beweis

- Sei $x \in \overline{A \cap B}$.
  $\Rightarrow\ x \notin (A \cap B) \Rightarrow x \notin A$ oder $x \notin B \Rightarrow x \in \overline{A}$ oder $x \in \overline{B} \Rightarrow x \in \overline{A} \cup \overline{B}$.

Somit gilt $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$.

- Sei umgekehrt $x \in \overline{A} \cup \overline{B}$.
  $\Rightarrow\ x \in \overline{A}$ oder $x \in \overline{B} \Rightarrow x \notin A$ oder $x \notin B \Rightarrow x \notin (A \cap B) \Rightarrow x \in \overline{A \cap B}$.

Somit gilt auch $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$ und die erste Gleichheit folgt.

- Für die zweite Identität folgern wir zuerst aus der ersten Regel (angewandt auf $\overline{A}$ und $\overline{B}$)

$$\overline{\overline{A} \cap \overline{B}} = \overline{\overline{A}} \cup \overline{\overline{B}} = A \cup B$$

und Komplementbildung auf beiden Seiten ergibt $\overline{A} \cap \overline{B} = \overline{A \cup B}$. □

BOOLEsche Algebren

DE MORGAN für Mengen: $\overline{A \cap B} = \overline{A} \cup \overline{B}$ und $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Satz (DE MORGAN für Aussagen)

Für Aussagen p und q gilt: $\neg(p \wedge q) = \neg p \vee \neg q$ und $\neg(p \vee q) = \neg p \wedge \neg q$.

Beweis: Wahrheitstafeln (Übung/Selbststudium) $\square$

Bemerkungen

- Distributivgesetze, DE MORGAN-Regel gibt es jeweils für Mengen und Aussagen
- enger Zusammenhang zwischen Mengen und Aussagen

	Komplement	Vereinigung	Schnitt
Mengen	$\overline{A}$	$A \cup B$	$A \cap B$
Aussagen	$\neg p$	$p \vee q$	$p \wedge q$
	Negation	Disjunktion	Konjunktion

  wobei Komplementbildung (bzw. Negation) $\cup/\cap$ (bzw. $\vee/\wedge$) vertauscht.
- Abstraktion führt zum Begriff der BOOLEschen Algebra, z. B.
  - die Schaltkreisalgebra $(\{0, 1\}, \vee, \wedge, \neg, 0, 1)$ auf den Wahrheitswerten 0 und 1 mit den logischen Verknüpfungen,
  - die Potenzmengenalgebra $(\wp(M), \cup, \cap, \overline{}, \varnothing, M)$ in $\wp(M)$ für eine $M \neq \varnothing$ mit den mengentheoretischen Verknüpfungen.
- in diesem Kontext entspricht die DE MORGANsche Regel dem Dualitätspinzip

Kartesisches Produkt

Definition

Für Mengen A und B ist das kartesische Produkt/Kreuzprodukt definiert durch

$$A \times B := \{(a, b) \colon a \in A \text{ und } b \in B\}$$

als die Menge aller **geordneten** Paare mit dem ersten Element aus A und dem zweiten B.
Allgemeiner für definieren wir für Mengen $A_1, \dots, A_n$ die Menge

$$A_1 \times \dots \times A_n := \{(a_1, \dots, a_n) \colon a_1 \in A_1, \dots, a_n \in A_n\}$$

die Menge aller entsprechenden **geordneten** n-Tupel.

- falls $A_1 = \dots = A_n = A$ gilt, dann schreiben wir A^n für $A_1 \times \dots \times A_n$
- falls $A_i = \varnothing$ für ein i, dann ist $A_1 \times \dots \times A_n = \varnothing$
- für $n = 0$ ist $A^0 = \{(\,)\}$ die Menge bestehend aus dem leeren Tupel $(\,)$

Abbildungen/Funktionen

Definition

Eine Abbildung/Funktion f von einer Menge A in eine Menge B ist eine **Zuordnung**, die jedem Element von A ein Element von B zuordnet und wir schreiben abkürzend

$$f\colon A \to B$$

und sagen f ist eine Abbildung/Funktion von A nach B.

Die Menge A heißt Definitionsbereich und B ist der Wertevorrat von f.

Für jedes $a \in A$ bezeichnen wir mit $b = f(a)$ das Element $b \in B$, das die Funktion f dem Element a zuordnet und wir sagen f bildet a auf b ab und schreiben

$$a \mapsto b\,,$$

wenn klar ist, welche Funktion f gemeint ist.

Die Teilmenge $\{f(a)\colon a \in A\}$ des Wertevorrats heißt Bild von f.

Eigenschaften von Funktionen

Definition

Eine Funktion $f: A \to B$ heißt

- injektiv, falls für alle $a, a' \in A$ gilt $f(a) = f(a') \Rightarrow a = a'$.
- surjektiv, falls für alle $b \in B$ ein $a \in A$ existiert, so dass $f(a) = b$ gilt.
- bijektiv, falls sie sowohl **injektiv**, als auch **surjektiv** ist.

Beispiele

- $f_1: \mathbb{N} \to \mathbb{N}$ mit $x \mapsto x^2$ ist injektiv, aber nicht surjektiv
- $f_2: \mathbb{Z} \to \mathbb{Z}$ mit $x \mapsto x^2$ ist weder injektiv, noch surjektiv
- $f_3: \mathbb{R} \to \mathbb{R}$ mit $x \mapsto x^3 + x^2$ ist nicht injektiv, aber surjektiv
- $f_4: \mathbb{R} \to \mathbb{R}$ mit $x \mapsto x^3$ ist bijektiv
- $g: \mathbb{R} \to \mathbb{R}$ mit $x \mapsto \exp(x)$ ist injektiv, aber nicht surjektiv mit dem Bild $\{r \in \mathbb{R}: r > 0\}$
- konstante Funktionen $h \equiv z$, $h: M \to M$ mit $x \mapsto z$ für festes $z \in M$ sind im Allgemeinen weder injektiv, noch surjektiv
- Identität auf M $\mathrm{id}_M: M \to M$ mit $x \mapsto x$ ist bijektiv

Operationen

Definition

Eine *n-stellige Operation*/(innere) *n-stellige Verknüpfung* auf einer Menge M ist eine Abbildung $f\colon M^n \to M$.

Beispiele

- jede 0-stellige Operation auf einer Menge M ordnet dem leeren Tupel $(\,)$ ein Element in M zu und kann als **konstante Funktion** bzw. einfach als Darstellung einer Konstante angesehen werden
- Negation $(\neg)$ ist eine 1-stellige (unäre) Operation auf den Aussagen
- Komplement $(\overline{})$ ist eine 1-stellige Operation auf $\wp(M)$ für jedes M
- die logischen (xor, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$) und mengentheoretischen ($\cup$, $\cap$, $\smallsetminus$) Verknüpfungen sind 2-stellige (binäre) Operationen
- oft schreiben wir bei binären Operationen den Operand zwischen die beiden Argument, z. B. $A \cap B$ an Stelle von $\cap(A, B)$
- Grundrechenarten Addition $(+)$ und Multiplikation $(\cdot)$ sind binäre Operationen

Summen- und Produktzeichen

Definition ($\sum$ und $\prod$)

Für Zahlen $x_1, \dots, x_n$ sei

$$\sum_{i=1}^{n} x_i := x_1 + x_2 + \cdots + x_n \quad \text{und} \quad \prod_{i=1}^{n} x_i := x_1 \cdot x_2 \cdot \ldots \cdot x_n\,.$$

Dabei heißt i der Laufindex, 1 ist die untere Summations-/Produktgrenze und n ist die obere Summations-/Produktgrenze.

Für $n = 0$ definieren wir die leere Summe $\sum_{i=1}^{0} x_i$ als 0 und das leere Produkt $\prod_{i=1}^{0} x_i$ als 1.

- Laufindex muss nicht mit i bezeichnet werden und mit 1 beginnen

$$\sum_{k=-2}^{3} 2^{k+1} = 2^{-1} + 2^0 + 2^1 + 2^2 + 2^3 + 2^4 = 31{,}5 = \sum_{i=1}^{6} 2^{i-2}$$

- Potenzen von -1 ermöglichen alternierende Summen/Produkte mit wechselndem Vorzeichen

$$\sum_{i=0}^{3} (-1)^i 3^i = 1-3+9-27 = -20 \quad \text{und} \quad \sum_{i=0}^{3} (-1)^{i+1} 3^i = -1+3-9+27 = 20$$

Rechenregeln

- für $x_1 = \dots = x_n = x$ erhalten wir

$$\sum_{i=1}^{n} x = n \cdot x \quad \text{und} \quad \prod_{i=1}^{n} x = x^n$$

- Linearität der Summe: folgt aus dem Distributivgesetz

$$a \sum_{i=1}^{n} x_i = a \cdot (x_1 + \dots + x_n) = ax_1 + \dots + ax_n = \sum_{i=1}^{n} ax_i$$

und aus der Assoziativität und Kommutativität der Addition

$$\sum_{i=1}^{n} (x_i + y_i) = (x_1 + y_1) + \dots + (x_n + y_n)$$

$$= (x_1 + \dots + x_n) + (y_1 + \dots + y_n) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$$

- Ausmultiplizieren ergibt

$$\begin{aligned}\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{m} y_j\right) &= (x_1 + \cdots + x_n)\cdot(y_1 + \cdots + y_m)\\ &= x_1y_1 + x_1y_2 + \cdots + x_1y_m\\ &\qquad + x_2y_1 + \cdots + x_2y_m\\ &\qquad + \cdots +\\ &\qquad + x_ny_1 + \cdots + x_ny_m\\ &= \sum_{i=1}^{n}\sum_{j=1}^{m} x_iy_j\end{aligned}$$

- Kommutivität erlaubt dann die Vertauschung

$$\sum_{i=1}^{n}\sum_{j=1}^{m} x_iy_j = \sum_{j=1}^{m}\sum_{i=1}^{n} x_iy_j$$

2. Natürliche Zahlen und vollständige Induktion

Natürliche Zahlen

Definition

Mit $\mathbb{N}$ bezeichnen wir die Menge der natürlichen Zahlen

$$\mathbb{N} := \{1, 2, 3, \dots\}$$

und mit $\mathbb{N}_0$ die natürlichen Zahlen einschließlich der Null

$$\mathbb{N}_0 := \{0\} \cup \mathbb{N} = \{0, 1, 2, 3, \dots\}.$$

- oftmals wird auch die Null als natürliche Zahl angesehen
- die Existenz der natürlichen Zahlen (so wie wir sie kennen) kann aus den Zermelo-Fraenkel-Axiomen abgeleitet werden (Unendlichkeitsaxiom)
- in dieser VL werden wir $\mathbb{N}$ mit der Addition $(+)$ und Multiplikation $(\cdot)$ und den geltenden Rechenregeln erstmal als gegeben annehmen

Rechengesetze für natürliche Zahlen

Für alle Zahlen a, b, $c \in \mathbb{N}_0$ gelten:

- Assoziativgesetze:

$$a + (b + c) = (a + b) + c \qquad \text{und} \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

- Kommutativgesetze:

$$a + b = b + a \qquad \text{und} \qquad a \cdot b = b \cdot a$$

- Distributivgesetz:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

- Existenz der neutralen Elemente:

$$a + 0 = a \qquad \text{und} \qquad a \cdot 1 = a$$