Grundlagen Theoretischer Informatik I

SoSe 2011 in Trier

Henning Fernau
Universität Trier
fernau@uni-trier.de

Grundlagen Theoretischer Informatik I Gesamtübersicht

- Organisatorisches; Einführung
- Logik & Beweisverfahren
- Mengenlehre
- reguläre Sprachen

Nochmal: Organisatorische Hinweise

Abgabe in Gruppen zu 2-3 Leuten ist ausdrücklich erwünscht.
Das sollte die Mitarbeit untereinander fördern.
Es ist also im Allgemeinen nicht nötig (bei uns), dass dieselben Lösungen zweimal abgeschrieben werden.
Nur so schaffen wir es auch, die Aufgaben in zwei Tagen durchzukorrigieren.

Tutorensprechstunde montags wird bislang nicht angenommen. Gründe?

B.Ed.-Studierende erfahren “andere Behandlung”.
Daher sinnvoll (?): Aussetzen der Montags-Übungsgruppe für die nächsten drei Wochen?!

Begriffserklärung 

Auf Georg Cantor geht folgende Definition über Mengen (Mannigfaltigkeiten) zurück:

Eine *Menge* ist eine Zusammenfassung bestimmter, wohlunterschiedlicher Dinge unserer Anschauung oder unseres Denkens, welche *Elemente* der Menge genannt werden, zu einem Ganzen.

Kultureller Exkurs: Die Oper "Cantor — Die Vermessung des Unendlichen" von Ingomar Grünauer widmet sich dem Leben und Werk Georg Cantors; Uraufführung aus Anlass des 1200-jährigen Stadtjubiläums am 10. November 2006 im Opernhaus Halle.

Beispiel: $\emptyset$: die *leere Menge*

Schulkasse (als Menge von Schülerinnen und Schülern)

$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$: die Menge der natürlichen Zahlen

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots\}$: die Menge der ganzen Zahlen

$\mathbb{Q}$: die Menge der rationalen Zahlen

$\mathbb{R}$: die Menge der reellen Zahlen

Warnung vor naivem Zugang: “Menge aller Mengen”

Elementrelation und Angabe von Mengen

Um auszudrücken, dass x ein Element der Menge M ist, schreiben wir: $x \in M$.
Anstelle von $\neg(x \in M)$ schreibt man kürzer: $x \notin M$.

Endliche Mengen kann man durch vollzählige Aufzählung ihrer Elemente beschreiben, z.B. eine Schulklasse durch Auflistung der Schüler.
$M = \{\text{Martin, Michael, Carla}, \ldots\}$

Allgemein kann man (unter Zugrundelegung eines bekannten Universums) Mengen auch durch Eigenschaften (Aussageformen) beschreiben:
$x \in M \iff P(x)$ notiert man oft auch: $M = \{x \mid P(x)\}$ oder $M = \{x : P(x)\}$.
Das Universum kann bei dieser Schreibweise mit angegeben werden, z.B.:
$\{x \in \mathbb{R} \mid x^2 - 2x = -1\}$.
Die *leere Menge* können wir (unabhängig vom Universum) beschreiben durch:
$\emptyset = \{x \mid x \neq x\}$ (oder irgendein anderes Falsum als Eigenschaft)

Mengengleichheit

Zwei Mengen M_1 und M_2 sind *gleich*, i.Z.: $M_1 = M_2$, gdw.
$x \in M_1 \iff x \in M_2$.
Anstelle von $\neg(M_1 = M_2)$ schreiben wir auch $M_1 \neq M_2$.
Achtung: $\{1, 2, 2, 1\} = \{1, 2\} = \{2, 1\}$,
mehrfache Nennung oder Reihenfolge sind also unerheblich.

Wie beweist man Mengengleichheit ?
(Zumeist) unter Verwendung der Tautologie $p \iff q \equiv (p \Rightarrow q) \land (q \Rightarrow p)$.
$\rightsquigarrow$ Beweis in zwei Schritten (Richtungen)

Beispiel: “Die leere Menge” hängt nur scheinbar vom Universum ab.
Beweis: Betrachte $\emptyset_U$ und $\emptyset_V$. Wähle $a \in U$ beliebig. Dann gilt $a \notin \emptyset_U$. Also ist $(x \in \emptyset_U \implies x \in \emptyset_V)$ wahr. Die Rückrichtung sieht man entsprechend; vertausche U und V.

Mengenkomplement

Es sei M eine Menge über dem Universum U (das auch als Menge angesehen wird). Das *Komplement* von M, i.Z. $\overline{M}$, ist die Menge $\overline{M} = \{x \mid x \notin M\}$.
Beispiel: $\overline{U} = \emptyset$, $\overline{\emptyset} = U$.
Doppeltes Komplement (ähnlich doppelter Verneinung):
$\overline{\overline{M}} = \{x \mid x \notin \overline{M}\} = \{x \mid \neg(\neg x \in M)\} = \{x \mid x \in M\} = M$.

Sei $M = \{x \mid P(x)\}$.
Mit $P(x)$ ist auch $\neg P(x)$ Aussageform.
Damit gilt: $\overline{M} = \{x \mid \neg P(x)\}$.

M und $\overline{M}$ heißen auch *komplementär* zueinander.
Beispiel: Für $U = \mathbb{Z}$ "sind" die ungeraden Zahlen das Komplement von $\{x : 2|x\}$.

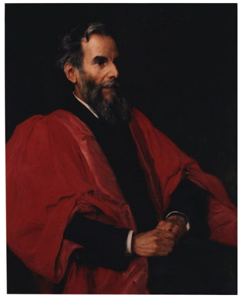
Teilmengen und Obermengen

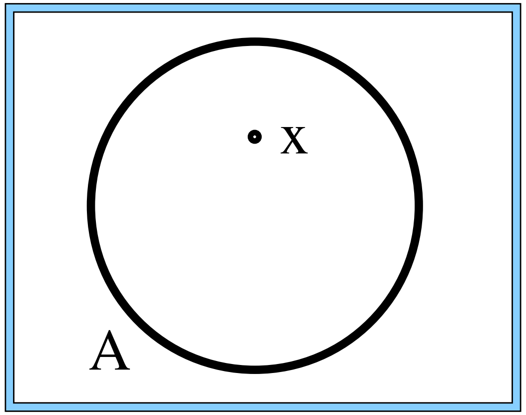
N heißt *Teilmenge* von M ($N \subseteq M$) gdw. M heißt *Obermenge* von N ($M \supseteq N$) gdw. $\forall x(x \in N \Rightarrow x \in M)$.
Gilt überdies $N \neq M$, so sprechen wir von einer *echten Teilmenge* bzw. einer *echten Obermenge* und notieren $N \subset M$ bzw. $M \supset N$.

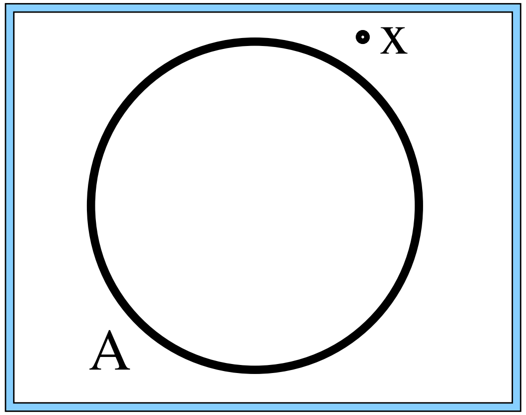
Beispiel: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

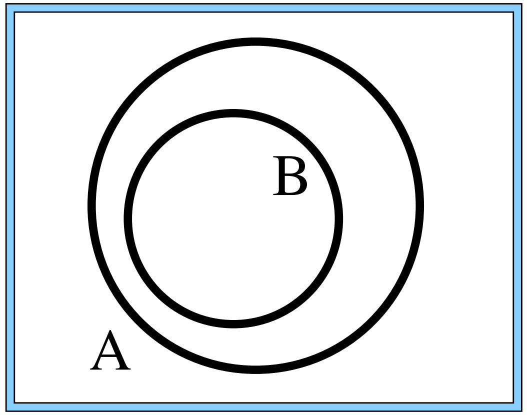
Satz: $N = M$ gdw. $(N \subseteq M) \wedge (M \subseteq N)$.

Beweis: (*elementweise Argumentation*) $N = M$ gdw. $\forall x(x \in N \iff x \in M)$ gdw.
$\forall x((x \in N \implies x \in M) \wedge (x \in M \implies x \in N))$ gdw.
$\forall x(x \in N \implies x \in M) \wedge \forall x(x \in M \implies x \in N)$ gdw.
$(N \subseteq M) \wedge (M \subseteq N)$.

Venn-Diagramme 







Problem: Uneinheitliche Beschriftung

Potenzmengen

Zu jeder Menge M gibt es eine weitere Menge, die *Potenzmenge* von M, geschrieben 2^M (oder auch $\mathcal{P}(M)$), die genau die Teilmengen von M als Elemente enthält.

Lemma: Die Potenzmenge 2^M enthält in Sonderheit die Elemente $\emptyset$ und M.

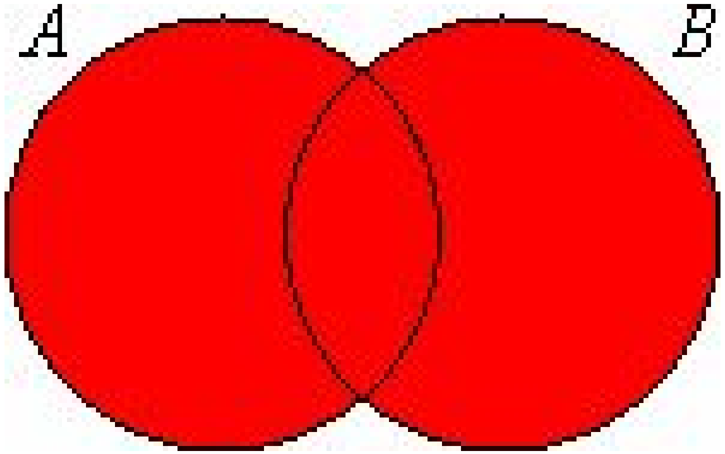
Beweis: Es bleibt zu zeigen: $\emptyset \in 2^M$, also: $\emptyset \subseteq M$.

Die Implikation $(x \in \emptyset \implies x \in M)$ ist stets wahr, da die Prämisse falsch ist.

Beispiel: $2^{\{1,2,3\}} = \{\, \{1,2,3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1\}, \{2\}, \{3\}, \emptyset \,\}$.

Mengenalgebra: Vereinigung

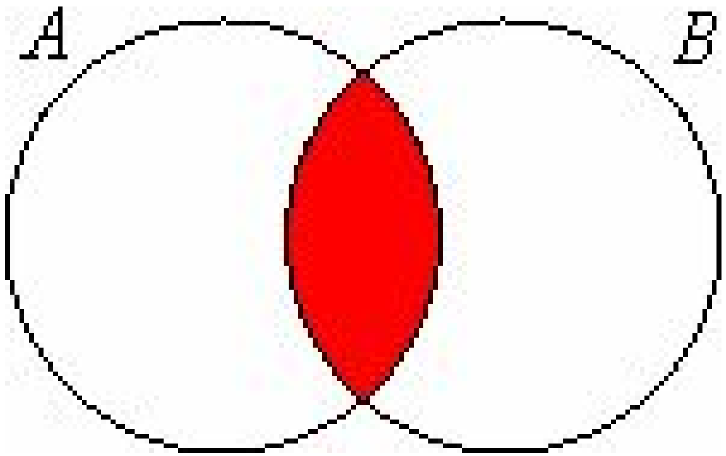
Es seien A, B Mengen (mit Elementen desselben Universums). Die Gesamtheit der Elemente, die zu A oder auch zu B gehören, wird als *Vereinigung* von A und B bezeichnet; Schreibweise: $A \cup B$

Venn-Diagramm: 

Es gilt: $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$.

Mengenalgebra: Durchschnitt

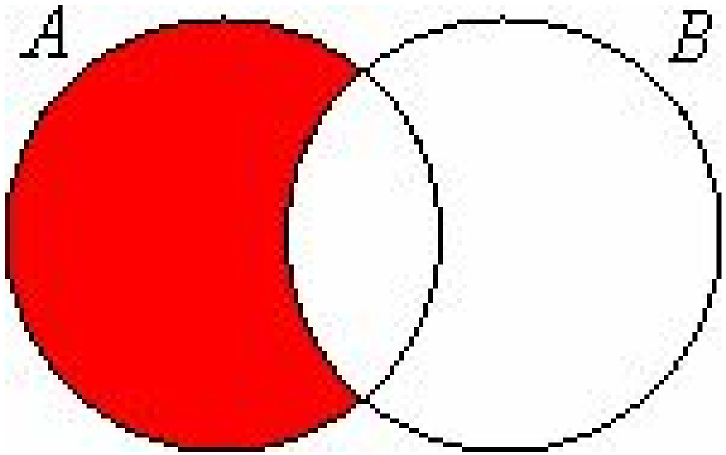
Es seien A, B Mengen (mit Elementen desselben Universums). Die Gesamtheit der Elemente, die sowohl zu A als auch zu B gehören, wird als *Durchschnitt* von A und B bezeichnet; Schreibweise: $A \cap B$

Venn-Diagramm: 

Es gilt: $A \cap B = \{x \mid (x \in A) \land (x \in B)\}$.
A und B heißen *disjunkt* oder *fremd* gdw. $A \cap B = \emptyset$.

Mengenalgebra: Differenz

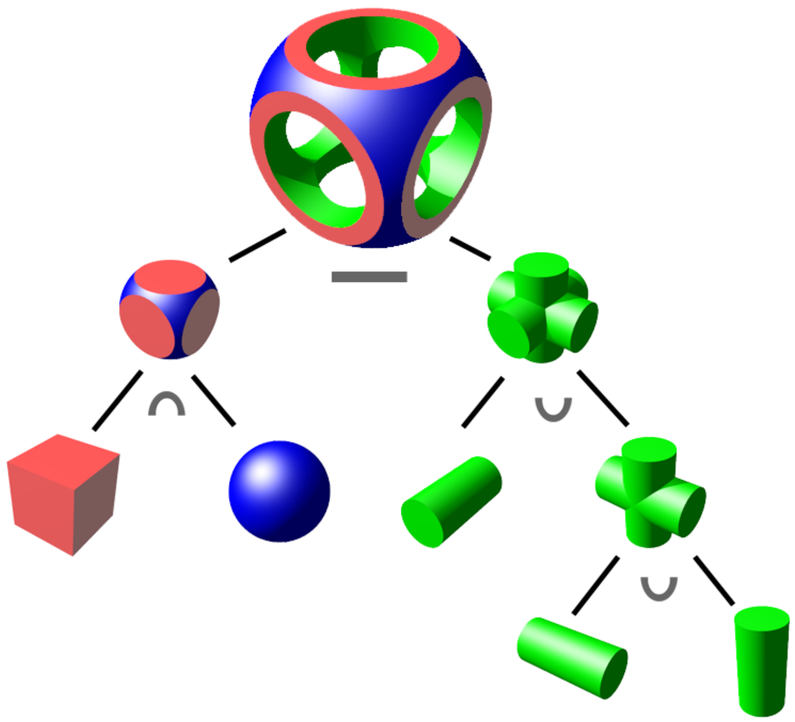
Es seien A, B Mengen (mit Elementen desselben Universums). Die Gesamtheit der Elemente, die zwar zu A aber nicht zu B gehören, wird als *Differenz* von A und B bezeichnet; Schreibweise: $A \setminus B$, $A - B$

Venn-Diagramm: 

Es gilt: $A \setminus B = \{x \mid (x \in A) \wedge \neg(x \in B)\} = \{x \mid (x \in A) \wedge (x \notin B)\}$.

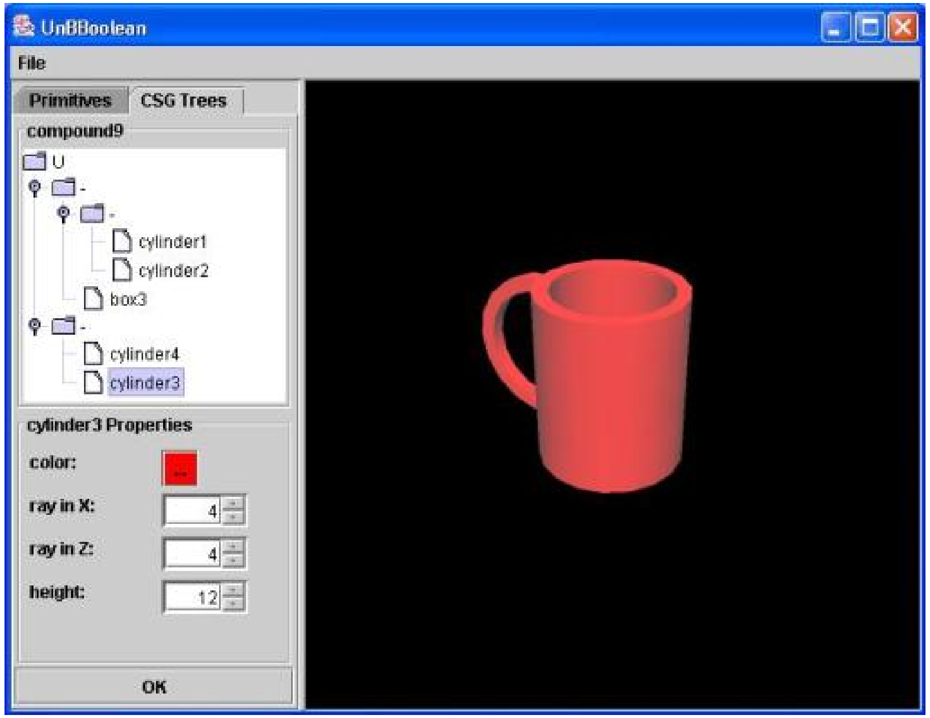
CSG: Constructive Solid Geometry:

Eine Beschreibungssprache für komplexe Oberflächen, im Wesentlichen beruhend auf einfachen Punktmengenoperationen



CSG: Constructive Solid Geometry:

Es gab jedenfalls auch einmal ein sourceforge-Projekt “unbboolean” für JAVA



Mengenalgebra: Aussagen

Satz: $A \cap B \subseteq A \subseteq A \cup B$; $A \cap B \subseteq B \subseteq A \cup B$.

Satz: $A \cup A = A \cap A = A$.

Satz: $A \cup B = B \cup A$; $A \cap B = B \cap A$.

Satz: $(A \cup B) \cup C = A \cup (B \cup C)$; $(A \cap B) \cap C = A \cap (B \cap C)$.

Satz: $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$; $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

Satz: $\overline{A \cup B} = \overline{A} \cap \overline{B}$; $\overline{A \cap B} = \overline{A} \cup \overline{B}$;

Satz: $(A \cup B = B) \iff A \subseteq B \iff (A \cap B = A)$.

Satz: $(A \subseteq B) \implies ((A \cup C \subseteq B \cup C) \wedge (A \cap C) \subseteq (B \cap C))$.

Mengenalgebra: Aussagen

Beweis elementweise für ein Distributivgesetz als Beispiel:

Satz: $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$; ($(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$).

Beweis: Sei $x \in (A \cup B) \cap C$. $\rightsquigarrow$ (1) $x \in (A \cup B)$ und (2) $x \in C$.
Wir unterscheiden wegen (1) zwei Fälle, von denen einer zutreffen muss:
1. Fall: $x \in A$: Mit (2) gilt $x \in A \cap C$.
2. Fall: $x \in B$: Mit (2) gilt $x \in B \cap C$.
Da 1. oder 2. zutrifft, gilt: $x \in (A \cap C) \cup (B \cap C)$.

Betrachte umgekehrt $x \in (A \cap C) \cup (B \cap C)$. $\rightsquigarrow$ (1) $x \in A \cap C$ oder (2) $x \in B \cap C$.

Sowohl aus (1) wie aus (2) folgt: $x \in C$.

Zudem gilt: Wegen (1) liegt x in A oder wegen (2) liegt x in B.

Zusammen folgt: $(x \in C) \wedge (x \in A \vee x \in B)$, also $(x \in C) \wedge (x \in (A \cup B))$, d.h. $x \in (A \cup B) \cap C$.

Mengen aus Mengen I **Potenzmengen**

Zu jeder Menge M gibt es eine weitere Menge, die *Potenzmenge* von M, geschrieben 2^M (oder auch $\mathcal{P}(M)$), die genau die Teilmengen von M als Elemente enthält.

Lemma: Die Potenzmenge 2^M enthält in Sonderheit die Elemente $\emptyset$ und M.

Beweis: Es bleibt zu zeigen: $\emptyset \in 2^M$, also: $\emptyset \subseteq M$.

Die Implikation $(x \in \emptyset \implies x \in M)$ ist stets wahr, da die Prämisse falsch ist.

Beispiel: $2^{\{1,2,3\}} = \{ \{1,2,3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1\}, \{2\}, \{3\}, \emptyset \}$.

Hasse-Diagramme 

(für endliche Potenzmengen)

Stellt Mengen als Punkte dar.

Mengen mit gleichviel Elementen erscheinen auf einer Ebene.

Oben erscheinen die größeren, unten die kleineren Mengen.

Durch einen (geraden) Strich werden solche Mengen A und B verbunden, für die $A \subset B$ gilt, sich aber kein C findet mit $A \subset C \subset B$.

Mengen aus Mengen II **Produktmenge**: Ziel und Problem

Ziel: Die *Produktmenge* der Mengen M und N soll aus den *geordneten Paaren* (x, y) von Elementen $x \in M$ und $y \in N$ bestehen.

Frage: Brauchen wir grundsätzlich neue Begriffe, oder können wir diesen Begriff "ableiten" ?

Hinweis: geordnetes Paar $\neq$ Zweiermenge, denn die Reihenfolge ist bei Zweiermengen unerheblich.

Für geordnete Paare soll gelten: $(a, b) = (c, d) \iff (a = c \wedge b = d)$.

Für Zweitermengen gilt: $\{a, b\} = \{c, d\} \iff ((a = c \wedge b = d) \vee (a = d \wedge b = c))$.

Produktmenge: Lösung des Problems

Satz: Die Mengen $M_1 = \{\{a\}, \{a, b\}\}$ und $M_2 = \{\{c\}, \{c, d\}\}$ sind gleich gdw. $a = c$ und $b = d$.

Beweis: $\Rightarrow$: Nach Def. der Mengengleichheit folgt $(*)$ $\{a\} = \{c\}$ und $\{a, b\} = \{c, d\}$, oder aber $(**)$ $\{a\} = \{c, d\}$ und $\{c\} = \{a, b\}$.
Gilt $(*)$, so folgt zunächst $a = c$ und dann damit $b = d$.
Gilt $(**)$, so ist $a = c = d$ sowie $c = a = b$ und somit $a = b = c = d$.

$\Leftarrow$: Mit $a = c$ und $b = d$ gilt: $\{a\} = \{c\}$ und $\{b\} = \{d\}$ und mithin $\{a, b\} = \{c, d\}$.

Wir können also $(a, b) := \{a, \{a, b\}\}$ definieren.

Produktmenge: Weitere Festlegungen

geordnetes n-Tupel (rekursiv für $n > 2$): $(a_1, \ldots, a_{n-1}, a_n) := ((a_1, \ldots, a_{n-1}), a_n)$.

Beispiel: Geometrie: Punkte der Ebene $\sim$ geordnete Paare;
Punkte des dreidimensionalen Raumes $\sim$ geordnete Tripel, also 3-Tupel

Allgemein definiere das *Mengenprodukt* von Mengen M und N durch:

$$M \times N := \{(x, y) \mid x \in M \wedge y \in N\}$$

Noch allgemeiner:

$$M_1 \times \cdots \times M_n := \{(x_1, \ldots, x_n) \mid x_1 \in M_1 \wedge \cdots \wedge x_n \in M_n\}$$

oder rekursiv:

$$M_1 \times \cdots \times M_n = (M_1 \times \cdots \times M_{n-1}) \times M_n$$

Mengenalgebra mit Produktmengen

Satz: $M \times \emptyset = \emptyset \times M = \emptyset$.

Satz: Für beliebige Mengen M, N, P gilt: $M \times (N \cup P) = (M \times N) \cup (M \times P)$.

Satz: Für beliebige Mengen M, N, P gilt: $M \times (N \cap P) = (M \times N) \cap (M \times P)$.

(Distributivgesetze wieder wegen elementweiser Distributivität)

Relationen

Erinnerung: Mengenprodukt

Es seien $M_1, \dots, M_n$ Mengen.
R heißt *n-stellige Relation zwischen* $M_1, \dots, M_n$ gdw.

$$R \subseteq M_1 \times \cdots \times M_n.$$

M_i heißen auch *Grundmengen* von R.

Gilt $M = M_i$ für $i \in \{1, \dots, n\}$, so heißt R eine *n-stellige Relation über* M.
Schreibweise: $R(x_1, \dots, x_n)$ statt $(x_1, \dots, x_n) \in R$
Spezialfall $n = 2$: *binäre Relation* Schreibweise: $x_1 R x_2$ statt $R(x_1, x_2)$ (*Infixnotation*)

Relationen und Prädikate: “$(x_1, \dots, x_n) \in R$” ist Aussageform mit Variablen $x_1, \dots, x_n$
Umgekehrt definieren Aussageformen Relationen.

Relationen: Beispiele

$M_1 = M_2 = M_3 = \mathbb{R}$: *Zwischenrelation* R:

$$R = \{(a, b, c) \in \mathbb{R} \mid (a \leq b) \wedge (b \leq c)\}.$$

$M_1 = M_2 = \{g \mid g$ ist Gerade in der Ebene $\}$. *Parallelitätsrelation* $\|$:

$$g \| h \iff g \text{ und } h \text{ liegen parallel.}$$

$M_1 = M_2 = \mathbb{Z}$: *Teilbarkeitsrelation* $\mid$

$$a \mid b \iff \exists k : b = a \cdot k.$$

$M_1 = M_2 = \mathbb{R}$: *Kleinerrelation* $<$.
$M_1 = M_2 = \mathbb{Z}$; *Paritätsrelation* P: $(x, y) \in P \iff 2 \mid (x + y)$.

Spezielle Relationen: Betrachte Relationen über Menge M.

Nullrelation: $R = \emptyset$.
Allrelation: $R = M \times M$ (evtl. auch für andere Stelligkeiten)
Gleichheitsrelation, auch *Diagonale* oder *Identitätsrelation*:
$\Delta_M = \{(x, x) \mid x \in M\}$.

Hinweis: Nullrelation und Allrelation auch für Relationen zwischen Mengen gebräuchlich.

Operationen auf Relationen: Mengenoperationen

Sind R und S Relationen zwischen denselben Grundmengen, so sind
$R \subseteq S$, d.h., R ist *Teilrelation* von S,
$\overline{R}$ *Komplementrelation*,
$R \cup S$ und
$R \cap S$ wohldefiniert.

Beispiel: $\overline{\Delta_M}$ ist die *Ungleichheitsrelation*.

Beispiel: Betrachte $< \subset \mathbb{R} \times \mathbb{R}$ und $\Delta_{\mathbb{R}}$; definiere $\leq := < \cup \Delta_{\mathbb{R}}$.

Beispiel: Betrachte $| \subset \mathbb{Z} \times \mathbb{Z}$. $| \cap \overline{\Delta_{\mathbb{Z}}}$ beschreibt ...???
Beispiel: Was haben Primzahlen zu tun mit: $| \cap (\overline{\Delta_{\mathbb{Z}}} \cup \overline{\{-1, 1\} \times \mathbb{Z}})$?

Operationen auf Relationen: Inversenbildung

Es sei $R \subseteq M_1 \times M_2$. Die *Inverse von* oder *Transposition zu* R ist gegeben durch:

$$R^- = R^{-1} = R^T = \{(y, x) \mid (x, y) \in R\}$$

Satz: $(R^-)^- = R$.
Satz: $(R \cup S)^- = R^- \cup S^-$.
Satz: $(R \cap S)^- = R^- \cap S^-$.

Anwendung von Relationen: relationale Datenbanken

(endliche) Relationen als Tabellen: (1) Persönliche Daten (PD)

Matrikel	Name	Vorname	m/w	Geb.datum	Anschrift
4000124	Kramer	Lutz	m	03.06.85	Thebäerstr. 8, Trier
4001031	Ludewig	Marianne	w	07.07.84	Am Weidengraben 95, Trier
4000327	Müller	Bernd	m	06.08.84	Kirchstr. 84, Fell
4001234	Meyer	Manfred	m	13.11.84	M.-Erzberger-Str. 9, Schweich
4000222	Schulz	Christian	m	22.12.84	H.-Reinholz-Str., Konz

Anwendung von Relationen: relationale Datenbanken

(endliche) Relationen als Tabellen: (2) Kursergebnisse (Noten)

Matrikel	Analysis	Programmieren	DSL	AFS	Rechnerstr.
4000124	1,3	2,3	1,7	1,3	3,0
4001031	3,3	2,0	2,3	2,0	1,0
4000327	2,0	2,0	1,7	2,0	2,3
4001234	5,0	4,0	5,0	—	4,0
4000228	2,3	5,0	2,3	—	—

Anwendung: Operationen auf relationalen Datenbanken

1. *Projektion* (project): Spaltenauswahl

2. *select*: Zeilenauswahl (gemäß gewisser Kriterien)

3. *join*: verbindet zwei Tabellen

Anwendung: Projektion

Beispiel: Auswahl aller Matrikelnummern, Vornamen, Namen und Anschriften aus PD liefert: R_1

Matrikel	Vorname	Name	Anschrift
4000124	Lutz	Kramer	Thebäerstr. 8, Trier
4001031	Marianne	Ludewig	Am Weidengraben 95, Trier
4000327	Bernd	Müller	Kirchstr. 84, Fell
4001234	Manfred	Meyer	M.-Erzberger-Str. 9, Schweich
4000222	Christian	Schulz	H.-Reinholz-Str., Konz

Anwendung: Selektion

Beispiel: Auswahl aller Matrikelnummern von Studenten, die DSL mindestens mit 2,0 bestanden haben (aus Tabelle Noten) liefert: R_2

Matrikel	Analysis	Programmieren	DSL	AFS	Rechnerstr.
4000124	1,3	2,3	1,7	1,3	3,0
4000327	2,0	2,0	1,7	2,0	2,3

Noch deutlicher wird das Ergebnis durch anschließende Projektion auf Matrikel und DSL (R_3):

Matrikel	DSL
4000124	1,7
4000327	1,7

Anwendung: join

Beispiel: Sämtliche Studenten, die DSL mit mindestens 2,0 bestanden haben, sollten angeschrieben werden. Dazu bilde den Join von R_1 und R_3:

Matrikel	Vorname	Name	Anschrift	DSL
4000124	Lutz	Kramer	Thebäerstr. 8, Trier	1,7
4000327	Bernd	Müller	Kirchstr. 84, Fell	1,7

Vor dem ersten Doppelstrich stehen die gemeinsamen Attribute, dann folgen die Attribute aus R_1 und dann die aus R_3.

Diskussion: Gemeinsamkeiten / Unterschiede der Relationenbegriffe bei den Datenbanken und “bei uns” ?