WS 2011/12

Zentralübung zur Vorlesung Diskrete Strukturen (Prof. Mayr)

Dr. Werner Meixner

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2011WS/ds/uebung/

26. Oktober 2011

Vorbemerkungen:

Spielregeln

Didaktik

Mathematik

ZÜ I

Übersicht:

1. Übungsbetrieb
2. Ziele der Zentralübung
3. Brückenschlag zu verwandten Vorlesungen
4. Metasprachliche Konzepte
5. Fragen zur Vorlesungshausaufgabe
6. Vorbereitung auf Tutorübungen Blatt 2

1. Übungsbetrieb

1.1 Organisation der Zentralübung

- Zeit: Mi 17.45–19:15 Ort: MW 0001
- Webseite:
  http://www14.in.tum.de/lehre/2011WS/ds/uebung/
- Kontakt Dr. W. Meixner:
  - Epost: meixner@in.tum.de
  - Telefon: 089 289 17713
  - Raum: MI 03.09.040
  - Sprechstunde: n.V.
- Material:
  - Gliederung auf Folien (siehe Webseite)
  - Ausarbeitung auf Tafel oder Handfolie

1.2 Aufgabenstruktur der Übungen

Die Übungsblätter bestehen aus Aufgaben für Vorbereitung (VA), Aufgaben für Tutorübung (TA) und Hausaufgaben (HA) mit folgender

Zielsetzung:

VA: Vorbereitung der Tutorübungen (inhaltlich parallel zur Vorl.).

TA: Stoff der Gruppenarbeit in der Tutorübung,

HA: Wiederholung und Lernkontrolle (Prüfungsstil).

Bearbeitung:
VA für Eigenstudium und Besprechung in der Zentralübung (ZÜ).
HA werden nicht besprochen, aber korrigiert.

Musterlösungen:
Zu allen Aufgaben der Übungsblätter und Klausur wird es Musterlösungen auf der Übungswebseite geben.

1.3 Persönliche Kommunikation

- Rückkopplung zur Übungsleitung:
  Dr. W. Meixner,
  Elpost: meixner@in.tum.de,
  Büro: MI 03.09.040,
  Sprechstunde: nach Zentralübung und n.V.
- Mitarbeit bei Musterlösungen
- Kontakt mit Tutoren im Arbeitsraum für DS Teilnehmer
- Kummerkasten: DS-Briefkästen und Epost

2. Ziele der Zentralübung

Diese sind: Spezielle und allgemeine didaktische Ziele.

Spezielle:

- **Vorbereitung und Nachbesprechung** für Tutor-, Haus- bzw. Prüfungsaufgaben der Übungsblätter bzw. Mittelklausur.
- **Persönliche Kommunikation**:
  - Rückkopplung zu Übungsleitung und Tutoren
  - Antworten auf Kummerkasten: Briefkästen und Epost

Allgemeine:

- **Brückenschlag** zu verwandten Vorlesungen in der Grundausbildung.
- Vertiefung der informellen **Metasprache**

3. Brückenschlag zu verwandten Vorlesungen

3.1

Mathematisch–Theoretische Informatik in den ersten 4 Semestern:

• Diskrete Strukturen	(DS)
• Informatik 1	(Info1)
• Lineare Algebra	(LA)
• Grundlagen: Algorithmen und Datenstrukturen	(GAD)
• Analysis	(A)
• Diskrete Wahrscheinlichkeitstheorie	(DWT)
• Theoretische Informatik	(Theo)

3.2

Spezielle Beziehungen von **DS** zu

- **Info1:** Algorithmenbegriff, Beweisverfahren, Aussagenlogik, Prädikatenlogik, Mengenlehre, Bäume, Rekursion und Induktion.
- **LA:** Matrizen, Matrixpotenzen, Vektorräume, Algebren, Körpertheorie.
- **GAD:** Bäume, Graphen, Zählverfahren, Landau Symbole.
- **A:** Reelle und komplexe Zahlen, Grenzwerte, Potenzreihen, Polynome.
- **DWT:** Zählmaße und Zählprobleme, Kombinatorik.
- **Theo:** Graphentheorie, Eigenschaften von Algorithmen, Rekursionstheorie, Komplexitätstheorie.

4. Grundlegende Metasprachliche Begriffe

4.1 Basisbegriffe der Informatik

Struktur — Aussage — Beweis — Verfahren

stehen wechselseitig in Beziehung:

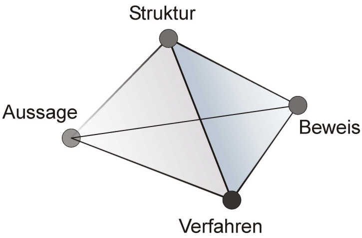
5. Grundlegende Metasprachliche Begriffe

5.1 Basisbegriffe der Informatik

Struktur — Aussage — Beweis — Verfahren

stehen wechselseitig in Beziehung:

Tetraeder der Basisbegriffe



Informelle Präzisierung:

- Struktur: (Art der) Zusammenfassung (einer Vielheit) von (abstrakten) Objekten.
- Verfahren: (Art der) Zusammenfassung (einer Vielheit) von (abstrakten) Vorgängen.

- Aussage: Sprachliches Gebilde, für das es sinnvoll ist zu sagen, dass es wahr oder falsch ist. (*Aristoteles*)
- Beweis: Verfahren zur Bestimmung des Wahrheitswertes einer Aussage.

Die Begriffe 'Objekt' und 'Vorgang' bedingen sich gegenseitig wie folgt:

- Jeder (logische) Vorgang führt zu einem (logischen) Objekt als Ergebnis.
- Umgekehrt ist jedes (logische) Objekt das Ergebnis eines (logischen) Vorgangs.

Fundamentalsatz

,,In der mathematisch–theoretischen Informatik ist das logische Konzept des 'Vorgangs' gleichberechtigt zum logischen Konzept des 'Objekts':
sie bedingen sich gegenseitig.“
(*Meixner, 2003*)

Daraus folgt:

,,Die mathematisch–theoretische Informatik kann nicht wie die Mathematik allein auf der Mengenlehre aufgebaut werden.“

Damit erhalten Verfahren oder Algorithmen ihre Bedeutung.

Bemerkung:

In natürlichen Sprachen gibt es zweideutige (bivalente) Begriffe, die sowohl als Begriff für Objekte als auch als Begriff für Vorgänge gedeutet werden können. Beispiel: 'Zusammenfassung'.

Das Wort 'Zusammenfassung' kann sowohl den Vorgang des Zusammenfassens als auch das 'objektive' Ergebnis dieses Vorgangs bedeuten.

Diese Zweideutigkeit ermöglicht eine Vertauschung einer operationellen gegen eine beschreibende Interpretation.

Die gegenseitige Bedingtheit der Begriffe „Objekt“ und „Vorgang“ begründet fundamentale Dualitätsbeziehungen in der Informatik.

Dies kann erst am Ende des Semesters diskutiert werden mit Rückgriff sowohl auf die Ergebnisse von DS als auch von Info1.

$\perp$

Das *total unbestimmte Objekt* ist der Inbegriff eines namenlosen, gedanklich erzeugten, logischen Platzhalters, der „logischen Stelle“, die frei von jeder inhaltlichen Bestimmung ist und als zählbares „Exemplar“ „mehrfach“ auftreten bzw. erzeugt werden kann. Das total unbestimmte Objekt ist der Begriff eines „Vorgangs“ schlechthin und ihm ist keine Bestimmung zugeordnet. Man kann auch sagen, dass ihm nur die leere Bestimmung zugeordnet ist.

(Meixner, 2007)

Wir bezeichnen total unbestimmte Objekte mit

$\perp$ (gesprochen „Boden“ oder „bottom“).

$\top$

Der Gegenbegriff (begriffliche Antithese) zum total unbestimmten Objekt ist das *total bestimmte Objekt* oder (mathematische) *Universum*. Das Universum ist definiert als der Inbegriff des bestimmten Objekts, das nicht konstruiert werden kann, sondern a priori vorhanden ist. Es bedeutet den „logischen Raum“, in dem alle konstruierten, mathematischen Objekte gedacht werden.

(Meixner, 2007)

Wir bezeichnen es mit

$$\top \qquad \text{(gesprochen „Topp“).}$$

Wir können $\perp$ bzw. $\top$ auch als *initiales* bzw. *finales* Objekt bezeichnen.

5.2 Vertiefung der informellen Metasprache

Wissenschaftliche Schulung und Entwicklung
vollzieht sich im Spannungsfeld folgender Begriffspaare:

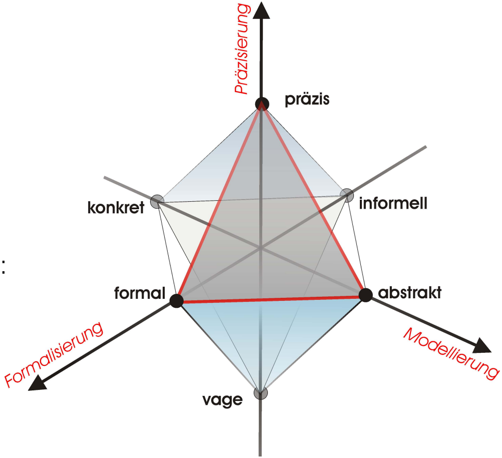
- vage — präzis
- konkret — abstrakt
- informell — formal

5.3 Vertiefung der informellen Metasprache

Wissenschaftliche Schulung und Entwicklung
vollzieht sich im Spannungsfeld folgender Begriffspaare:

- vage — präzis
- konkret — abstrakt
- informell — formal

Darstellung im Oktaeder:



- *Durch „Abstraktion“ „erzeugen“ wir abstrakte (= von uns gedachte) Inhalte (Objekte, Vorgänge), die* **nicht identisch** *sind mit dem „konkret Gemeinten“!*
  (Modellierung)
- *Wir formalisieren abstrakte Inhalte, indem wir sie durch konkrete Zeichen(folgen) „benennen“.*
  (Formalisierung)
- *Wir präzisieren abstrakte Inhalte, indem wir logische Konsequenzen mit dem Gemeinten vergleichen, und dann die Modellierung adäquat ändern.*
  (Präzisierung)

Abstraktionen versus Phantasien:

„Wer über einen gedachten Stein stolpert und sich dabei den Arm bricht, der hat ein Problem mit der

Wahrnehmung der Wirklichkeit.“

6. Fragen zur Vorlesungshausaufgabe

6.1 Assoziativität des Relationenprodukts

Sei M eine Menge. Seien R, S und T Relationen über M, d. h. $R, S, T \subseteq M \times M$.

Zeigen Sie das Assoziativgesetz $R \circ (S \circ T) = (R \circ S) \circ T$!

Beweis:

$$(x, y) \in R \circ (S \circ T)$$

$$\iff \quad (\exists u)\ [(x, u) \in R \text{ und } (u, y) \in S \circ T]$$

$$\iff \quad (\exists u)\ [(x, u) \in R \text{ und } (\exists v)\ [(u, v) \in S \text{ und } (v, y) \in T]\,]$$

$$\iff \quad (\exists u\, \exists v)\ [(x, u) \in R \text{ und } (u, v) \in S \text{ und } (v, y) \in T]$$

$$\iff \quad (\exists v)\ [\,(\exists u)\,[(x, u) \in R \text{ und } (u, v) \in S] \text{ und } (v, y) \in T]$$

$$\iff \quad (\exists v)\ [(x, v) \in R \circ S \text{ und } (v, y) \in T] \quad \iff$$

$$(x, y) \in (R \circ S) \circ T\,.$$

Daraus folgt die Mengengleichung $R \circ (S \circ T) = (R \circ S) \circ T$.

7. Vorbereitung TÜ Blatt 2

7.1 VA 1

1. Zeichnen Sie ein Hasse-Diagramm für die natürliche $\leq$-Ordnung der Zahlen $[6]$.

   Wie ergibt sich die $\leq$-Ordnung auf $[6]$ aus dem entsprechenden Hasse-Diagramm?

Erklärung:

Ein **Hasse-Diagramm** ist eine graphische Darstellung einer transitiven und reflexiven, binären Relation R.

Paare (a, b) werden als Pfeile
oder z. B. als Kanten von oben nach unten
zwischen Punkten a und b dargestellt.

Dabei ist das wichtigste darstellerische Prinzip,
dass all Jenes nicht gezeichnet wird,
was sich durch die Eigenschaften der Transitivität und Reflexivität
der darzustellenden Relation von selbst versteht.

Abstrakt betrachtet ist aber das Hasse-Diagramm selbst wieder eine Relation H, die in einem definierten Verhältnis zu R steht.

Antwort:

- Für ein Hasse-Diagramm H einer transitiven und reflexiven Relation R gilt stets $H \subseteq R$.
  Die reflexive und transitive Hülle von H ist gleich R.
- H ist stets minimal in dem folgenden Sinn:
  H enthält keine reflexiven Pfeile (x, x) und nur solche Pfeile $(x, y) \in R$, die sich nicht aus der transitiven Verkettung von Pfeilen $(x, z) \in H$ und $(z, y) \in H$ ergeben.
- Für das (abstrakte) Hasse-Diagramm H der geordneten Menge $[6]$ gilt damit

$$H = \{(1,2),(2,3),(3,4),(4,5),(5,6)\}\,.$$

(Zeichnung)

R ergibt sich dann aus H als reflexive und transitive Hülle.

2. Wir entfernen das Paar $(3,4)$ aus der Relation $\leq$ auf $\mathbb{N}$. Ist dann die resultierende Relation noch transitiv? Begründung!

Antwort: Die resultierende Relation ist immer noch transitiv.

Begründung: Die Eigenschaft der Transitivität für eine Relation R ist genau dann verletzt, wenn einer der beiden folgenden Fälle vorliegt:

1. Fall: Es gibt paarweise verschiedene Elemente x, y und z, so dass $(x,y) \in R$ und $(y,z) \in R$ gilt, nicht aber (x,z) aus R, d. h. dass $(x,z) \notin R$ gilt.

2. Fall: Es gibt verschiedene Elemente x, y, so dass $(x,y) \in R$ und $(y,x) \in R$ gilt, aber gleichzeitig $(x,x) \notin R$ gilt.

Entfernt man das Paar $(3,4)$ aus $\leq$, dann muss man prüfen, ob nun der Fall 1 eintreten kann.

Nun gilt: Die resultierende Relation ist immer noch transitiv, weil es kein anderes Element z „echt zwischen" 3 und 4 gibt, d. h. ein z mit $3 \leq z$ und $z \leq 4$ und $z \neq 3, z \neq 4$.

Gäbe es ein solches z, dann könnte $(3,4)$ nicht entfernt werden, ohne die Transitivitätseigenschaft nach Fall 1 zu verletzen.

Dann aber dürfte auch $(3,4)$ nicht im Hasse-Diagramm sein.

(Zeichnung)

3. Für welche Mengen M ist die Inklusionsrelation $\subseteq$ auf der Potenzmenge $\mathcal{P}(M)$ eine totale Ordnung? Begründung!

Antwort: Nur für $|M| \leq 1$ ist $\mathcal{P}(M)$ total geordnet.

Falls $a, b \in M$ mit $a \neq b$,
dann gilt weder $\{a\} \subseteq \{b\}$ noch $\{b\} \subseteq \{a\}$.

7.2 VA 2

1. Gibt es eine injektive Abbildung $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$? Begründung!

Antwort:
Sei $f(m, n) = 2^m \cdot 3^n$. Dann ist f injektiv.

Begründung:
Wir betrachten zwei Paare $x_1 = (m_1, n_1)$ und $x_2 = (m_2, n_2)$ natürlicher Zahlen und nehmen an, dass beide Paare auf ein und dieselbe natürliche Zahl y abgebildet werden, also dass gilt

$$f(x_1) = 2^{m_1} \cdot 3^{n_1} = y = 2^{m_2} \cdot 3^{n_2} = f(x_2)\,.$$

O.B.d.A. können wir $m_1 \leq m_2$ annehmen.

Es folgt

$$3^{n_1} = 2^{m_2 - m_1} \cdot 3^{n_2} \,.$$

Wäre $m_2 - m_1 > 0$,
dann müßte 2 ein Teiler von 3 sein, weil 2 prim ist.
Aber 3 ist unzerlegbar.
Also folgt $m_1 = m_2$.

Analog erhält man $n_1 = n_2$, mithin $x_1 = x_2$.

Wir haben also gezeigt:
Es kann nicht sein, dass zwei verschiedene Elemente x_1 und x_2 durch f auf ein und dasselbe y abgebildet werden.
Genau das besagt die Injektivität von f.

2. Gibt es eine surjektive Abbildung $f : \mathbb{N} \to \mathbb{Z}$? Begründung!

Antwort:
Sei

$$f(n) = \begin{cases} \frac{n}{2} & : \quad n \text{ gerade} \\ \frac{1-n}{2} & : \quad n \text{ ungerade} \end{cases} .$$

f ist surjektiv.

Begründung:
Es gibt zu jeder ganzen Zahl y eine natürliche Zahl n, so dass $f(n) = y$.
Denn:
Falls $y > 0$, gilt dies für $n = 2y$.
Falls $y \leq 0$, gilt dies für $n = -2y + 1$.

Bemerkung: f ist sogar injektiv, also insgesamt bijektiv.

3. Gilt für $f : X \to Y$ und $A \subseteq X$ stets $f^{-1}(f(A)) \subseteq A$? Begründung!

Antwort: Nein!

Begründung:
Seien $X = \{1, 2\}, Y = \mathbb{N}$ und $f(1) = 3, f(2) = 3$.
Wir betrachten $A = \{1\}$.

Dann gilt $f(A) = \{3\}$ und $f^{-1}(\{3\}) = \{1, 2\}$.
Offenbar gilt $2 \notin A$, aber $2 \in f^{-1}(f(A))$,
d. h. $f^{-1}(f(A)) \not\subseteq A$.

7.3 VA 3

Eine der grundlegendsten Operationen der Analysis und Funktionentheorie ist die Bildung der Potenz p^q.

Man nennt die daraus abgeleitete Funktion x^a Potenzfunktion,

und die Funktion a^x Exponentialfunktion
mit dem Spezialfall e^x.

Die Umkehrung von a^x führt auf die Logarithmusfunktion $\log_a x$.

Allgemein wird der Logarithmus einer Zahl x zur Basis b mit

$$\log_b x$$

bezeichnet. Soll eine Aussage für beliebige positive Basen gelten, so schreibt man häufig

$$\log x\,.$$

Die Formel für die Umrechnung verschiedener Basen lautet dann

$$\log_b x = \frac{\log x}{\log b}\,.$$

Für $b = e$ wird $\ln x$,
für $b = 10$ wird $\lg x$,
für $b = 2$ wird $\operatorname{ld} x$
geschrieben.

Im Folgenden setzen wir die grundlegenden Eigenschaften der Logarithmus- bzw. Exponentialfunktion als bekannt voraus, also z. B.

$$\begin{aligned} 0 < e^{x+y} &= e^x \cdot e^y\,, \\ e^0 &= 1 < e^z\,, \end{aligned}$$

für alle $x, y \in \mathbb{R}$ und $z \in \mathbb{R}^+$.

Insbesondere setzen wir die Stetigkeit der Funktionen voraus.

1. Geben Sie einen direkten Beweis für die folgenden Gleichungen:

$$a^{\log_b c} = c^{\log_b a}\,, \qquad n^{\ln \ln n} = (\ln n)^{\ln n}\,,$$

wobei

$$0 < a\,,\ 0 < b\,,\ 0 < c \text{ bzw. } 0 < n$$

vorausgesetzt wird.

Anwort:

Die Beweise kann man durch Logarithmieren führen.

Zum Beweis einer Gleichung

$$x = y$$

für positive x und y beweist man zunächst

$$\log_d x = \log_d y\,,$$

weil daraus wegen $d^{\log_d z} = z$ für $z = x$ und $z = y$,
sofort $x = y$ folgt.

Wir zeigen also

$$\log_b a^{\log_b c} = \log_b c^{\log_b a} \qquad \text{bzw.} \qquad \ln n^{\ln \ln n} = \ln\,(\ln n)^{\ln n}\,.$$

Es gilt

$$\begin{aligned}\log_b a^{\log_b c} &= (\log_b c) \cdot (\log_b a) \\ &= (\log_b a) \cdot (\log_b c) \\ &= \log_b c^{\log_b a} \qquad (1)\end{aligned}$$

und

$$\begin{aligned}\ln n^{\ln \ln n} &= (\ln \ln n) \cdot (\ln n) \\ &= (\ln n) \cdot \ln (\ln n) \\ &= \ln (\ln n)^{\ln n} \, . \qquad (2)\end{aligned}$$

7.4 VA 4

1. Geben Sie eine aussagenlogische Formel F an, so dass F und $\neg F$ erfüllbar ist!

Antwort:

Sei $F = (x \equiv y)$.

Dann ist die Formel F unter der Belegung $x \mapsto 1, y \mapsto 1$ wahr, denn es gilt $(1 \equiv 1) = 1$ (siehe Tabelle in der Vorlesung).

Also ist F erfüllbar.

Die Formel $\neg F$ ist unter der Belegung $x \mapsto 1, y \mapsto 0$ wahr, denn es gilt $(1 \equiv 0) = 0$ und deshalb $\neg(1 \equiv 0) = 1$.

Also ist $\neg F$ erfüllbar.

2. Geben Sie eine nicht erfüllbare Formel an!

Antwort:

$F = \text{false}\,.$

oder

$F = x \wedge \neg x\,.$

7.5 VA 4

Bestimmen Sie die Semantik des folgenden aussagenlogischen Ausdrucks in den Variablen x, y, z als Wahrheits(wert)tabelle:

$$((x \Rightarrow y) \land \neg(x \Rightarrow z)) \lor (z \Rightarrow y)\,.$$

Wir berechnen in mehreren Spalten die Zwischenergebnisse. Die Eingabeparameter sollten aus Gründen der besseren Lesbarkeit stets lexikographisch sortiert werden.

Sei $F = ((x \Rightarrow y) \land \neg(x \Rightarrow z)) \lor (z \Rightarrow y)$.

x	y	z	$x \Rightarrow y$	$\neg(x \Rightarrow z)$	$(x \Rightarrow y) \land \neg(x \Rightarrow z)$	$z \Rightarrow y$	F
0	0	0	1	0	0	1	1
0	0	1	1	0	0	0	0
0	1	0	1	0	0	1	1
0	1	1	1	0	0	1	1
1	0	0	0	1	0	1	1
1	0	1	0	0	0	0	0
1	1	0	1	1	1	1	1
1	1	1	1	0	0	1	1

Man kann die Zwischenergebnisse auch direkt in eine Spalte unter den Operator schreiben und dazu nur die Formel F einmalig in die Kopfzeile der Tabelle schreiben.

Allerdings leidet dann die Übersichtlichkeit.

7.6 VA 6

Welcher Zusammenhang besteht zwischen einem allgemeinen Venn-Diagramm für drei Mengen A, B und C einerseits und andererseits
der Menge der Vollkonjunktionen für drei Aussagenvariablen p, q, r ?

Antwort:

Allgemeine Venn-Diagramme dreier Mengen A, B und C
stellen schematisch zunächst
alle möglichen Durchschnitte dieser drei Mengen dar.

(siehe dazu Blatt 1, insbesondere Tutoraufgabe 2.2 dort)

Zeichnerische Darstellungsmittel sind z. B. Kreise oder Quadrate.

Bei Zeichnung eines Kreises (oder Quadtrats) gibt es grundsätzlich die Möglichkeit,

den Innenbereich und den Außenbereich

als Darstellung je einer Menge aufzufassen.

Mit drei Kreisen für A bzw. B bzw. C
kann man also deren Komplemente $\overline{A}$ bzw. $\overline{B}$ bzw. $\overline{C}$ darstellen,

und mithin alle Durchschnitte der 6 Mengen A, B, C, $\overline{A}$, $\overline{B}$, $\overline{C}$.

Die leere Menge wird als Außenbereich des Universums, d. h. der gesamten Zeichnungsebene, aufgefaßt.

Das Universum kann durch den Durchschnitt von 0 Mengen als Grenzfall des Durchschnitts von n Mengen dargestellt werden.

Frage:

Wie viele verschiedene Durchschnitte können dargestellt werden?

Einen Zusammenhang des Venn-Diagramms mit den Vollkonjunktionen über p, q und r kann man herstellen, indem man z. B. eine Zuordnung

$$p \mapsto A,\ q \mapsto B \text{ und } r \mapsto C$$

definiert und die

Konjunktion als Mengendurchschnitt

sowie die

Negation als Komplementbildung

interpretiert.

Dann entspricht jeder Vollkonjunktion über p, q und r genau eines der kleinsten, nicht weiter unterteilten Gebiete im Venn-Diagramm.

Dies sind jene Gebiete, die alle zusammen eine

Partitionierung des Universums

darstellen, d. h.
eine Aufteilung des Universums in disjunkte (Teil-)Mengen.

Bemerkung:

Es stellt sich die interessante weitergehende Frage,
welche Aussage man den Aussagenvariablen, z. B. p, zuordnen
könnte anstelle einer Menge, z. B. A?

Dahinter steht die Frage, wie die Aussagenlogischen Formeln mit Mengen und Mengengesetzen zusammenhängen.

Die Antwort auf die letztgestellte Frage ist wie folgt:

Für jedes Element x eines Universums U
und jede Teilmenge A von U gibt es die Aussage $x \in A$.

Und A ist dann nichts anderes als die Menge aller x, für die die Aussage $x \in A$ zutrifft:

$$A = \{x\,;\, x \in A\} \quad \text{(intensionale Mengendarstellung)}\,.$$