Übung: Teilmengen

A, B seien Mengen.

Zu zeigen ist: wenn $A \subseteq B$ dann auch $2^A \subseteq 2^B$

Beweis:

Für alle Elemente m einer Menge M, die Teilmenge einer Menge N ist, gilt, dass m auch Element von N ist. (Definition der Teilmenge)

$$\text{für alle } a \in A : a \in B$$

Dies gilt auch für alle Elemente in Teilmengen von A, somit sind alle Teilmengen von A auch Teilmengen von B,

$$\text{für alle } C \subseteq A : C \subseteq B$$

und damit Element von 2^B. (Definition der Potenzmenge)

$$\text{für alle } C \subseteq 2^B$$

Damit sind alle Elemente von 2^A auch Element von 2^B, also gilt:

$$2^A \subseteq 2^B \blacksquare$$

Gilt auch die Umkehrung?

Funktionen (= Abbildungen)

Eine Relation F von M nach N heisst

partielle Funktion gdw.

wenn $\langle x, y\rangle \in F$ und $\langle x, z\rangle \in F$, dann $y = z$.

D.h., ein $x \in M$ wird auf höchstens ein $y \in N$ abgebildet.

Schreibweise: $F : A \to B$; $F(a) = b$

$a \in A$ *Argumente*, $b \in B$ *Werte*.

A heisst auch *Urbild*,

$\{b \mid b \in B$ und es gibt a mit $F(a) = b\}$ *Bild* von F,

a Urbild von $F(a)$.

oft Kleinbuchstaben $f, g, h, ...$ für Funktionen

(*totale*) Funktion von M nach N: jedes $x \in M$ ...

Beispiel: Sei L eine Menge von lexikalischen Schlüsseln, E die Menge der Einträge.
Ist $f : L \mapsto E$ mit $f(l) =$ Eintrag zu l eine Funktion?

Eigenschaften von Funktionen

surjektiv:

$\{F(a) \mid a \in A\} = B$

“jedem Element von B ist ein Urbild zugeordnet”

injektiv: Eins-zu-eins-Abbildung, d.h.:
wenn $F(a) = F(b)$, dann $a = b$.

“verschiedene Argumente haben verschiedene Funktionswerte.”

bijektiv: injektiv und surjektiv

“jedem Element von B ist genau ein Urbild zugeordnet”

Übungen zu Funktionseigenschaften

Sei $f : A \to B$. Sind die folgenden Aussagen wahr oder falsch?

1. f ist genau dann bijektiv, wenn f umkehrbar ist.
2. Ist f surjektiv, so hat jedes $a \in A$ mindestens ein Bild $f(a) \in B$.
3. Hat jedes $a \in A$ mindestens ein Bild $f(a) \in B$, so ist f surjektiv.
4. Gibt es zu jedem $a \in A$ höchstens ein $b \in B$ mit $f(a) = b$, so ist f injektiv.
5. Gibt es zu jedem $b \in B$ ein $a \in A$ mit $f(a) = b$, so ist f injektiv.
6. f ist genau dann bijektiv, wenn zu jedem $a \in A$ genau ein $b \in B$ existiert mit $f(a) = b$.
7. f ist genau dann bijektiv, wenn zu jedem $b \in B$ genau ein $a \in A$ existiert mit $f(a) = b$.
8. Ist f bijektiv, so gibt es zu jedem $b \in B$ höchstens ein $a \in A$ mit $f(a) = b$.

1, 2, 5, 7, 8 sind wahr, die anderen falsch.

1. Ist f bijektiv, so gibt es zu jedem $a \in A$ höchstens ein $b \in B$ mit $f(a) = b$.
2. Folgt aus $f(a_1) = f(a_2)$ für alle $a_1, a_2 \in A$, dass $a_1 = a_2$, dann ist f injektiv.
3. Sind A und B endlich und ist f injektiv, dann ist f auch bijektiv.
4. $f : A \to f(A)$ ist stets surjektiv.
5. Gilt $B \subset A$, so kann f nicht bijektiv sein.
6. Ist f surjektiv und die Umkehrrelation von f eine injektive Abbildung, so ist f auch injektiv.
7. Ist f injektiv und die Umkehrrelation von f eine surjektive Abbildung, so ist f bijektiv.
8. Ist f surjektiv und nicht injektiv, so ist die Umkehrrelation eine surjektive, nicht injektive Funktion.
9. Ist $A = B$, so ist jede Injektion auch eine Bijektion
10. Jede Injektion lässt sich durch Einschränkung des Wertebereichs zu einer Bijektion machen.

1, 2, 4, 5, 6, 7, 10 sind wahr, die anderen falsch.

Verknüpfung von Funktionen

Komposition, Verknüpfung

Gegeben: $F : A \to B, G : B \to C,$

dann: $G \circ F : A \to C$ mit $(G \circ F)(a) = G(F(a))$

(Achtung: Schreibrichtung...)

Sei $F : A \to B$ gegeben. Dann gilt:

$$id_B \circ F = F = F \circ id_A$$

und für bijektive F:

$$F^{-1} \circ F = id_A \text{ und } F \circ F^{-1} = id_B$$

mehrstellige Funktionen: mit Hilfe von Tupeln...

Beispiel Komposition

Gegeben: Mengen von Sätzen in natürlichen Sprachen: E englisch, D deutsch, S spanisch.

Ausserdem Funktionen:

$f_1 : E \to D$,

$f_2 : S \to E$,

$f_3 : D \to S$,

Wie übersetze ich einen deutschen Satz s in einen englischen?

zuerst deutsch nach spanisch, dann spanisch nach englisch:

$$f_2(f_3(s)) = (f_2 \circ f_3)(s)$$

Wie viele einzelne Übersetzungsfunktionen braucht man, um Übersetzer für n Sprachen zu konstruieren?

Wenn nicht mehr als zwei Schritte vorgenommen werden sollen?

Mengen mit unendlicher Kardinalität

Zwei (endliche) Mengen heissen äquivalent, wenn sie die gleiche *Anzahl* von Elementen haben : $A \sim B$ gdw. $|A| = |B|$

Zwei Mengen sind äquivalent, wenn zwischen ihnen eine bijektive Abbildung existiert.

Eine Menge ist unendlich, wenn sie zu einer ihrer echten Teilmengen äquivalent ist.

Beispiel: Abbildung von **N** $= \{0, 1, 2, 3, ...\}$ auf $\{0, 2, 4, 6, ...\}$? Auf die Menge der ganzen Zahlen?

Mengen, die äquivalent sind zur Menge der Natürlichen Zahlen **N**, heissen aufzählbar.

Kardinalität dieser Mengen: $\aleph_0$ (Aleph)

Noch “grössere” Mengen?

Prinzip der vollständigen Induktion

Ziel: eine allgemeine Aussage über Elemente aufzählbarer Mengen zu beweisen.

Vorgehensweise:

1. A(1), Induktionsanfang: Beweis für das erste Element.
2. A(k) $\rightarrow$ A(k+1), Induktionsschritt:
   (a) Annahme: Aussage gelte für die ersten k Elemente.
   (b) Zeige, dass daraus Aussage über $k+1$. Element folgt.
3. Induktionsschluss: Daraus folgt, dass die Aussage für alle Elemente gilt!

Beispiel

Behauptung:

Die Anzahl der Elemente der Potenzmenge einer endlichen Menge A ist gleich 2 hoch der Anzahl der Elemente von A

Beweis durch Induktion über die Anzahl der Elemente von A:

1. Induktionsanfang: A habe genau ein Element, e_1. Dann ist $2^A = \{\emptyset, \{e_1\}\}$, und hat zwei Elemente, $2 = 2^1$
2. Induktionsschritt:
   (a) Annahme: Sei $A = \{e_1, ..., e_k\}$, $|\, 2^A \,| = 2^{|\, A \,|}$
   (b) Sei $A' ::= A \cup \{e_{k+1}\}$.
   Dann gilt: $2^{A'} = 2^A \cup \{A'\} \cup ... \cup \{e_1, e_{k+1}\} \cup \{e_{k+1}\}$,
   d.h. alle Teilmengen von A erweitert um $\{e_{k+1}\}$,
   d.h. genau $2^{|\, A \,|}$ mehr Mengen.
   Daraus folgt: $|\, 2^{A'} \,| = 2^{|\, A \,|} + 2^{|\, A \,|} = 2^{|\, A \,|+1}$
3. Induktionsschluss:
   Daraus folgt, dass $|\, 2^A \,| = 2^{|\, A \,|}$ für alle endlichen Mengen gilt.

überaufzählbare Mengen

Theorem von Cantor:

die Potenzmenge einer Menge hat eine grössere Kardinalität als die Menge selbst.

$$|\, A \,| \;<\; |\, 2^A \,|$$

Beweis durch Widerspruch:

Annahme: es existiert bijektive $F : A \to 2^A$.

Sei $B = \{x \in A \mid x \notin F(x)\}$.

Es muss $y \in A$ mit $F(y) = B$ geben.

Ist y Element von B?

Daraus folgt: $|\, \mathbf{N} \,| \;<\; |\, 2^{\mathbf{N}} \,|$

Diagonalisierungsargument (Gödel):

Wenn $\mathbf{N} \sim 2^{\mathbf{N}}$, dann muss es eine Möglichkeit geben, $2^{\mathbf{N}}$ systematisch hinzuschreiben.

Sei diese Folge von Mengen $S_0, S_1, S_2, ...$

Sei $S* ::= \{n \mid n \notin S_n\}$.

Es gibt kein n mit $S* = S_n$, $S*$ kann nicht in der Liste stehen, also kann es diese Liste gar nicht geben.

Algebren

Eine *algebraische Struktur* oder *Algebra* **A** ist eine Menge A zusammen mit einer oder mehreren Operationen f_i ($+, \circ, \times$ für f_i):

$$\mathbf{A} = \langle A, f_1, f_2, ..f_n \rangle$$

Beschränkungen: die Stelligkeit jeder Operation muss endlich sein; jede Anwendung der Operationen ergibt genau ein Element aus A.

Gegeben: $\langle A, \circ \rangle$

Axiom 1 Abgeschlossenheit:

A ist unter $\circ$ abgeschlossen, d.h. für alle $a, b \in A$ existiert ein $c \in A$ mit $a \circ b = c$.

Axiom 2 Eindeutigkeit:

Wenn $a = a'$ und $b = b'$, dann $a \circ b = a' \circ b'$

$\langle B, \circ \rangle$ ist eine *Unterstruktur / Subalgebra* vom $\langle A, \circ \rangle$ gdw. $B \subset A$ und B abgeschlossen bez. $\circ$

Eigenschaften von Operationen

Gegeben: eine Operation $\circ$ in A.

Für alle $a, b, c \in A$:

- *Assoziativität*

$$(a \circ b) \circ c = a \circ (b \circ c)$$

  assoziativ: Addition, Multiplikation; nicht-assoziativ: Subtraktion, Division

- *Kommutativität*

$$a \circ b = b \circ a$$

  kommutativ: Multiplikation, ...; nicht kommutativ: Subtraktion, ...

- *Idempotenz*

$$a \circ a = a$$

  idempotent: Schnittmengenbildung, ...

- *Distributivität* zusätzlich: zweite Operation $\diamond$

$$a \circ (b \diamond c) = (a \circ b) \diamond (a \circ c)$$

  Multiplikation distribuiert über Addition, aber nicht umgekehrt

spezielle Elemente

- *links- bzw. rechtsneutrales Element, neutrales Element*

  $$e_l \circ a = a \text{ bzw. } a \circ e_r = a$$

  Komposition von Funktionen $F : M \to N$: identische Abbildung id_M, bzw. id_N; 0 ist rechtsneutral für Subtraktion ...

  Bei kommutativen Operationen gilt $e_l = e_r = e$, neutrales Element. (Kommutativität hinreichend, nicht notwendig)

  Wenn ein neutrales Element existiert, ist es eindeutig! Beweis...

- *inverse Elemente*

  Gegeben neutrales Element e.

  Für a existiert rechts-(links-)inverses El. $a_r(a_l)$, wenn

  $$a \circ a_r = e \text{ bzw. } a_l \circ a = e$$

  $a^{-1} = a_l = a_r$ heisst *inverses* Element von a.

  Wenn a invers zu b, dann auch b zu a!

  Beispiele?

Verknüpfungstafeln

Zeigen von Eigenschaften: “durchrechnen”

z.B. mit Verknüpfungstafeln:

Bsp: Addition modulo 4 in $\{0, 1, 2, 3\}$

$+_{mod4}$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

abgeschlossen, kommutativ, inverse Elemente, neutrales Element...

Morphismen

Abbildungen zwischen Algebren, φ : **A** $\rightarrow$ **B**. Gleiche Anzahl der Operationen!

Sei **A** $= \langle A, \circ \rangle$, **B** $= \langle B, \diamond \rangle$

- *Morphismus*: Funktion φ mit

$$\varphi(a_1 \circ a_2) = \varphi(a_1) \diamond \varphi(a_2)$$

, φ heisst *verknüpfungstreu*.

- *Isomorphismus:*
  verknüpfungstreue, bijektive Funktion φ
  A und **B** heissen *isomorph*, wenn es einen Isomorphismus zwischen ihnen gibt.

- *Automorphismus:*
  Isomorphismus von **A** auf sich selbst,
  z.B. identische Abbildung

Gruppen

Eine Struktur **G** $= \langle G, \circ \rangle$ ist eine *Gruppe*, wenn gilt:

G1: **G** ist eine Algebra (d.h. $\circ$ ist vollständig definiert und G ist unter $\circ$ abgeschlossen)

G2: $\circ$ ist assoziativ

G3: G enthält ein neutrales Element

G4: Jedes Element in G hat ein inverses.

Bsp: positive rationale Zahlen und Multiplikation, Addition modulo 4 in $\{0, 1, 2, 3\}$, gerade Zahlen und Addition.

Abelsche Gruppe: zusätzlich kommutativ.

Gruppen II

Untergruppe: Subalgebra und selbst Gruppe

Ordnung einer Struktur: Anzahl der Elemente der Menge

- Die Ordnung jeder Untergruppe einer endlichen Gruppe **G** teilt die Ordnung von **G**.

Beispiel: Addition modulo 4 in $\{0, 1, 2, 3\}$,

$\mathbf{G}_{+_{mod4}} = \langle \{0, 1, 2, 3\}, +_{mod4} \rangle$

Untergruppen:

$\langle \{0, 1, 2, 3\}, +_{mod4} \rangle$

$\langle \{0, 2\}, +_{mod4} \rangle$

$\langle \{0\}, +_{mod4} \rangle$

- Alle Subalgebren von endlichen Gruppen sind ebenfalls Gruppen, d.h., nur Abgeschlossenheit muss gezeigt werden...

- Der Schnitt zweier Untergruppen ist wieder eine Untergruppe.

Halbgruppen: nur G1 + G2

Monoide: G1, G2 + G3

Abelsches Monoid: kommutatives Monoid

Integritätsringe

D $= \langle D, +, \cdot \rangle$ ist ein Integritätsring, wenn gilt:

$\langle D, + \rangle$ ist Abelsche Gruppe mit neutralem Element 0

$\langle D, \cdot \rangle$ ist Abelsches Monoid mit neutralem Element $1, 1 \neq 0$

(Distributivgesetz)
Für alle $a, b, c \in D, a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

(Kürzungsregel)
Wenn $c \neq 0$ und $c \cdot a = c \cdot b$, dann $a = b$.

Beispiel: Ganze Zahlen, Addition und Multiplikation